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 IPR2023-01281
U.S. Patent No. 10,715,878 B2
Issue Date: July 14, 2020

Title: TARGETED TELEVISION ADVERTISEMENTS BASED ON ONLINE BEHAVIOR

DECLARATION OF CHRISTOPHER M. SCHMANDT

I. INTRODUCTION AND QUALIFICATIONS 7
A. Qualifications and Experience 7
B. Materials Considered 9
II. PERSON OF ORDINARY SKILL IN THE ART 11
III. STATEMENT OF LEGAL PRINCIPLES 12
A. Claim Construction 12
B. Obviousness 14
IV. THE ’878 PATENT 20
A. Overview of the Specification 20
B. The Challenged Claims 23
V. APPLICATION OF THE PRIOR ART TO CHALLENGED CLAIMS 24
A. Brief Summary of Prior Art 25
1. Prior Art Common to All Grounds 25
(a) Baig and Baig Provisional (EX1003/1004) 25
(b) Laidlaw (EX1006) 37
(c) Sitaraman (EX1007) 42
(d) Hahn (EX1008) 43
2. Additional Prior Art for Certain Dependent Claims 45
(a) Xu (EX1009) 45
(b) Gerace (EX1010) 47
B. Ground 1: Claims 1-2, 8-10, 13-14, 19, and 22 Are Obvious Over Baig in view of Laidlaw, Sitaraman, and Hahn. 49
1. Claim 1 49

(a) "with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:".....59

(i) "a device identifier;".....59

(ii) "at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and".....59

(iii) "at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;".....59

(b) "wherein determining the association in part (a) is done by using the stored association-detection information to determine that the two or more Internet-accessing electronic devices have separately accessed the Internet through a router of the LAN during a predetermined period of time via a common IP address;" 88

(c) "wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and".....92

(d) "with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices." 94

2. Claim 2: "The method of claim 1 wherein the first device comprises a mobile device that is connected to the LAN only intermittently." 108

3. Claim 8: "The method of claim 1 wherein the device identifier of at least one of the first device and the second device is a cookie readable by the computer system." 110

4. Claim 9: "The method of claim 8 further comprising, using the computer system, automatically storing, in a memory in the first device, the cookie." 110

5. Claim 10: "The method of claim 1 wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device." 113

6. Independent Claim 13 114

7. Claims 14 and 19 116

8. Independent Claim 22 117

C. Ground 2: Claims 3-4, 15-16 Are Obvious Over Ground 1 Prior Art in Further View of Xu 120

1. Claim 3: "The method of claim 2 wherein the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN." 120

2. Claim 4: "The method of claim 3 wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN." 126

3. Claims 15-16 132

D. Ground 3: Claims 6-7, 17-18 Are Obvious Over Ground 1 Prior Art in Further View of Gerace. 133

1. Claim 6: "The method of claim 1 wherein the automatic action comprises selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device."..... 133

2. Claim 7: "The method of claim 6 wherein the automatic action comprises causing the selected advertisement to be directed to the second device."..... 133

3. Claims 17-18 140

E. Ground 4: Claims 11-12, 20-21, 23 Are Obvious Over Ground 1 Prior Art with Xu and Gerace..... 141

1. Claim 11: "The method of claim 1 wherein"..... 141

(a) "(i) the first device comprises a mobile device that is connected to the LAN only intermittently,"..... 141

(b) "(ii) the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN,..... 141

(c) "(iii) wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN, and" 141

(d) "(iv) the automatic action comprises (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device." 142

2. Claim 12: "The method of claim 11 wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device." 142

3. Claims 20-21 and 23 142

VI. ENABLEMENT OF THE PRIOR ART 145

VII. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS 147

VIII. CONCLUSION 149

I, Christopher M. Schmandt, declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

A. Qualifications and Experience

1. I have recently retired from my position as a Principal Research Scientist at the Media Laboratory at Massachusetts Institute of Technology ("M.I.T"), after 40 years of employment by M.I.T. In that role, I also served as faculty for the M.I.T. Media Arts and Sciences academic program. I have more than 40 years of experience in the field of Media Technology, and was a founder of the M.I.T. Media Laboratory.

2. I received my Bachelor of Science degree in Electrical Engineering and Computer Science from M.I.T. in 1978, and my Master of Science degree in Visual Studies (Computer Graphics), also from M.I.T. I had been employed at M.I.T. since 1980, initially at the Architecture Machine Group, which was an early computer graphics research lab. In 1985, I helped found the Media Laboratory and continued to work there until my retirement. I ran a research group titled "Living Mobile." My research spanned distributed communication and collaborative systems, with an emphasis on multi-media and user interfaces; I have more than 70 published conference and journal papers and one book in these fields.

3. In my faculty position, I taught courses and directly supervised student

research and theses at the Bachelors, Masters, and Ph.D. level. I oversaw the Masters and Ph.D. thesis programs for the entire Media Arts and Sciences academic program. Based on the above experience and qualifications, I have a solid understanding of the knowledge and perspective of a person of ordinary skill in this technical field since at least 1980.

4. During my career at the MIT Media Laboratory I worked extensively with issues in management, delivery, and interaction with multimedia content through user context modeling. This work emphasized asynchronous or synchronous delivery of current news, either as audio, video, or text. In this context I have worked with a wide variety of network technologies and protocols, connecting a broad assortment of devices. Because much of my work also involved client-server computing with segments in home networks or mobile networks, I am well versed in NAT technologies and IP port management.

5. In this context I developed network protocols, servers, client software, and user interfaces and applications for networked real time data. Related to this work, for some years in the 1990s I was a member of an IETF (Internet Engineering Task Force, later IAB, Internet Activities Board) working group exploring network requirements for real time delivery of multimedia content, both point to point as well as multicast.

6. In the late 1980s I was involved in the installation and management of a broadband IP network using cable television hardware. In addition I have consulted with major cable television suppliers, some of whom were sponsors of work at the Media Laboratory of which I was a part. As such I am familiar with data-over-cable technologies such as Docsis, cable modem protocols, and media gateway protocols on such mixed use video plus IP networks, with delivery media spanning copper, fiber, and hybrid layered network architectures.

7. My Curriculum Vitae is attached as **Exhibit A**.

8. I have been retained by counsel for Petitioner to provide my expert opinion in connection with the above-captioned proceeding as set forth herein.

B. Materials Considered

9. The analysis that I provide in this Declaration is based on my education, research, and experience, as well as the documents I have considered. In forming my opinions, I have read and considered U.S. Patent No. 10,715,878 B2 ("'878 patent") **[EX1001]** and its prosecution history. I have cited to the following documents in my analysis below:

Exhibit No.	Description of Document
1001	U.S. Patent No. 10,715,878 B2 to Roy Shkedi (filed December 20, 2018, issued July 14, 2020) ("'878" or "'878 patent")

Exhibit No.	Description of Document
1003	U.S. Patent Application Publication No. 2008/0113674 A1 to Mohammad Faisal Baig (filed October 31, 2007, published May 15, 2008) ("Baig")
1004	U.S. Provisional Application No. 60/858,204 to Mohammad Baig (filed Nov. 10, 2006) ("Baig Provisional")
1005	Redline document showing differences between Baig (EX1003) and Baig Provisional (EX1004)
1006	U.S. Patent Application Publication No. 2004/0128547 A1 to Robert Laidlaw et al. (filed December 31, 2002, published July 1, 2004) ("Laidlaw")
1007	U.S. Patent No. 6,427,170 B1 to Aravind Sitaraman et al. (filed December 8, 1998, issued July 30, 2002) ("Sitaraman")
1008	Excerpts from Harley Hahn, *The Internet Complete Reference* (2d ed. 1996) ("Hahn")
1009	U.S. Patent No. 7,730,030 B1 to Yongyong Xu (filed August 15, 2004, issued June 1, 2020) ("Xu")
1010	U.S. Patent Application Publication No. 2006/0282328 A1 to Thomas Gerace et al. (filed June 12, 2006, published December 14, 2006) ("Gerace")
1011	Excerpts from Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) ("Zeff")
1012	U.S. Patent Application Publication No. 2005/0175181 A1 to Magnus H. Bergs et al. (filed September 7, 2004, published August 11, 2005) ("Bergs")
1013	Excerpts from *Microsoft Computer Dictionary* (5th ed. 2002)

II. PERSON OF ORDINARY SKILL IN THE ART

10. I understand that, under the patent laws in effect before the America Invents Act ("AIA") of 2011, an assessment of claims of a patent filed before the AIA took effect should be undertaken from the perspective of a person of ordinary skill in the art as of the earliest claimed priority date (i.e., the "time the invention was made"). I have assumed that date to be April 17, 2007, the filing date of the earliest application to which the '878 patent claims priority (Appl. Ser. No. 11/736,544).

11. I have also been advised that to determine the appropriate level of a person having ordinary skill in the art, the following factors may be considered: (1) the types of problems encountered by those working in the field and prior art solutions thereto; (2) the sophistication of the technology in question, and the rapidity with which innovations occur in the field; (3) the educational level of active workers in the field; and (4) the educational level of the inventor.

12. The '878 patent states "[t]he field of the present invention relates to online access and targeted delivery of advertisements." ('878, 1:23-24.) In my opinion, a person of ordinary skill in the art would have possessed a bachelor's degree in electrical engineering or computer science, and two years of work experience in the field of network-based computer systems, such as systems for

sending and receiving information over local networks and wide area networks (such as the Internet or World Wide Web). A person could also have qualified as a person of ordinary skill in the art with some combination of (1) more formal education (such as a master's of science degree) and less technical experience, or (2) less formal education and more technical or professional experience.

13. My opinions regarding the level of ordinary skill in the art are based on, among other things, my over 40 years of experience in the field of computer science, my understanding of the basic qualifications that would be relevant to an engineer or scientist tasked with investigating methods and systems in the relevant area, and my familiarity with the backgrounds of colleagues, co-workers, and employees, both past and present.

14. Although my qualifications and experience exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the '878 patent have been based on the perspective of a person of ordinary skill in the art as of April 2007.

III. STATEMENT OF LEGAL PRINCIPLES

A. Claim Construction

15. I understand that a purpose of claim construction is to determine what a person of ordinary skill in the art would have understood the claim terms to mean.

Claim terms are generally given their ordinary and customary meaning, which is the meaning that the term would have to a person of ordinary skill in the art in question as of the effective filing date.

16. I understand that the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification. I understand that the patent specification, under the legal principles, has been described as the single best guide to the meaning of a claim term, and is thus highly relevant to the interpretation of claim terms. And I understand for terms that do not have a customary meaning within the art, the specification usually supplies the best context of understanding the meaning of those terms.

17. I further understand that other claims of the patent in question, both asserted and unasserted, can be valuable sources of information as to the meaning of a claim term. Because the claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often illuminate the meaning of the same term in other claims. Differences among claims can also be a useful guide in understanding the meaning of particular claim terms.

18. I understand that the prosecution history can further inform the meaning of the claim language by demonstrating how the inventors understood the invention

and whether the inventors limited the invention in the course of prosecution, making the claim scope narrower than it otherwise would be. Extrinsic evidence, such as dictionaries, may also be consulted in construing the claim terms.

19. I understand that, in *Inter Partes* Review (IPR) proceedings, a claim of a patent shall be construed using the same claim construction standard that would be used to construe the claim in a civil action filed in a U.S. district court (which I understand is called the "*Phillips*" claim construction standard), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent.

20. I have been instructed by counsel to apply the "*Phillips*" claim construction standard for purposes of interpreting the claims in this proceeding, to the extent they require an explicit construction. The description of the legal principles set forth above thus provides my understanding of the "*Phillips*" standard as provided to me by counsel.

B. Obviousness

21. I understand that a patent claim is obvious if, as of the effective filing date, it would have been obvious to a person having ordinary skill in the field of the technology (the "art") to which the claimed subject matter belongs.

22. I understand that the following factors should be considered in analyzing obviousness: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; and (3) the level of ordinary skill in the pertinent art. I also understand that certain other facts known as "secondary considerations" such as commercial success, unexplained results, long felt but unsolved need, industry acclaim, simultaneous invention, copying by others, skepticism by experts in the field, and failure of others may be utilized as indicia of nonobviousness. I understand, however, that secondary considerations should be connected, or have a "nexus," with the invention claimed in the patent at issue.

23. I understand that a reference qualifies as prior art for obviousness purposes when it is analogous to the claimed invention. The test for determining what art is analogous is: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.

24. I understand that a person of ordinary skill in the art is assumed to have knowledge of all prior art. I understand that one skilled in the art can combine various prior art references based on the teachings of those prior art references, the general knowledge present in the art, or common sense. I understand that a

motivation to combine references may be implicit in the prior art, and there is no requirement that there be an actual or explicit teaching to combine two references. Thus, one may take into account the inferences and creative steps that a person of ordinary skill in the art would employ to combine the known elements in the prior art in the manner claimed by the patent at issue. I understand that one should avoid "hindsight bias" and ex post reasoning in performing an obviousness analysis. But this does not mean that a person of ordinary skill in the art for purposes of the obviousness inquiry does not have recourse to common sense.

25. I understand that when determining whether a patent claim is obvious in light of the prior art, neither the particular motivation for the patent nor the stated purpose of the patentee is controlling. The primary inquiry has to do with the objective reach of the claims, and that if those claims extend to something that is obvious, then the entire patent claim is invalid.

26. I understand one way that a patent can be found obvious is if there existed at the time of the invention a known problem for which there was an obvious solution encompassed by the patent's claims. I understand that a motivation to combine various prior art references to solve a particular problem may come from a variety of sources, including market demand or scientific literature. I understand that a need or problem known in the field at the time of the invention can also provide

a reason to combine prior art references and render a patent claim invalid for obviousness. I understand that familiar items may have obvious uses beyond their primary purpose, and that a person of ordinary skill in the art will be able to fit the teachings of multiple prior art references together like the pieces of a puzzle. I understand that a person of ordinary skill is also a person of at least ordinary creativity. I understand when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions, a person of ordinary skill has good reason to pursue the known options within his or her technical grasp. If this finite number of predictable solutions leads to the anticipated success, I understand that the invention is likely the product of ordinary skill and common sense, and not of any sort of innovation. I understand that the fact that a combination was obvious to try might also show that it was obvious, and hence invalid, under the patent laws. I understand that if a patent claims a combination of familiar elements according to known methods, the combination is likely to be obvious when it does not more than yield predictable results. Thus, if a person of ordinary skill in the art can implement a predictable variation, an invention is likely obvious. I understand that combining embodiments disclosed near each other in a prior art reference would not ordinarily require a leap of inventiveness.

27. I understand that obviousness may be shown by demonstrating that it

would have been obvious to modify what is taught in a single piece of prior art to create the patented invention. Obviousness may also be shown by demonstrating that it would have been obvious to combine the teachings of more than one item of prior art. I understand that a claimed invention may be obvious if some teaching, suggestion, or motivation exists that would have led a person of ordinary skill in the art to combine the invalidating references. I also understand that this suggestion or motivation may come from the knowledge of a person having ordinary skill in the art, or from sources such as explicit statements in the prior art. I understand that when there is a design need or market pressure, and there are a finite number of predictable solutions, a person of ordinary skill may be motivated to apply common sense and his skill to combine the known options in order to solve the problem.

28. I understand the following are examples of approaches and rationales that may be considered in determining whether a piece of prior art could have been combined with other prior art or with other information within the knowledge of a person having ordinary skill in the art:

(1) Some teaching, motivation, or suggestion in the prior art that would have led a person of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention;

(2) Known work in one field of endeavor may prompt variations of it for use in the same field or a different field based on design incentives or other market forces if the variations would have been predictable to a person of ordinary skill in the art;

(3) Combining prior art elements according to known methods to yield predictable results;

(4) Applying a known technique to a known device, method, or product ready for improvement to yield predictable results;

(5) Applying a technique or approach that would have been "obvious to try" (choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success);

(6) Simple substitution of one known element for another to obtain predictable results; or

(7) Use of a known technique to improve similar products, devices, or methods in the same way.

29. I understand that, when determining whether a claimed combination is obvious, the correct analysis is not whether one of ordinary skill in the art, writing on a blank slate, would have chosen the particular combination of elements described in the claim. Instead, I understand the correct analysis considers whether

one of ordinary skill, facing the wide range of needs created by developments in the field of endeavor, would have seen a benefit to selecting the combination claimed.

30. I understand that the test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference. The test for obviousness, in other words, is not whether the references could be physically combined but whether the claimed inventions are rendered obvious by the teachings of the prior art as a whole.

IV. THE '878 PATENT

A. Overview of the Specification

31. The '878 patent states that "[t]he field of the present invention relates to online access and targeted delivery of advertisements." ('878, 1:23-24.) 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 determine an action to perform with respect to a second device. (*E.g.*, '878, 8:13-25.) In an exemplary embodiment, the patent describes applying its techniques to target advertisements to a user's television based on the online activities of the user's computer. (*E.g.*, '878, 8:52-9:8 ("[O]ne person might access the online site while the corresponding television ad might be delivered to another person in the household, office, business, or other site or establishment. The delivery end-point

may be one television set….”).) Figure 1 of the patent depicts a basic layout of a system for targeting advertisements in accordance this exemplary context:

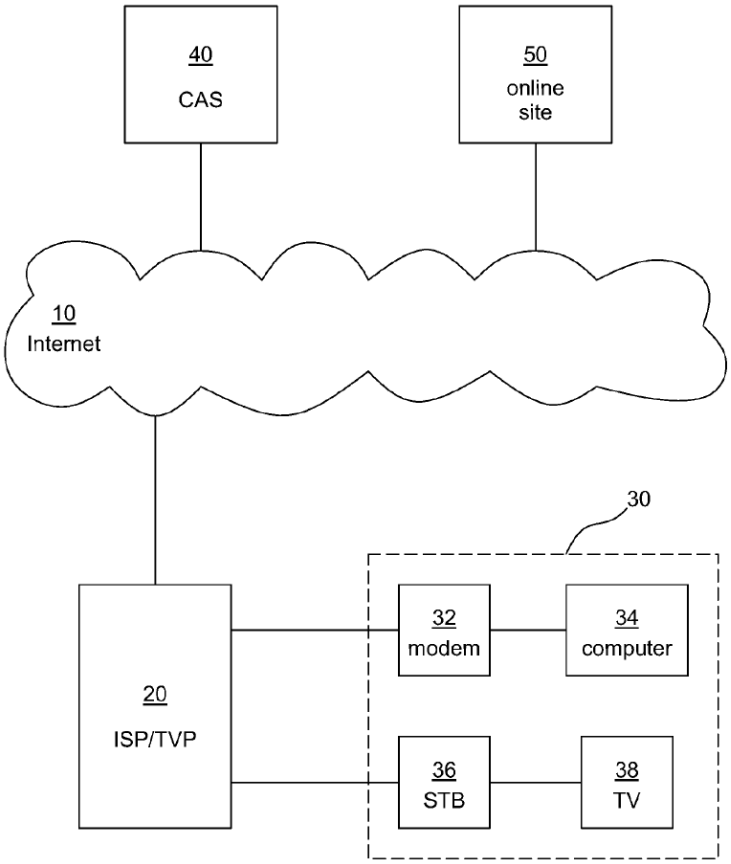


FIG. 1

(’878, Fig. 1.) As shown, the system 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**. (’878, 9:36-40, 2:49-67.) Common service provider **20** can offer both Internet access via the online access device **32** as well as television service

through STB **36**. ('878, 9:45-56.) Common service provider **20** also provides to Central Ad Server ("CAS") **40** the IP addresses of the user's devices, such as computer **34** and STB **36**. And online site **50** reports to CAS **40** computer **34**'s online activities at the site. ('878, 11:8-15.) Thus, by determining the computer **34** and STB **36** are related to each other, CAS **40** can provide targeted advertisements to STB/TV based on the computer's online activities. ('878, 11:4-62.)

32. In order to determine that, for example, computer **34** and STB **36** are related to each other, the '878 patent explains that IP address information associated with those devices can be used. ('878, 9:57-10:18, 10:49-11:3.) 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 of those devices. ('878, 10:4-5 ("[T]he modem IP address is the only address 'seen' by the remote network."), 10:40-44, 13:4-46 ("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)." ('878, 14:1-6.) I discuss

additional aspects of the ’878 patent as needed in the analysis below.

B. The Challenged Claims

33. This Declaration addresses claims 1-4 and 6-23 of the ’878 patent. Independent claim 1 recites:

> 1. A method for identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the method comprising:
>
> (a) with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:
>
> (i) a device identifier;
>
> (ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and
>
> (iii) at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;
>
> (b) wherein determining the association in part (a) is done by using the stored association-detection information to determine that the two or more Internet-accessing electronic devices have separately accessed the

Internet through a router of the LAN during a predetermined period of time via a common IP address;

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

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

('878, 24:25-62 (Claim 1).)

34. I address the claims further in my detailed analysis in **Part V** below.

V. APPLICATION OF THE PRIOR ART TO CHALLENGED CLAIMS

35. I have reviewed and analyzed the prior art references and materials listed in **Part I.B** above. In my opinion the claims of the '878 patent would have been obvious to a person of ordinary skill in the art based on the following combinations of the prior art.

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

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

36. I am informed by counsel that each of the references cited in the grounds above qualifies as prior art to the challenged claims because each reference was filed and/or published before the '878 patent priority date (April 17, 2007).

A. Brief Summary of Prior Art

1. Prior Art Common to All Grounds

(a) Baig and Baig Provisional (EX1003/1004)

37. **Baig**, U.S. Patent Publication No. 2008/0113674 A1 to Mohammad Baig is entitled "Vicinity-Based Community for Wireless Users" (EX1003). Baig is a published patent application filed on October 31, 2007, after the filing date of the earliest application to which the '878 patent claims priority. But Baig claims priority to U.S. Provisional Application No. 60/858,204 (EX1004), filed on November 10, 2006. I am informed by counsel that Baig properly qualifies as prior art to the '878 patent, provided that Baig is entitled to the filing date of its provisional application. In my opinion, Baig is so entitled, which I will discuss below.

38. Baig incorporates-by-reference the Baig Provisional. (Baig, ¶0001.) For consistency and simplicity, I will refer to the published Baig patent application

(**EX1003**) as "**Baig**," and the provisional application (**EX1004**) as "**Baig Provisional**." As explained below, there are no material differences between Baig and the Baig Provisional, and the disclosures upon which I rely from Baig were contained (without material differences) in the Baig Provisional. I will therefore include, for each citation to Baig, a parallel citation to the Baig Provisional where the same subject matter can be found.

39. Baig purports to take advantage of WiFi networking and WiFi "hotspots" that were common fixtures in the mid 2000s in airports, coffee shops, and other public places. Baig discloses a technique for creating "vicinity-based" communities of users who are connected to the same WiFi hotspot. As Baig explains:

> A vicinity-based community service is a service provided by the VCSP which discovers (i.e., identifies) and connects wireless users within physical vicinity (i.e., proximity) of each other at a WiFi hotspot. Once a "vicinity-based community" at a physical location (i.e., a hotspot) is created, the users can potentially interact physically or non-physically with each other.

(Baig, ¶0038; Baig Provisional, 0010.) Figure 1 shows a block diagram showing the primary components of the system:

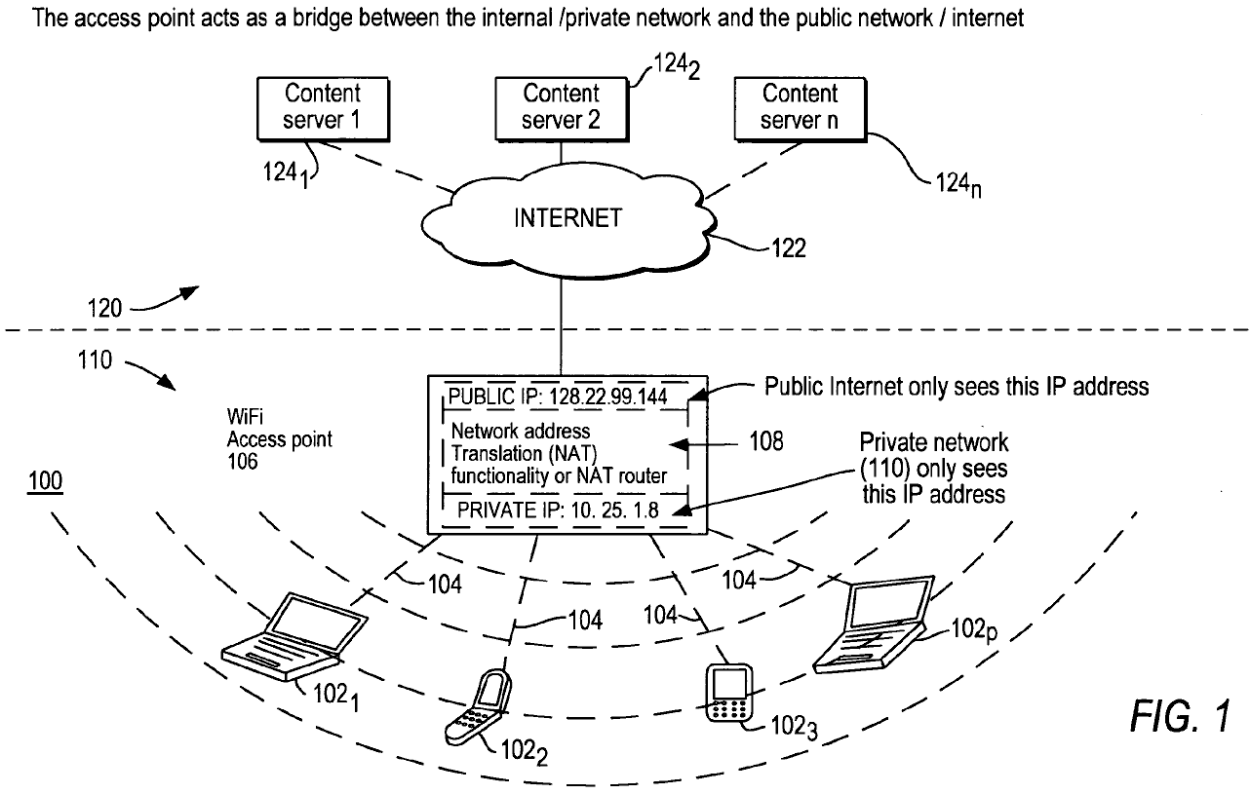


FIG. 1

(Baig & Baig Provisional, Fig. 1.)[1] Figure 1 above is "a block diagram is shown illustrating how one or more mobile devices **102** at a public WiFi hotspot **110** interact with the public network **120**." (Baig, ¶0042; Baig Provisional, 0010.) The

[1] The figures from Baig that I cite in my Declaration are from the published Baig application (EX1003), and are more refined (formal) drawings based on the figures in the Baig Provisional (EX1004). There are no material differences in subject matter between the figures that I cite in Baig and the Baig Provisional.

portion of Figure 1 below the dashed line shows a WiFi hotspot **110** that includes an access point **106** wirelessly connected to several mobile devices (**102_1** through **102_p**). (Baig, ¶0043; Baig Provisional, 00011.) "Thus, the mobile devices **102** at the hotspot **110** form a local network **104** with the access point **106**." (*Id.*) Access point **106** in turn acts as a bridge to facilitate communications over the Internet **122** between the mobile devices **102** and one or more content servers (**124_1** through **124_n**), shown above the dashed line in Figure 1. (Baig, ¶¶0046-0047, Baig Provisional, 0012.)[2] Access point **106** allocates "local" IP addresses to each mobile device **102** to which it is connected, but in communications over the Internet, replaces that address with the IP address of the access point **106**. (Baig, ¶¶0049-0050; Baig Provisional, 0012.) Access point **106** uses a technique known as network address translation (NAT) to perform the IP address replacement. (Baig, ¶¶0043 ("The access point **106** includes network address translation device **108**, and provides network address translations (NAT)."), 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."); Baig Provisional, 0011-0012.)

[2] The content server in Baig is also shown in Figure 2 and referred to throughout Baig as "content server **224**."

40. The content servers **124** shown above the dashed line in Figure 1 are a key aspect of the system, in that they are responsible for actually creating a vicinity-based group of users. The servers run programs that, among other things, "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**." (Baig, ¶0052; Baig Provisional, 0012-0013.) The content server can readily identify mobile devices connected to the same hotspot because those devices will be communicating using the common IP address of the access point. (Baig, ¶¶0038 ("The VSCP identifies a group of users at a wireless hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."), 0052 ("The server **224**… identif[ies] 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**."); Baig Provisional, 0010, 0012-0013.)

41. Once a vicinity-based group is created, members can access a website that allows them to play video games, participate in chat rooms and message boards, share files such as music, and engage in other activities. (Baig, ¶0059; Baig Provisional, 0014.) The website can also display a list of other users who are connected to the same hotspot. (Baig & Baig Provisional, Figs. 6-7 (list 606); Baig, ¶¶0076, 0080; Baig Provisional, 0018-0019.) I will provide further information

about Baig in my discussion of the claims below.

Priority Date of Baig

42. As mentioned above, Baig was filed on October 31, 2007, claiming priority to U.S. Provisional Application No. 60/858,204 (EX1004), filed on November 10, 2006. I understand and am informed by counsel that for Baig to be considered prior art as of the filing date of the Baig Provisional (rather than the filing date of the published non-provisional application), (1) the portions of Baig cited for invalidity must be supported by disclosure in the Baig Provisional, and (2) at least one claim in the Baig published application must be supported by disclosure in the Baig Provisional, *i.e.*, the Baig Provisional must disclose the subject matter of the claim and enable a person of ordinary skill in the art to make and use the claim.[3] The Baig Provisional satisfies both requirements.

43. The first requirement is easily met because the disclosures in Baig that I cite in my analysis below were also contained in the Baig Provisional. Attached as **EX1005** is a redline document comparing the subject matter of Baig against the earlier-filed Baig Provisional. As shown, there are few differences, and with respect

[3] (*See Manual of Patent Examining Procedure (MPEP)*, § 2136 (available at <https://www.uspto.gov/web/offices/pac/mpep/s2136.html>.)

to the portions that I cite in my analysis below, there are no material differences. For convenience, therefore, in each place where I cite to Baig (EX1003) in my analysis, I will include a parallel citation to the Baig Provisional (EX1004) to identify where the same corresponding disclosure in the Baig Provisional appears. I also found no material differences in the figures from Baig that I cite in my analysis below.

44. With respect to the second requirement, the Baig Provisional provides sufficient description and support for several of the claims in the published Baig application. I understand and am informed by counsel that, under the patent laws, claims that were originally-filed with the Baig Provisional can be used to show that the provisional application provides adequate support for the claims of the published Baig application. In this case, seventeen (17) claims of the published Baig application (*i.e.*, claims 1-3, 8-16, 18-22) are word-for-word identical to originally-filed claims of the Baig Provisional, and many other claims present only minor differences. (EX1005, 0026-0028.) This confirms that the Baig Provisional discloses the subject matter of these claims, and as I explain below, the disclosures in the Baig Provisional would have been sufficient to enable an ordinarily skilled artisan to make and use the subject matter of these claims. I have also provided a table below showing that the subject matter of at least claim 1 of the published application is supported by disclosures in the Baig Provisional beyond the claims:

Claim 1 from Published Baig Application	Exemplary Disclosures from Baig Provisional
1. A method for providing vicinity-based community services at a wireless access location by a public network service provider, comprising the steps of:	"The present invention provides a vicinity-based community for wireless users at a hotspot as described herein. In particular, the present invention includes a method and apparatus for providing vicinity-based community services at a wireless access location, such as a hotspot." (Baig Provisional, 007.) "In particular, the present invention is directed to a method and apparatus for creating vicinity-based communities over the Internet by a vicinity-based community service provider (VCSP) to wireless mobile devices of end-users who have accessed the VCSP via a wireless access point at a wireless hotspot." (Baig Provisional, 0010.) *Baig also makes clear that the claimed "public network" incudes the Internet:* "In particular, a communications network 100 includes a public WiFi hotspot 110 communicably coupled to a public network 120 via an access point 106. The public network 120 includes, for example, content servers 124_1 through 124_p (collectively content servers 124) that store and/or host information (e.g., multimedia information and data), illustratively, from websites, and are communicably linked together to form the public internet 122." (Baig Provisional, 0010-0011.)
receiving over a public network, at least one request for vicinity-based community services from at	"The method includes the steps of receiving over a public network at least one request for vicinity-based community services from at least one end-user accessing the wireless access point, grouping end-users accessing common wireless access

Claim 1 from Published Baig Application	Exemplary Disclosures from Baig Provisional
least one end-user accessing said wireless access point;	points, and providing the vicinity-based community services in real time to end-users accessing the public network service provider from the wireless access point. The apparatus includes means for carrying out the method described above." (Baig Provisional, 007.) "Referring now to FIG. 3, the flow diagram provides an illustrative embodiment of a method 300 for forming WiFi hotspot based mesh networks. The method 300 starts at step 301, where <u>at least one user located at each of one or more hotspots have established wireless connectivity with the Internet</u>. That is, <u>the users at each hotspot are provided with Internet connectivity via an associated access point 106 as discussed above</u>. At step 302, <u>the at least one server 224 of the VCSP 202 receives a **login request** from a user that is connected to a particular WiFi access point</u> (hotspot)" (Baig Provisional, 0013.)
grouping end-users accessing common wireless access points; and	"The method includes the steps of receiving over a public network at least one request for vicinity-based community services from at least one end-user accessing the wireless access point, <u>grouping end-users accessing common wireless access points</u>, and providing the vicinity-based community services in real time to end-users accessing the public network service provider from the wireless access point. The apparatus includes means for carrying out the method described above." (Baig Provisional, 007.)

Claim 1 from Published Baig Application	Exemplary Disclosures from Baig Provisional
	"The VSCP identifies a group of users at a wireless hotspot based on their common public IP address and interconnect [sic] them, thereby creating a vicinity-based user group." (Baig Provisional, 0010.) "The server 224 includes at least one processor, memory and support circuitry for running programs that, for example, 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." (Baig Provisional, 0012-0013.) "At step 312, the server 224 forms a vicinity-based user group at each hotspot 110. A vicinity-based user group allows the VCSP 202 to provide services to the member users of the group. In particular, when a user at a hotspot logs into the website of the VCSP 202, the user automatically becomes part of the vicinity-based user group." (Baig Provisional, 0014.)
providing said vicinity-based community services in real time to end-users accessing said public network service provider from said wireless access point.	"The method includes the steps of receiving over a public network at least one request for vicinity-based community services from at least one end-user accessing the wireless access point, grouping end-users accessing common wireless access points, and providing the vicinity-based community services in real time to end-users accessing the public network service provider from the wireless access point. The apparatus includes means for carrying out the method described above." (Baig Provisional, 007.)

Claim 1 from Published Baig Application	Exemplary Disclosures from Baig Provisional
	"At step 312, the server 224 forms a vicinity-based user group at each hotspot 110. A vicinity-based user group allows the VCSP 202 to provide services to the member users of the group. In particular, when a user at a hotspot logs into the website of the VCSP 202, the user automatically becomes part of the vicinity-based user group. The user can then access various web pages from the VCSP website to participate or receive particular service offered by the VCSP 202. The services include receiving particular advertisements, a goods and services exchange program, sharing of files (e.g., music) as permissible under law, a chat room, a message board for blogs and the like, among other services, as discussed below with respect to FIGS. 4-23. Thus, users accessing a hotspot and who have logged into the website of the VCSP 202 can receive and participate in the services offered by the VCSP 202, as well as communicate with each other (e.g., chat room)." (Baig Provisional, 0014.) *Baig confirms that several of these services are, in fact, provided "in real-time." For example:* "In another embodiment, the vicinity-based community services include a lost and found service. End-users at a particular wireless access point can post, in real-time, lost or found items at the location of the wireless access point." (Baig, Provisional, 007.) "In another embodiment, real-time advertising is provided at one or more physical locations (e.g., billboard at Times Square, NY) based on real-time

Claim 1 from Published Baig Application	Exemplary Disclosures from Baig Provisional
	bidding between advertising." (Baig Provisional, 0024.) *An ordinarily skilled artisan would also have understood that Baig's chat room feature to be provided in real time as it provides real-time (instant) messaging between users:* "The chat-room service includes instant messaging, checking profiles, file transfers, among other features." (Baig Provisional, 0027; *see also* Baig Provisional, Fig. 7 ("Moving the mouse over any name will reveal a one liner profile. Users should also be able to send instant messages and share files etc.").)

45. In my opinion, therefore, the Baig Provisional provides more than sufficient support for at least claim 1 of the published Baig application. Not only does published claim 1 identically appear in the Baig Provisional, but as shown in the table above, the Baig Provisional provides other disclosures that sufficiently support each limitation of the claim. (The table above shows exemplary support for the claim limitations, but I may provide additional detail should it be required to address arguments by Patent Owner.) Additionally, the disclosures in the Baig Provisional would have provided sufficient detail to enable an ordinarily skilled artisan to implement the subject matter of each of the published claims, without undue experimentation. The underlying technology is not complex, and the claimed

techniques involved nothing beyond conventional technologies widely available by April 2007. For example, WiFi access points that could facilitate communications between mobile devices and servers connected to the Internet were well-known and commercially available. As I explain in detail in the discussion of claim 1(a) below for **Ground 1**, the way in which the access point in the Baig Provisional uses a common IP addresses for each connected mobile device was a well-known feature of conventional network address translation (NAT) technologies. And the features of the content server in the Baig Provisional, including grouping users and providing web-based services to them, could have been implemented using conventional programming techniques well-known to persons of ordinary skill in the art. In my opinion, therefore, the disclosures in the Baig Provisional show that the inventor was in possession of at least published claim 1 as of November 10, 2006 (the filing date of the Baig Provisional), and those disclosures would have enabled a person of ordinary skill in the art to have made and used the subject matter of each of the published claims without undue experimentation.

(b) Laidlaw (EX1006)

46. **Laidlaw**, U.S. Patent Application Publication No. 2004/0128547, is entitled "Method and System for Modular Authentication and Session Management." I am informed that Laidlaw qualifies as prior art because it was filed

and published before the earliest priority date of the ’878 patent.

47. My Declaration relies on Laidlaw for limitations in the independent claims reciting “**electronically stored association-detection information**” for two or more Internet-accessing electronic devices, which includes at least three pieces of information for each device (*e.g.* “**device identifier**,” “**IP address**,” “**timestamp**”), recited in the independent claims.

48. Laidlaw discloses a system for managing “sessions” in a network-based computer system. In computer science and in the context here, the term “session” generally refers to a period of time when two devices maintain a connection over a network. (*See, e.g.*, *Microsoft Computer Dictionary* (5th ed. 2002), p.008 (“**session** *n*…. **2**. In communications, the time during which two computers maintain a connection.”) (bold and italics in original).) A “session” generally commences when a first device logs into or accesses a second device (for example using a username and password), and persists until the first device logs out or otherwise ceases its connection with the second device. (Laidlaw, ¶¶0003-0005.)

49. One of the key concepts disclosed in Laidlaw is a session “token,” included a request for each, that identifies the requesting device. (Laidlaw, ¶0004.) In the context of the Internet and Web, Laidlaw explains that the session token takes the form of a cookie. As explained in Laidlaw:

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

(Laidlaw, ¶0006.)

50. The "cookie" described in Laidlaw refers to a well-known and industry standard technology developed in the 1990s by Netscape Communications, the company that published the Netscape Navigator web browser that was popular in the early days of the Web. A cookie is a file stored on the user computer by the web browser that can be used by a web site to identify the user when it visits the web site. (*See* Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0026 ("A cookie is a text that can be written to a text file on the user's hard drive when visiting a Web site. In most cases, that text will be a unique string, allowing the person to be identified.").) Laidlaw explains that cookies were developed to address a limitation of the Hypertext Transport Protocol (HTTP), the protocol used to transport requests and responses between web browsers and web servers. HTTP is often referred to as a "stateless" protocol because when a user (via a web browser) transmits an HTTP request to a web server, the server generally has no knowledge

of the user's previous requests. (Laidlaw, ¶0006 ("When a user requests a Uniform Resource Locator ('URL') from a web browser, there is no standard method for the receiving HTTP server to recognize the user identity or the fact that earlier requests originated from the same client.").)

51. But if a stored "cookie" exists, the information in the "cookie" can be transmitted by the browser to the server with the HTTP request, thus allowing the responding server to know the identity of the requesting device and user. (Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0026 ("For example, a site may assign you a cookie with the text string '123.' Every time you access a page on the site, the server can request the cookie it placed and recognize that '123' is back again and track where '123' goes on the site.").) Cookies were and remain in widespread use today on hundreds of millions of websites to allow delivery of customized information to visitors and for tracking the activity of users on a website.

52. Laidlaw explains that session-related information is stored in a "session table." (Laidlaw, ¶¶0016.) And one of the pieces of information in the session table of Laidlaw is the aforementioned session token in the form of a cookie:

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

the token is obtained from a session table that is keyed by session token. (Laidlaw, ¶0016.) The process above attempts to determine, in response to receiving a cookie from the requesting device, whether that session token in the cookie is stored in the session table. Laidlaw explains that the session table, in fact, is "keyed by session token," which means that the session token is the field used to locate the session table for its respective device, thus indicating that the session token is in fact stored in the table. (Laidlaw, ¶0040 ("A 'key field' partitions the database according to the high-level class of objects defined by the key field.").) It therefore would have been obvious that the session token in the cookie is in fact stored in the session table.

53. Laidlaw also explains that the session table includes "information regarding the host that the user logged in from (e.g., the IP address)." (Laidlaw, ¶0022.) Under the proposed combination of Baig with Laidlaw, as explained below, the session table would have stored the IP address of the access point **106** used to log into the content server. Laidlaw also discloses that the session table includes a timestamp, *i.e.*, "information regarding the last time the session was accessed." (Laidlaw, ¶0017.) Under the proposed combination with Baig, as discussed below, the session table would also have included a timestamp indicating when each mobile device accessed the content server through access point **106**.

54. I will provide more detail about Laidlaw below.

(c) Sitaraman (EX1007)

55. **Sitaraman**, U.S. Patent No. 6,427,170 B1, is entitled "Integrated IP Address Management." I am informed that Sitaraman qualifies as prior art because it was filed and issued before the earliest priority date of the '878 patent.

56. My Declaration relies on Sitaraman primarily for claim 1(a)(ii), which requires that the "**IP address**" in the stored association-detection information of claim 1(a) be a "**dynamically assigned**" IP address. Baig does not expressly disclose the use of a dynamic IP address for access point **106**, but this would have been obvious based on the general knowledge of an ordinarily skilled artisan, as confirmed by Sitaraman.

57. Sitaraman discloses a technique for managing dynamic IP address allocation. (Sitaraman, Abstract.) Sitaraman acknowledges that with the exponential growth of the Internet, companies and users were faced with an increasing shortage of IP addresses, since there is a finite number of static addresses. (Sitaraman, 3:21-29.) One well-known approach to address this problem is "dynamic" IP addresses, in which a device is assigned an IP address that is dynamically assigned by a server known as a Dynamic Host Configuration Protocol (DHCP) server. DHCP refers to an industry-standard technique in which a device on a network (such as a client) can ask a DHCP server "to provide it with an IP

address and configuration parameters. A DHCP server on the network that is authorized to configure this client will offer an IP address by sending a reply to the client." (Sitaraman, 3:34-40.) Sitaraman explains that DHCP servers are used, for example, by Internet Service Providers (ISPs) who typically maintain a "pool" of available IP addresses that can be dynamically assigned upon request. (Sitaraman, 3:64-4:1, 6:63-66 ("The dynamic IP address server **8** maintains a pool **22** of IP addresses and leases the IP addresses of the pool **22**. In accordance with a preferred embodiment, the dynamic IP address server **8** is a DHCP server.").)

58. If the client accepts the offered IP address, "the chosen DHCP server sends an acknowledgement with the offered IP address having an associated 'lease' time," which can be renewed by the client upon request. (Sitaraman, 3:42-47.) "Once the lease expires, the IP address can be 'recycled' and given to another machine." (Sitaraman, 3:49-51.)

59. As I will explain below for claim 1(a), it would have been obvious to adapt the system of Baig to include a "**dynamically assigned**" IP address for access points, which could be stored. I will provide more details about Sitaraman below.

(d) Hahn (EX1008)

60. **Hahn**, a book entitled *The Internet Complete Reference* (2d ed. 1996), describes basic and well-known features of conventional web technologies. My

Declaration relies on Hahn in combination with other prior art for claim 1(d), which taking "**automatic action with respect to a second of the associated Internet-accessing electronic devices**." In particular, my Declaration relies on Hahn to show that it would have been obvious for the claimed "**action**" in Baig corresponding to claim 1(d) take place automatically.

61. Hahn discloses a series of well-known techniques for causing a web server to automatically send updated web pages to a user's web browser. As Hahn explains, conventional webpages do not automatically change after display:

> **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, referred to as "CLIENT PULL," involves the web browser automatically requesting that the page be reloaded at periodic intervals, for example every 30 seconds. (*Id.*) The second technique, which Hahn refers to as a "SERVER PUSH," involves the server automatically sending new data to the client without the

web browser having to make a request. (*Id.*)

62. Both of these techniques qualify as "**automatic**," as they occur without requiring user action. 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 in CLIENT PULL periodically issues a request to reload the page, the update is still "automatic" because both the client request and the server response occur without user action. The SERVER PUSH technique is similarly automatic, except that it does not even require the client to issue a request. (*Id.*) I will provide more information about Hahn in the discussion in the grounds below in which it is cited.

2. Additional Prior Art for Certain Dependent Claims

(a) Xu (EX1009)

63. **Xu**, U.S. Patent No. 7,730,030 B1, is entitled "Resource Based Virtual Communities." I am informed that Xu qualifies as prior art because it issued from a patent application filed on August 15, 2004, which is before the earliest filing date of the '878 patent.

64. My Declaration cites Xu for **Ground 2** and in connection with dependent claims 3 and 15. Xu discloses a system similar in some respects to Baig for creating virtual communities that allow users to share resources such as websites,

software, chat channels, discussion threads, or any other type of resource. (Xu, 10:24-31, 11:41-46.)

65. As I will explain below for the independent claims, Baig discloses a feature in which, after the user logs into the content server, the user may receive a list of other users who are in the same vicinity-based community. (Baig, *e.g.*, Fig. 6 (list 606), ¶0074; Baig Provisional, 0017.) Baig also discloses a feature in which users can decide whether or not they will 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."); Baig Provisional, 0019, 0027.) But Baig is unclear as to whether the user's visibility setting is stored in the user profile such that it would be retained and used, for example, if the user logs off or disconnects from a current access point/hotspot and later logs back into the content server at another access point/hotspot.

66. Xu has a similar feature to the Figure 6 in Baig of allowing users to be made aware of the presence of other users in a virtual community. (Xu, 19:32-36.) But users in Xu can opt-out of being visible to other members of the community, and this information can be persistently stored in a database. (*Id.*) For example, "[u]sers have full control over their own privacies and securities in the global user

database. For example, he can choose to sign in anonymously or be invisible to others, whatever mode he chooses." (Xu, 27:32-35.) Xu further explains that a user's preference with respect to their visibility to others is part of the user's stored preferences in a global user database. (Xu, 26:5-17.) "The global user database is used to keep all individual users' information, for example, its identifier and current status such as whether it is online or offline." (Xu, 26:5-7.) "User preferences such as privacy, security settings can also be stored there. For example, the system uses them to determine if the user should be anonymous or invisible to the rest of the community." (Xu, 26:13-15.)

67. As I will explain below for **Ground 2**, it would have been obvious to adapt Baig to include storage of the user's visibility setting. I will provide more information about Xu below.

(b) Gerace (EX1010)

68. **Gerace**, U.S. Patent Application Publication No. 2006/0282328 A1, is entitled "Computer Method and Apparatus for Targeting Advertising." I am informed by counsel that Gerace qualifies as prior art because it was filed on June 12, 2006 and published on December 14, 2006, both dates being before the priority date of the '878 patent.

69. My Declaration cites Gerace for purposes of dependent claims 6 and 7

discussed in **Ground 3**. Claim 6 recites that the "**automatic action**" of claim 1 comprises "**selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device**." Claim 7 further specifies that "**the automatic action comprises causing the selected advertisement to be directed to the second device**."

70. Gerace discloses a system for targeted advertising based on a "user profile" for an end user. (Gerace, ¶¶0008-0009, 0083.) The user profile can also include a user's demographic information. (Gerace, ¶¶0010, 0062, 0083.) A key feature of Gerace, for our purposes here, is the ability to fill-in demographic information for a user profile (such as age and gender) of a registered user, even if that user has not provided such information. "When not provided by the user, the system may forecast demographic information for a user based on relationships with other users and/or group members," for example, "average age of friends is assumed to be the end-users age, dominant gender of friends is assumed to be gender of the end-user," and so forth. (Gerace, ¶0010.) Gerace explains:

> This profile information is used to better target the known user with advertisement[s]. The system **100** <u>deduces demographic information</u> (city, state, etc.) from a user's IP address, the type of article the user reads, search query he enters, <u>shared behavior with other users</u>

> (behavior or activities in common with) or shared relationships to other users. In one embodiment, the system **100** (a) assumes a Zip code for a given user based on Zip codes detected in the user's activities, (b) assumes age of the given user based on ages of others detected in the user's activities, and (c) assumes gender of the given user based on gender of others detected in the user's activities.

(Gerace, ¶0083.) The user profile can be used to target and display adds to the user. (Gerace, ¶0055 ("The present invention forms and maintains user profiles **17** (**FIG**. **2***h*) based on information received from end-users and information deduced by end-user activity as users of system **100**. The present invention employs the user profiles **17** in targeting ad campaigns.").)

71. Gerace therefore discloses selecting an advertisement to display to a user based, at least in part, on a portion of the user profile information of another user, such as the age or gender of other users detected in the user's activities. I will provide more information about Gerace in the analysis of clams 6-7 below.

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

1. Claim 1

72. For reference, claim 1 recites:

> 1. A method for identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the

method comprising:

(a) with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:

(i) a device identifier;

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

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

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

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

(d) with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier

> of a first of the associated Internet-accessing electronic devices, and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices.

('878, 24:25-62 (Claim 1).)

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

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

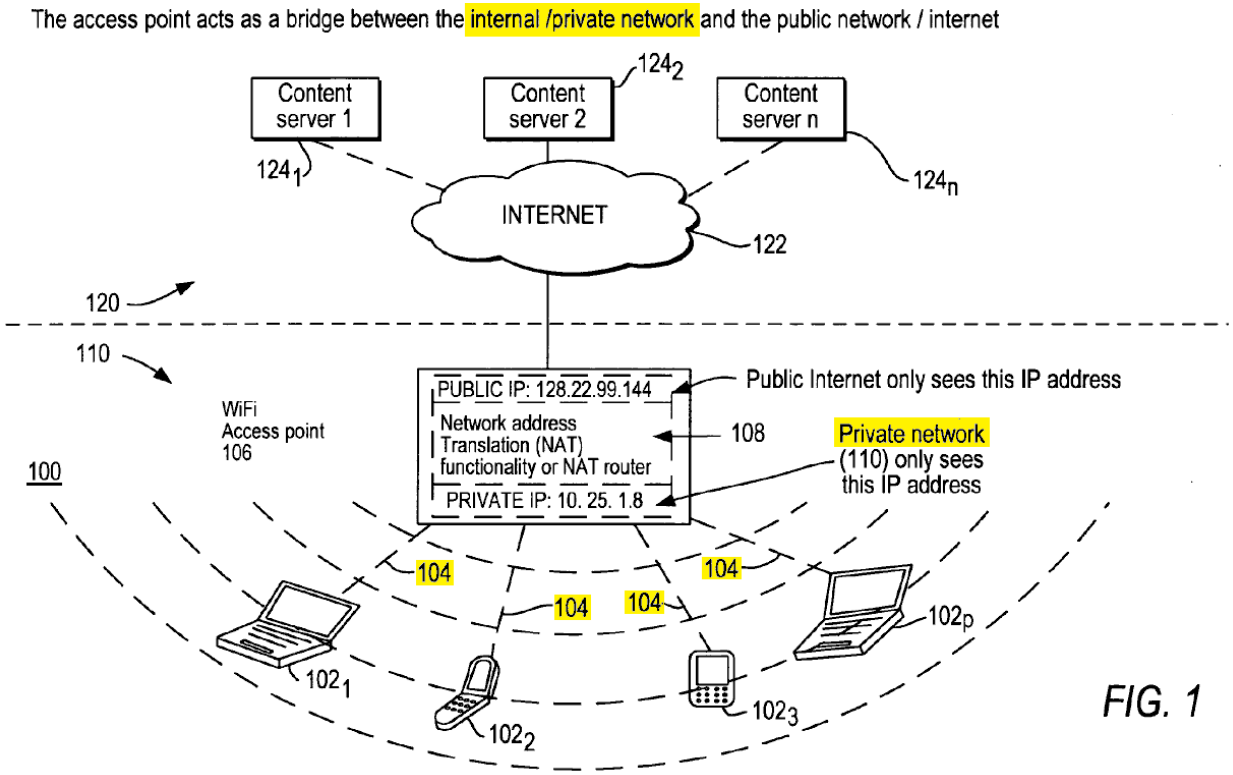


FIG. 1

(Baig, Fig. 1 (highlighting added).) Figure 1 above is a block diagram "illustrating how one or more mobile devices **102** at a public WiFi hotspot **110** interact with the public network **120**." (Baig, ¶0042; Baig Provisional, 0010.) The portion of Figure 1 below the dashed line shows a WiFi hotspot **110** that includes an access point **106** wirelessly connected to several mobile devices (**102_1** through **102_p**). (Baig, ¶0043; Baig Provisional, 00011.) Access point **106** in turn acts as a bridge to facilitate communications over the Internet **122** between the mobile devices **102** and one or more content servers (**124_1** through **124_n**), shown above the dashed line in Figure 1. (Baig, ¶¶0046-0047, Baig Provisional, 0012.)

75. As applied to the preamble, Baig discloses a method for "**identifying**

an association among multiple electronic devices of a group of devices connected through a common local area network (LAN)." The claimed "**common local area network (LAN)**" is shown as local private network **104** above in Figure 1, to which each of the mobile devices **102** are connected. As explained in Baig, "[t]he mobile devices **102** form a 'local network' **104** with the access point **106**, while everything outside of (i.e. external to) the hotspot **110**, i.e., all servers residing on the public Internet, is considered the 'public' network **120**." (Baig, ¶0043; Baig Provisional, 0011.) Local network **104** qualifies as a "**common**" local area network because each mobile device **102** shown in Figure 1 is connected through it. The "**multiple electronic devices of a group of devices**" correspond to any two or more mobile devices **102** within the plurality of mobile devices $\mathbf{102_1}$ through $\mathbf{102_p}$ and connected to local network **104**, as shown in Figure 1. (Baig, ¶0043; Baig Provisional, 0011.) As one illustration, the claimed "**multiple electronic devices**" could correspond to laptop computer $\mathbf{102_1}$ and mobile phone $\mathbf{102_2}$ shown in Figure 1, within the plurality of mobile devices $\mathbf{102_p}$.

76. Baig also discloses the step of "**identifying an association among**" the two or more mobile devices **102** that are connected through the common LAN. This step is performed by one or more content servers ($\mathbf{124_1}$ through $\mathbf{124_n}$) shown above the dashed line in Figure 1 above, which communicate with access point **106** over

the Internet **122**. (Baig, ¶¶0042-0043, Baig Provisional, 0010-0011.) As Baig explains and shown in Figure 1, access point **106** allocates a "local" IP address to each mobile device **102** to which it is connected, but in communications over the Internet to a content server **124**, replaces the private address with a common "public" IP address associated with access point **106**. (Baig, ¶¶0044-0046; Baig Provisional, 0011.) This is shown as the "PUBLIC IP" address in Figure 1 above.

77. In order to determine whether the two or more mobile devices **102** are connected to a common LAN, the content server in Baig checks to see if they are connected through an access point **106** having a common IP address. This is shown in Step **306** of Figure 3:

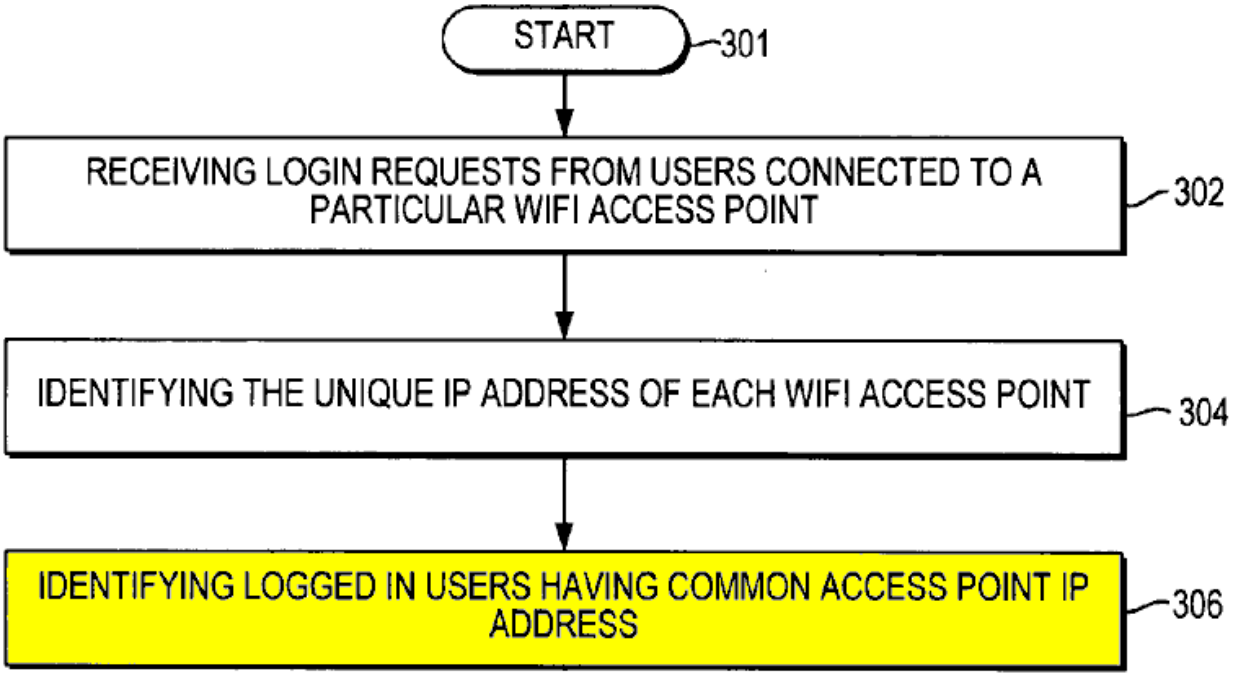


FIG. 3

(Baig & 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; Baig Provisional, 0013 ("At step **306**, the server **224** identifies the logged-in users having the same access point IP address."); *see also* Baig, ¶0038 ("The VSCP identifies a group of users at a wireless hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."); Baig Provisional, 0010.) Baig therefore discloses "**identifying an association among multiple electronic devices**," *i.e.*, that multiple mobile devices **102** are connected through the same

access point IP address which, in turn as noted, is used by the content server to determine whether the multiple mobile devices **102** are connected through "**a common local area network (LAN)**," as claimed.

78. Baig next discloses "**using the association for cross-device action**," as recited at the end of the preamble. After a user in Baig is logged-in, the user is taken to a webpage provided by content server **224** that shows, among other things, a list **606** of other users connected to the same hotspot **110**:

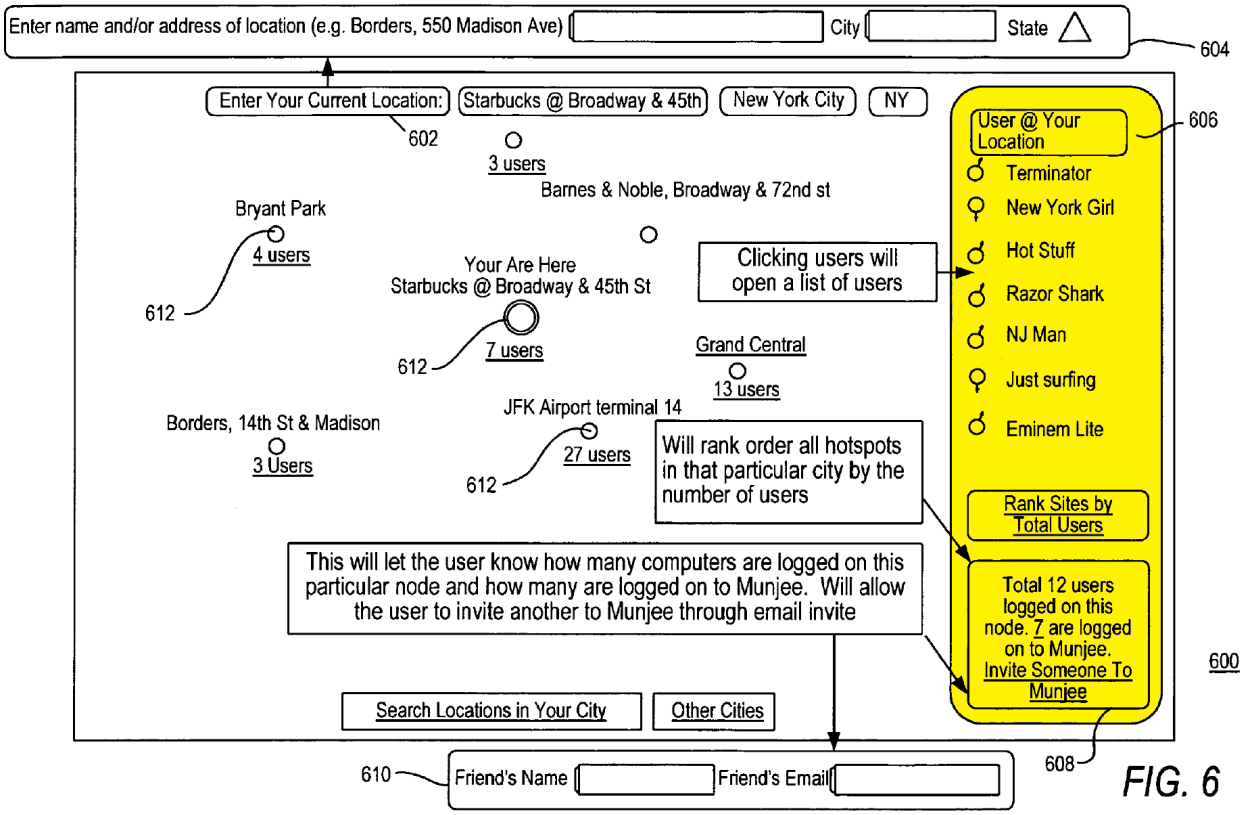


FIG. 6

(Baig, Fig. 6 (highlighting added); Baig, ¶0074 ("As described above, once a user registers on the web page illustrated in FIG. 5, and then logs into the VCSP website

on the home page as illustrated in FIG. 4, the server **224** presents the web page illustrated in FIG. 6 to the user on his/her mobile device **102**."); Baig Provisional, 0017.) Figure 6 shows list **606** shown in highlighting above, which "displays a list **606** of other users at the present hotspot **110**." As shown, the list includes the names of seven other users who are logged-on at hotspot **110** (*e.g.* "Terminator," "New York Girl"), and the list further shows, for each name, either a male or female gender symbol.

79. Baig discloses multiple examples of "**cross-device action**," *e.g.*, action taking place across multiple devices, that meet the claim. The display of list **606** above itself qualifies as "**cross-device action**" because it includes the action of transmitting the list to multiple mobile devices **102** that are connected to the same hotspot. As further examples, Baig explains that mobile device users within the vicinity of one another can engage in a number of services including "bartering services for goods and services among wireless users in a vicinity," "enabling WiFi users in the vicinity to play video games with one-another, providing chat rooms, among other activities and services." (Baig, ¶0054; Baig Provisional, 0013.) Figure 7, for example, shows a chat tab **706** allowing multiple users to engage in text chat with one another:

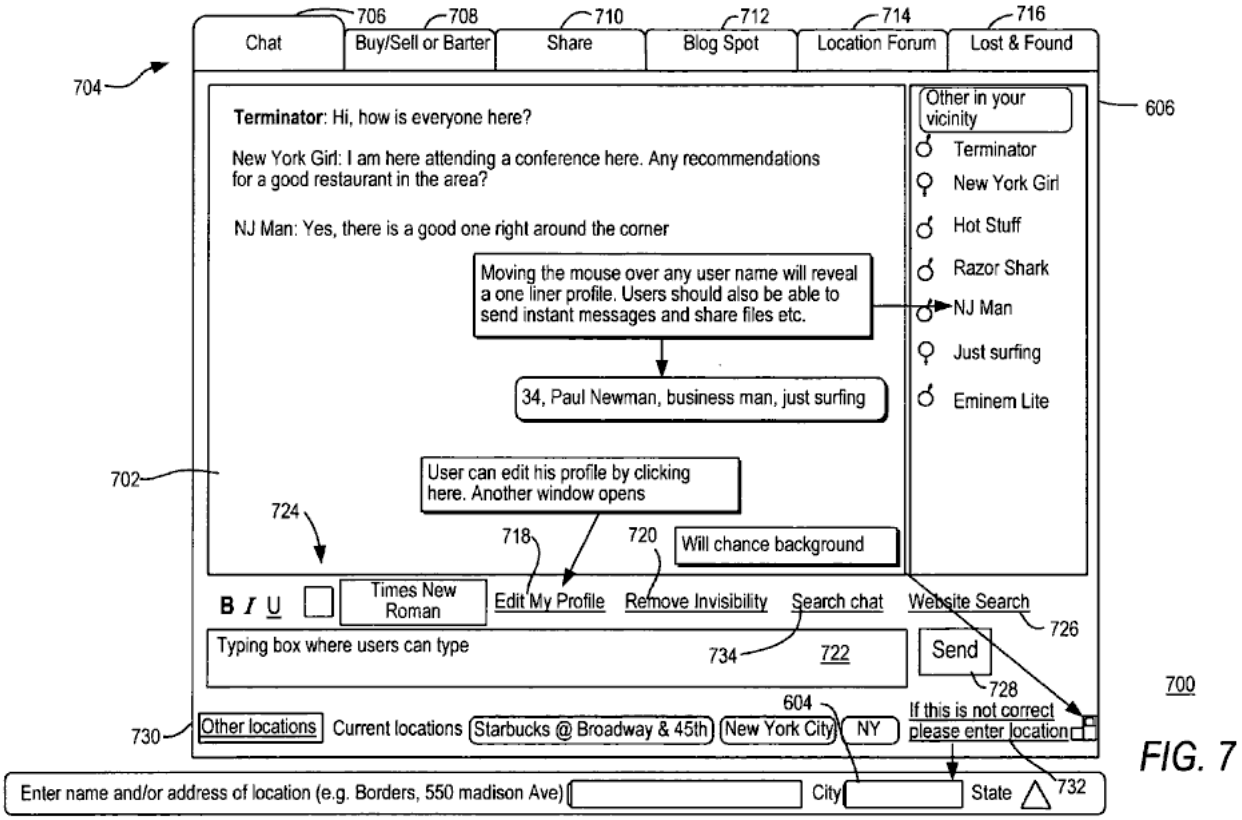


FIG. 7

(Baig, Fig. 7.) In this example, at least three users (*i.e.*, "Terminator," "New York Girl," and "NJ Man"), each identified in list **606** as being connected to the same hotspot **110**, are engaged in a text chat conversation.

80. Each of the example actions discussed qualifies as "**cross-device action**" because each action occurs across multiple devices. This cross-device action is also provided "**using the association**," as claimed, because the system uses the fact that the devices are connected to the same access point/hotspot, *i.e.*, to a common local area network (LAN), in order to identify these devices and provide the above-mentioned services and actions across mobile devices.

(a) "with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:"

(i) "a device identifier;"

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

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

81. For convenience, I prepared the following table to summarize how I have mapped the disclosures of the prior art to the limitations of claim 1(a):

Limitation from Claim 1(a)	Summary of Prior Art Disclosures
"a computer system"	At least one content server in Baig
"two or more Internet-accessing electronic devices"	Two or more mobile devices **102** in Baig, which are connected to and accessing at least one content server over the Internet
"determining an association between device identifiers"	Determining whether the two or more mobile devices **102** in Baig are connected to the content sever using an access point/hotspot having the same IP address
"electronically stored association detection information"	Information stored by the content server for each mobile device **102**, such as a session table under the combination with Laidlaw that includes at least the information specified in claims 1(a)(i)-(iii) (see below)

Limitation from Claim 1(a)	Summary of Prior Art Disclosures
"a device identifier"	A cookie containing a session token used to identify a mobile device **102** that is logged into the content server, based the combination with Laidlaw
"at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet"	The IP address of access point **106** (which includes router **108**) used by the mobile device **102** to log into the content server over the Internet, which is dynamically assigned via DHCP under the combination Sitaraman
"at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN"	Information specifying the last time that the mobile device **102** accessed the content server via access point **106**, based on the combination with Laidlaw

82. I will discuss these disclosures in more detail below.

83. As just explained in detail for the preamble, a content server ("**a computer system**") determines whether two or more mobile devices **102** ("**two or more Internet-accessing electronic devices**") are connected to the same hotspot **110**, and thus, to a common local area network. The content server thus performs the step of "**determining an association between device identifiers of two or more Internet-accessing electronic devices**," when it detects that at least two mobile devices **102** are both logged-in and connected to the content server via the same access point IP addresses. As explained in more detail below, each mobile device in Baig under the proposed combination would have had a "**device identifier**" in the form of a cookie stored by the content server that identifies its respective logged-in

mobile device **102**. I will provide a full explanation of the "**device identifier**" in a further discussion below.

84. Under the proposed combination, therefore, identifying two mobile devices **102** that are both logged in to the same hotspot clearly discloses "**determining an association between**" their respective device identifiers, under at least two independent theories. First, the association is determined because the device identifiers are associated with each other by virtue of referring to mobile devices logged-in using the same access point IP address, and thus, part of the same vicinity-based hotspot community. (Baig, ¶¶0056 ("At step **306**, the server **224** identifies all the users who have logged in from a common hot spot as having the same access point IP address."), 0040 ("Once the end-users at a particular access point log into the website of the VCSP, they are able to view other members of the VCSP who have also logged in from the same access point associated with a particular wireless hotspot."), 0069 ("The home page also includes a link **414** to see who else is logged in. By selecting link **414**, a list of users logged on to the website from the present vicinity-based hotspot is provided, as illustrated, for example, in the web pages of FIGS. 6 and 7."); Baig Provisional, 0013, 0010, 0017.) Second, the content server under the proposed combination with Laidlaw "**determin**[es] **an association**" between the "**device identifiers**" because it uses the cookie assigned

to each device to identify the device as being logged into the server, in order to place it into a vicinity-based community. (Baig, ¶0056 ("At step **306**, the server **224** identifies all the users who have logged in from a common hot spot as having the same access point IP address."), 0059 ("In particular, when a user at a hotspot logs into the website of the VCSP **202**, the user automatically becomes part of the vicinity-based user group."), 0076 ("The web page **600** also displays a list **606** of other users at the present hotspot **110**. In one embodiment, the list includes the user names associated with users that have logged into the VCSP website."), Baig Provisional, 0013-0014, 0018; Laidlaw, ¶¶0003-0006, 0016.) The content server in Baig, under the proposed combination, thus determines an association between device identifiers based on both the IP addresses of the devices (which are used to determine if they are connected via the same access point IP address) and their cookies (which are used to determine if they are currently logged-in) in order to place them into a group of devices connected via the same access point/hotspot.

85. Baig further discloses and renders obvious that the step of determining is "**based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices**," as claimed. For convenience of the Board, I will first address how the proposed combination renders obvious the claimed "**stored association-detection information**," and then explain how the

determining step is "**based on**" that information.

86. Subparts (i) through (iii) of claim 1(a), addressed in detail below, go on to specify particular information that must be included with the "**association-detection information**." Each of those pieces of information is rendered obvious over the proposed combination as explained below.

87. ***Subpart (i), "a device identifier"***: Based on the combination of Baig and **Laidlaw**, as described below, each mobile device **102** under the proposed combination would have had "**device identifier**" corresponding to a cookie stored by the content server, which would have been used by the content server to identify the computer used to log in.

88. Laidlaw discloses a system for managing "sessions" in a network-based computer system. In computer science and in the context here, the word "session" generally refers to a period of time when two devices maintain a connection over a network. (*See, e.g.*, *Microsoft Computer Dictionary* (5th ed. 2002), p.008 ("**session** *n*…. **2**. In communications, the time during which two computers maintain a connection.") (bold and italics in original).) A "session" generally commences when a first device logs into or accesses a second device and exists until the first device logs out or otherwise ceases its connection with the second device. (Laidlaw, ¶¶0003-0005.)

89. One of the key concepts disclosed in Laidlaw is a session "token," included in each request from a client device to a server, that identifies the requesting device. (Laidlaw, ¶0004.) In the context of the Internet and Web, the session token takes the form of a cookie:

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

(Laidlaw, ¶0006.)

90. The "cookie" described in Laidlaw refers to a well-known and industry standard technology developed in the 1990s by Netscape Communications, the company that published the Netscape Navigator web browser that was popular in the early days of the Web. A cookie is a file stored on the user computer by the web browser that can be used by a web site to identify the user when it visits the web site. (*See* Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0026 ("A cookie is a text that can be written to a text file on the user's hard drive when visiting a Web site. In most cases, that text will be a unique string, allowing the person to be identified.").) Laidlaw explains that cookies were developed to address

a limitation of the Hypertext Transport Protocol (HTTP), the protocol used to transport requests and responses between web browsers and web servers. HTTP is often referred to as a "stateless" protocol because when a user (via a web browser) transmits an HTTP request to a web server, the server generally has no knowledge of the user's previous requests. (Laidlaw, ¶0006 ("When a user requests a Uniform Resource Locator ('URL') from a web browser, there is no standard method for the receiving HTTP server to recognize the user identity or the fact that earlier requests originated from the same client.").) But if a stored "cookie" exists, the information in the "cookie" can be transmitted by the browser to the server with the HTTP request, thus allowing the responding server to know the identity of the requesting device and user. (Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0026 ("For example, a site may assign you a cookie with the text string '123.' Every time you access a page on the site, the server can request the cookie it placed and recognize that '123' Is back again and track where '123' goes on the site.").) Cookies were and remain in widespread use today on countless websites to allow websites to identify users who are logged in and to deliver customized information to visitors.

91. Turning back to the claim language, the "**stored association-detection information**" under the proposed combination would have included information

such as a session table described in Laidlaw stored by the content server in Baig under the proposed combination. (Laidlaw, ¶0016.) Session information (such as session tables described in Laidlaw) are a common feature of almost all network-based systems, which use this information to keep track of users who are currently logged-into the system. Laidlaw explains that the session table stores, on a per-user and/or per-device basis, a wide variety of information. (Laidlaw, ¶¶0016-0031.)

92. One of the pieces of information in the session table is the "session token," which takes the form of a cookie. As Laidlaw explains:

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

(Laidlaw, ¶0016.) The process above attempts to determine, in response to receiving a cookie from the requesting device, whether that session token in the cookie is stored in the session table. Laidlaw explains that the session table, in fact, is "keyed by session token," which means that the session token is the field used to organize the session table and locate the session table corresponding to its respective device, thus indicating that the session token is in fact stored in the table. (Laidlaw, ¶0040 ("A 'key field' partitions the database according to the high-level class of objects defined by the key field.").) Laidlaw explains that the session token can include a

sequence of encrypted data that uniquely identifies a session and includes, among other things, random data. (Laidlaw, ¶0032.) It therefore would have been obvious that the session token in the cookie ("**a device identifier**") would have been stored in the session table. I will provide a further discussion of the motivation to combine Baig and Laidlaw below.

93. My mapping of a session token/cookie to the claimed "**device identifier**" is also consistent with the '878 patent. Dependent claim 8, which I address below, depends from claim 1, makes clear that the claimed device identifier may be "**a cookie readable by the computer system**." The session token/cookie under the proposed combination provides a device identifier because it contains a session token uniquely identifying the mobile device **102** used by the user to access the content server. (Laidlaw, ¶0032.)

94. ***Subpart (ii), "at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet"***: Laidlaw explains that the session table includes "information regarding the host that the user logged in from (e.g., <u>the IP address</u>)." (Laidlaw, ¶0022.) Under the proposed combination of Baig with Laidlaw, therefore, the session table would also have stored the IP address of the access point **106** used to log into the content server.

95. It also would have been obvious based on Baig that this information

would have been stored by the content server. This is because Baig maintains a list of users whose devices are connected to the same hotspot 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 a second device, the server places both devices into a "vicinity-based" group of users. (Baig, *e.g.*, ¶0038 ("The VSCP identifies a group of users at a wireless hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."); Baig Provisional, 0010.) Baig explains that "[t]he [content] server **224** includes at least one processor, memory and support circuitry for running programs that, for example, 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**." (Baig, ¶0052; Baig Provisional, 0012-0013.) This is further shown in Figure 6, discussed above, showing exemplary webpage **600** showing, among other things, a list **606** of users connected to the same access point or hotspot:

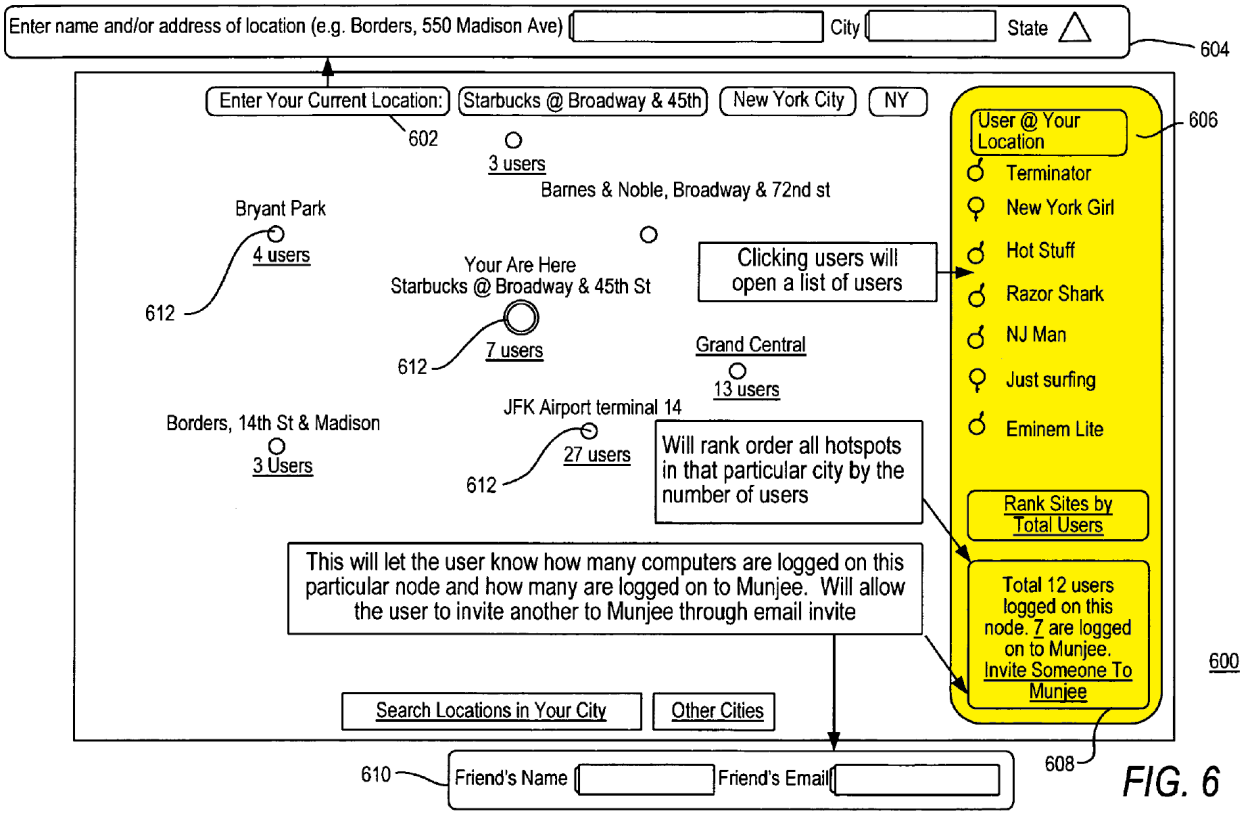


FIG. 6

(Baig, Fig. 6 (highlighting added).) The webpage shown in Figure 6 was generated and transmitted to the mobile device by the content server. (Baig, ¶0074 ("[T]he server **224** presents the web page illustrated in FIG. 6 to the user on his/her mobile device **102**."); Baig Provisional, 0017.) Webpage **600** includes list **606**, shown in highlighting, identifying several users whose devices were connected using the same access point/hotspot. (Baig, ¶0076 ("The web page **600** also displays a list **606** of other users at the present hotspot **110**."); Baig Provisional, 0018.) As noted previously, this means that the mobile devices associated with those users were connected to the same hotspot using the common IP address of its access point.

96. It would have been obvious that, in order for the content server in Baig to keep track of which mobile devices **102** are connected to the same access/point, the content server would have stored at least the access point IP address for each device. The list of users generated and stored by the content server in Baig thus further confirms the existence of "**electronically stored association-detection information**" that includes at least one "**IP address assigned to a modem that connects a router of the LAN to the Internet**," as claimed. The "**modem that connects a router of the LAN to the Internet**" is included within access point **106**, as shown again in Figure 1:

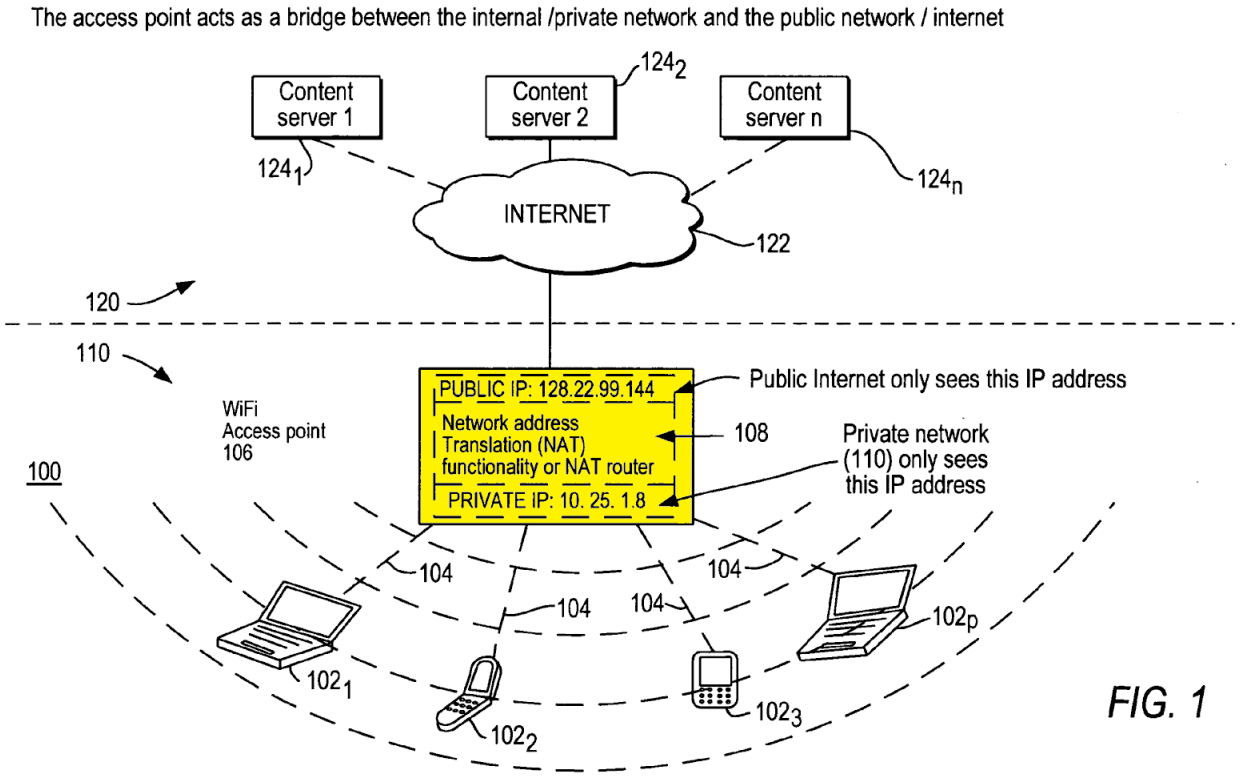


FIG. 1

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

97. It would also have been obvious that access point **106** includes "**a modem**" connected to the router, as confirmed by the fact that access point **106** "relays data between the wireless mobile devices **102** connected to the wireless network **104** and the external or public network, such as the Internet **122**." (Baig, ¶0044; *see also id.*, ¶0046 ("The access point **106** (which includes the NAT router **108**)… forwards the packets to the destination device (e.g., content server) on the Internet or external network **120**."); Baig Provisional, 0011.) It would have been obvious that access point **106** could not send information over a communications channel such as the Internet without a modem. The term "modem," which is short

for "modulator-demodulator," is a basic electronic device used for encoding ("modulating") signals for transmission over a communications medium, and decoding ("demodulating") signals received from another device via that communications medium. *See, e.g.*, *Microsoft Computer Dictionary* (5th ed. 2002), p.007 ("**modem** *n*…. **2**. Any communications device that acts as an interface between a computer or terminal and a communications channel.") (bold and italics in original).) For example, it was common for devices that connect directly to the Internet (such as an access point depicted in Baig) to use a communications medium for Internet technologies such as Digital Subscriber Line (DSL) for telephone-based wires, Data Over Cable Service Interface Specification (DOCSIS) for cable television (such as coaxial) wires, and among others. In any case, regardless of the particular communications medium used by the Internet in Baig, it would have been obvious that access point **106** would have included (among other components) a modem for sending and receiving signals and information over that medium. The IP address of the access point **106** is thus also assigned to the modem.

98. Accordingly, it would have been obvious that the IP address of the access point **106**, stored in a session table in content server 224 under the proposed combination, discloses "**at least one… IP address assigned to a modem that connects a router of the LAN to the Internet**."

99. I note that claim 1(a)(ii) specifies at least one "**dynamically assigned**" IP address. One embodiment in Baig states that WiFi access points may be static IP addresses. (Baig, *e.g.*, ¶¶0064 ("Since the IP addresses of WiFi hotspots are mostly static IP addresses…."), 0050 ("The WiFi access point **106** has a static IP address that is visible to communication networks external to the hotspot **110**."); Baig Provisional, 0015, 0012.) As I will explain in a further discussion below, it would have been obvious to adapt the system of Baig to also allow an access point that uses a "**dynamically assigned**" IP address. I will cover this topic in a separate discussion below.

100. ***Subpart (iii), "at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN"***: The '878 patent does not define the word "**timestamp**," nor does the term appear outside the claims. The term was widely understood by ordinarily skilled artisans as referring generally to information identifying a time, and timestamps were (and are today) often used to create a record of when a particular event occurred. Laidlaw discloses that the session table includes a timestamp, *i.e.*, "information regarding the last time the session was accessed." (Laidlaw, ¶0017.)

101. Under the proposed combination with Baig, therefore, the session table would have included a "**timestamp**," *i.e.*, information indicating a time, "**when the**

Internet-accessing electronic device," *i.e.*, when logged-on mobile device **102**, "**accessed the Internet via the router of the LAN**," *i.e.*, accessed the content server during the session, over the Internet through access point **106**.

102. It would have been obvious that the timestamp in Laidlaw could have been used for a variety of purposes; for example in Laidlaw, a session can be terminated after a period of inactivity. (Laidlaw, ¶¶0005, 0030.) The session table in Laidlaw, in fact, includes a "max inactivity time allowed" (Laidlaw, ¶0030), and it would have been obvious to use the "last time the session was accessed" to determine whether the max inactivity time has been reached (*e.g.*, the user has been timed-out and their session terminated).

103. ***Rationale and motivation to combine (Baig and Laidlaw)***: It would have been obvious to combine Baig with Laidlaw, predictably resulting in the system of Baig in which the content server included "**electronically stored association detection information**," for example, a session table that stores, for each logged-in mobile device **102**, (i) the cookie/session token information, (ii) the IP address of access point **106** used by the mobile device to access the content server, and (iii) a timestamp indicating the last time the mobile device accessed the content server over the Internet during the session. As further explained below, an ordinarily skilled artisan would have been motivated to provide this information, and to use it to

"**determine**[e] **an association between device identifiers**" of two or more mobile devices **102**. As noted, I will separately explain below, for part (ii), why it would also have been obvious to adapt the proposed combination to store a dynamically-assigned IP address.

104. Baig is analogous and in the same field of the '878 patent because Baig describes techniques for facilitating online access between devices through a common local network and via the Internet. Baig and Laidlaw are also analogous references in the broader field of the '878 patent of managing device access to computer networks and keeping track of connected devices. Baig and Laidlaw would also have been reasonably pertinent to a number of problems facing the inventors, including how to identify devices currently-connected to a common local area network (LAN) and how to store information keeping tracking of currently-connected devices (including among other things their IP addresses).

105. An ordinarily skilled artisan would have been amply motivated to combine. Laidlaw itself confirms that session management was a common technique for keeping track of devices connected over the Internet. (Laidlaw, ¶¶0002-0006.) It would have been obvious that in any network-based system that has the ability to keep track of logged-in users – such as Baig – the system would have stored information about those users to determine that they are in fact currently

logged-in (and to distinguish them non-logged-in users). It would therefore have been obvious to adapt the content server of Baig to store data, such as using a session table described in Laidlaw, to keep track of users and their respective mobile devices that are logged into the content server through access point **106**. Without the ability to store such information, as explained, the system of Baig would have been unable to later remember the identity of logged-in users.

106. And an ordinarily skilled artisan would have been further motivated to include each of the three pieces of information in the session table discussed above. With respect to claim 1(a)(i), it would have been obvious to store a session token/cookie and use it to determine that the user of mobile device **102** is currently logged-in. (Laidlaw, ¶0016 ("When the user authenticates at a login screen, the session token is placed into a cookie.").) Baig itself expressly suggests storing a cookie by disclosing the ability of the server to "remember" the user name and password of a user – a classic and textbook use case for cookies that was well-known to skilled artisans. (Baig, ¶0068 ("A check field **408** is provided for optionally remembering the user name and user password."); Baig Provisional, 0016; *see also* Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0028 ("When the user returns to that site, the server will automatically check the cookie it gave to that user to determine his or her name and password.").) An ordinarily

skilled artisan would have been motivated to use cookies as they represented an industry-standard and widely used technique for keeping track of the identity of users and their respective devices in web-based systems. Under the proposed combination, therefore, the content server would have stored the session token/cookie after the user logged in through access point **106** using mobile device **102**, and then used it to later identify the mobile device **102** when it receives subsequent requests from that device. It thus would also have been obvious to "**determin**[e] **an association between device identifiers**" of mobile devices **102**, under the proposed combination, based at least in part on the cookie/session token.

107. Laidlaw also recognizes that cookies are one of a small number of known techniques for web-based session management – and an ordinarily skilled artisan would have regarded cookies as superior in many ways to the two other alternatives described in Laidlaw, *i.e.*, "hidden form fields" and "URL mangling." (Laidlaw, ¶0006.) Hidden form fields rely on embedding session token information into a hidden field of a form, which would be passed back to the server when the user completes the web form and submits it for transmission to the server. This would have been unhelpful for a large majority of web pages that do not require or even use form-based input. With respect to "URL mangling" referenced in Laidlaw, as its name implies, this involves rewriting the URL to include session token

information. But this can not only make the URLs longer and harder to read, but it can also create potential security vulnerabilities. This is because the user could transmit the URL to another other user without realizing that the URL contains the user's session token. Depending on the implementation of the website, this might allow the other user to impersonate the original user on the website.

108. With respect to claim 1(a)(ii), as explained above, it would have been obvious to include the IP address of access point **106** used by mobile device **102** to access the content server. An ordinarily skilled artisan would have been motivated to store this information because, as explained above, Baig uses this IP address to create vicinity-based networks by identifying users who are connected to the content server via the same local area network (LAN). It thus would also have been obvious – and in fact necessary – to "**determin**[e] **an association between device identifiers**" of mobile devices **102**, under the proposed combination, based at least in part on the IP address of the access point **106**.

109. With respect to claim 1(a)(iii), an ordinarily skilled artisan would have been motivated to include the claimed timestamp, in this case the time when mobile device **102** last accessed content server **224**, in order to determine if the user should be "timed out" and logged out. (Laidlaw, *e.g.*, ¶¶0005, 0017, 0030.) An ordinarily skilled artisan would have been motivated to provide this feature for two reasons:

(1) it increases security by making it more difficult to impersonate or assume the identity of a user by using that user's device (for example if the user temporarily steps away from its device), and (2) it increases efficiency by releasing session resources that might be put to use by another user. Under the proposed combination, therefore, the timestamp would have been used to determine if a logged-on user should remain logged in. Additionally, a timestamp would have been valuable to determine the probability that a mobile device user connected to the content server is, in fact, still at the location associated with the access point/hotspot. For example, even in situations where mobile devices have not yet timed out, or where the content server is not programmed to automatically log users out due to inactivity, devices associated with more recent timestamps would have indicated more recent activity, thus identifying for other users those mobile device users more likely to be available for interaction through the various features in Baig. It thus would also have been obvious to "**determin**[e] **an association between device identifiers**" of mobile devices **102**, under the proposed combination, based at least in part on the timestamp, for example, as an additional step to determine whether each mobile device **102** connected through the same access point **106** is, in fact, still connected or should be timed out. As explained below, an ordinarily skilled artisan would have had a reasonable expectation of success in implementing the proposed combination. As

explained further below, an ordinarily skilled artisan would have had at least a reasonable expectation of success in combining Baig with Laidlaw.

110. ***"Dynamic" IP address***: Claim 1(a)(ii) requires "**at least one dynamically assigned IP address**." The term "IP address" generally refers to a unique address on the Internet where a device or other resource can be located. (*See, e.g.*, *Microsoft Computer Dictionary* (5th ed. 2002), p.005 ("**IP address** *n*… Short for **I**nternet **P**rotocol **a**ddress. A 32-bit (4-byte) binary number that uniquely identifies a host (computer) connected to the Internet to other Internet hosts, for the purposes of communication through the transfer of packets.").) IP addresses are commonly categorized as either being "static" or "dynamic." A static IP address is an address that is "practically permanently allocated and recorded, typically, in DNS servers." (Sitaraman, EX1007, 4:10-13.) The U.S. Patent and Trademark office, for example, has an IP address of 209.112.123.30, which appears to be a static IP address used for the uspto.gov website. Baig discloses that WiFi access points (such as access point **106**) use static IP addresses. (Baig, *e.g.*, ¶0064; Baig Provisional, 0015.)

111. Baig does not expressly disclose the use of a "**dynamic**" IP address for access point **106**, but this would have been obvious based on the general knowledge of an ordinarily skilled artisan, as confirmed by **Sitaraman** (EX1007). Sitaraman

discloses a technique for managing dynamic IP address allocation. (Sitaraman, Abstract.) My Declaration primarily relies on disclosures in the Background of Sitaraman, which would have been basic knowledge of ordinarily skilled artisans.

112. Sitaraman acknowledges that with the exponential growth of the Internet, companies and users are faced with an increasing shortage of IP addresses, since there is a finite number of static addresses. (Sitaraman, 3:21-29.) One well-known approach to address this issue is known as "dynamic" IP addresses, in which a device is assigned an IP address that is dynamically assigned by a server known as a Dynamic Host Configuration Protocol (DHCP) server. DHCP refers to an industry-standard technique in which a device on a network (such as a client) can ask a DHCP server "to provide it with an IP address and configuration parameters. A DHCP server on the network that is authorized to configure this client will offer an IP address by sending a reply to the client." (Sitaraman, 3:34-40.) Sitaraman explains that DHCP servers are used, for example, by Internet Service Providers (ISPs) who typically maintain a "pool" of available IP addresses that can be dynamically assigned upon request. (Sitaraman, 3:64-4:1, 6:63-66 ("The dynamic IP address server **8** maintains a pool **22** of IP addresses and leases the IP addresses of the pool **22**. In accordance with a preferred embodiment, the dynamic IP address server **8** is a DHCP server.").)

113. If the client accepts the offered IP address, "the chosen DHCP server sends an acknowledgement with the offered IP address having an associated 'lease' time," which can be renewed by the client upon request. (Sitaraman, 3:42-47.) "Once the lease expires, the IP address can be 'recycled' and given to another machine." (Sitaraman, 3:49-51.)

114. ***Rationale and Motivation to Combine (Baig and Laidlaw with Sitaraman)***: It would have been obvious to combine Baig and Laidlaw with Sitaraman. The combination would have predictably resulted in the Baig-Laidlaw system described above, with the further ability of access point **106** to have a dynamically-assigned IP address, for example, using the well-known DHCP techniques described in Sitaraman. Under the proposed combination, therefore, the IP address of access point **106** (which contains router **108**) would have been dynamically assigned by a DHCP server, and thus, the "**stored association-detection information**" for each mobile device **102**, under the proposed combination, would have included "**at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet**."

115. Sitaraman is an analogous reference in the same field of communication between devices over the Internet, including use of dynamic IP addresses. Sitaraman would also have been reasonably pertinent to a number of problems facing the

inventor, including understanding DHCP and how dynamic IP addresses are assigned and "leased" to requesting devices. I note that the '878 patent specification repeatedly refers to DHCP as being used to allocate dynamic IP addresses to modems, thus enhancing the relevance and pertinence of Sitaraman and its discussion of DHCP and dynamically-assigned IP addresses. ('878, *e.g.*, 4:7-48, 9:57-61, 10:58-62.)

116. An ordinarily skilled artisan would have been amply motivated to combine. At the outset, I note that an ordinarily skilled artisan would have understood that, despite Baig's use of static IP addresses for access points, the vicinity-based community system in Baig does not depend on access points only having static IP addresses. The vicinity-based community is instead based on whether users have logged into content server **224** from a common hot spot having the same access point IP address. (Baig, *e.g.*, ¶0056 & Fig. 3 (Step **306**), Baig Provisional, 0013.) Identifying users logged into a common hotspot would have functioned the same way regardless of whether the underlying IP address for the access point was static or dynamically-assigned.

117. An ordinarily skilled artisan would have been motivated to use a dynamically-assigned IP address for access point **106** in order to more efficiently assign and use available IP addresses. Sitaraman expressly acknowledges this

motivation by explaining that Internet Service Providers (ISPs) "are faced with an increasing shortage of IP addresses," and that DHCP was developed in part "to help solve the shortage of IP addresses." (Sitaraman, 3:25-33.) For example, traditional iPv4 addresses (which are typically represented as four numbers, *e.g.*, 209.112.123.30), which were the most common types of IP addresses in use as of April 2007, allow only four billion unique addresses worldwide. DHCP, by allowing IP addresses to be temporarily used (leased), and then recycled and used by other devices, allows for more efficient utilization of scarce IP addresses. For example, if access point **106** in Baig was used in a coffee shop, airport, or other commercial facility, there would likely be times when the access point would not be used, for example, during hours when the facility is closed or during vacations. Allowing access point **106** to use a dynamically-assigned IP address would have allowed access point **106** to have a unique IP address when it is in use, while not consuming that available IP address during those times when it is not in use.

118. An ordinarily skilled artisan would have also recognized other well-known benefits of dynamic IP addresses. For example, unlike dynamic addresses, static IP addresses are typically not free and usually require payment of periodic fees (for example through a third party service provider) to maintain the permanent address. As a result, the majority of users and devices on the Internet well before

April 2007 used dynamically-assigned IP addresses, which continues to be true today. The '878 patent itself expressly acknowledges this fact by stating that many users of online access services do not have static IP addresses, but rather, use dynamic IP addresses assigned using DHCP. ('878, 9:57-61.) Additionally, it was also well-known that systems that use static IP addresses were more susceptible to attacks by hackers and other malicious parties. This is because once a malicious party gained knowledge of a target system's static IP address, the party could continue attempting to penetrate that system for long periods using that same IP address. But with a dynamically-assigned IP address, the target system could be assigned a new and different dynamic IP address using DHCP, thus thwarting the malicious party from accessing the target system until or unless it finds a way to obtain the newly-assigned dynamic IP address.

119. An ordinarily skilled artisan would have also been motivated to use dynamic IP addresses to increase and expand the size and reach of the vicinity-based network system in Baig to include a larger group of access points, including those that have static addresses and others with dynamic addresses. It would have been obvious that WiFi hotspots, which were common as of April 2007, may not always have had static IP addresses because of cost and other considerations as discussed above. Static IP addresses were (and still are) most often used by larger corporations

and organizations. It is therefore likely that WiFi hotspots at smaller stores or establishments would have relied on the dynamically assigned IP addresses provided by their Internet service providers. Under the proposed combination, therefore, the vicinity-based system would have been able to support access points and hotspots having <u>either</u> static or dynamic IP addresses, thus increasing its potential audience (of both hotspots and thus users) and thus enhancing the commercial and financial potential of the system.

120. Finally, I note that Baig discloses that, in one embodiment, a static IP address of access point **106** can be used by the system to correlate a particular hotspot with a physical address. (Baig, ¶0064.) This is because, as explained in Baig, a user can provide the physical address (such as a street address), which can be stored in a database in association with the static IP address. (Baig, ¶0064 ("Therefore, the next time a user logs in to the website from that specific IP address, the VCSP **202** can correlate this specific IP address with the address."); Baig Provisional, 0016.) This functionality in Baig would have remained available even if access point **106** had a <u>dynamic</u> IP address; the only difference would be that a user may have to occasionally reenter the physical address when a different dynamic IP address is assigned. But this would have amounted to, at best, a minor inconvenience outweighed by the significant advantages of allowing dynamic IP addresses as

detailed above. Moreover, instances in which users would have had to reenter the physical address would likely have been infrequent. For example, an access point **106** could have leased the dynamic IP address for an extended period of time (such as multiple days or weeks), and even after the lease expires, it is not uncommon for DHCP servers to assign the same dynamic IP address to a device that it previously assigned (provided of course it is still available).

121. An ordinarily skilled artisan would have had at least a reasonable expectation of success in the combination of Baig, Laidlaw, and Sitaraman. As noted previously, the session management techniques in Laidlaw (including use of cookies and session tables), and the DHCP dynamic IP address techniques in Sitaraman, were within the general knowledge of an ordinarily skilled artisan. An ordinarily skilled artisan could have implemented the proposed combination using conventional programming techniques, and the disclosures of the prior art provide more than sufficient detail to carry out the disclosures on which I have relied to arrive at the claimed invention, without undue experimentation.

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

122. Claim 1(b) was largely addressed in the discussion above. As explained, the determining step of claim 1(a) is performed by using "**the stored association-detection information**," *i.e.*, the stored information (for example in a session table) under the proposed combination. For example, as explained, the stored association-detection information includes both a cookie/session token and a timestamp assigned to each mobile device **102**, which is used to determine that each mobile device **102** is in fact logged-in and not timed out – a prerequisite to joining a vicinity-based community under the proposed combination. (Baig, ¶0055 & Fig. 3 (Step **302**).) The stored association-detection information also includes a dynamic IP address of access point **106**, which is used to determine if two or more mobile devices 102 are connected to the same hotspot **110** on a common network. (Baig, ¶¶0056 & Fig. 3 (Step **306**).) The stored association-detection information is thus used in the detecting step.

123. Claim 1(b) further requires that the two or more devices "**have separately accessed the Internet through a router of the LAN… via a common**

IP address," but this requirement is also satisfied by Baig. For example, as discussed above for Figure 1, each mobile device **102** connected to the local network in Baig has its own local or private IP address. (Baig, ¶0049, Fig. 2 ("1. Devices A, B, C, D & E will be allocated 'local' IP addresses, not visible to the outside world….."); Baig Provisional, 0012, Fig. 2.) NAT router **108** within access point **106** routes outgoing and incoming communications between each mobile device and the Internet, with the IP address of the access point **106** ("**a common IP address**") being used for accessing the Internet. (Baig, ¶¶0050-0051; Baig Provisional, 0012.) Each mobile device **102** has "**separately**" accessed the Internet because, as anyone who had used an IP-based local network would have appreciated, if one device were to log off or disconnect from the Internet, another connected device could have continued to communicate using its separate local IP address. This is consistent with Figure 1 depicted above and reproduced below, which shows mobile devices **102** connected separately and independently of each other to a common local network **104** through access point **106**:

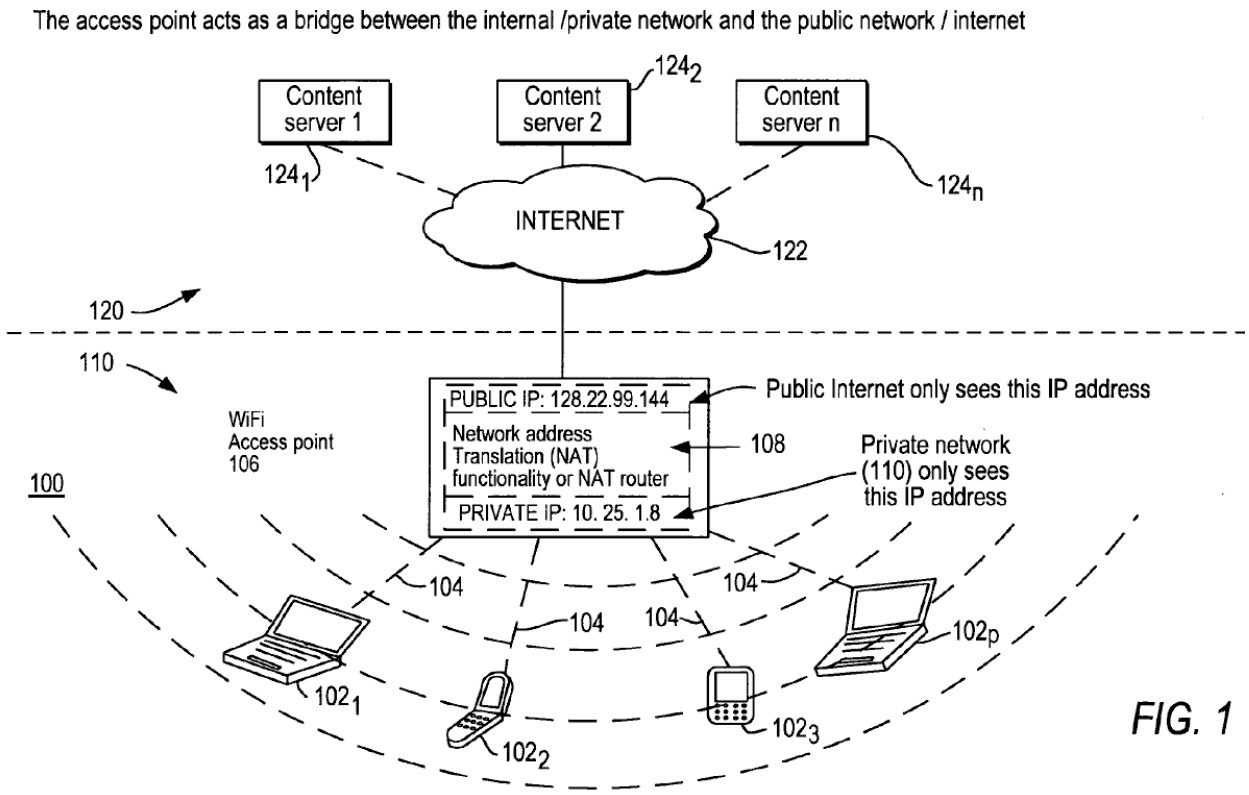


FIG. 1

(Baig, Fig. 1.) Figure 1 does not show any links, connections, or other dependencies between any of the mobile devices **102** connected to local network **104**. To the contrary, each mobile device **102** depends only on access point **106** – and not on other mobile devices **102**– for its connection to the Internet **122**. (Baig, ¶0043; Baig Provisional, 0011.) It therefore would have been obvious that each mobile device **102** accessing the Internet **122** through access point **106** has "**separately accessed the Internet through a router of the LAN**," and has done so "**via a common IP address**," *i.e.*, the common IP address of access point **106**.

124. This is further confirmed by the fact that, as Baig expressly confirms, mobile devices need not be connected to the content server at the same time. Figure

3 of Baig, discussed above, discloses a scenario in which a mobile device can wirelessly connect to a particular access point and make a login request (Steps **301-302**), and content server **224** responds by identifying other users who have already connected to that access point (Step **306**). (Baig, Fig. 3; Baig, ¶¶0055-0056; Baig Provisional, 0013.) The fact that mobile devices can connect to the access point at different times further confirms the separateness of their connection to the Internet. Nothing in Baig suggests that the connection of a mobile device to the local network depends on any other mobile devices on that network.

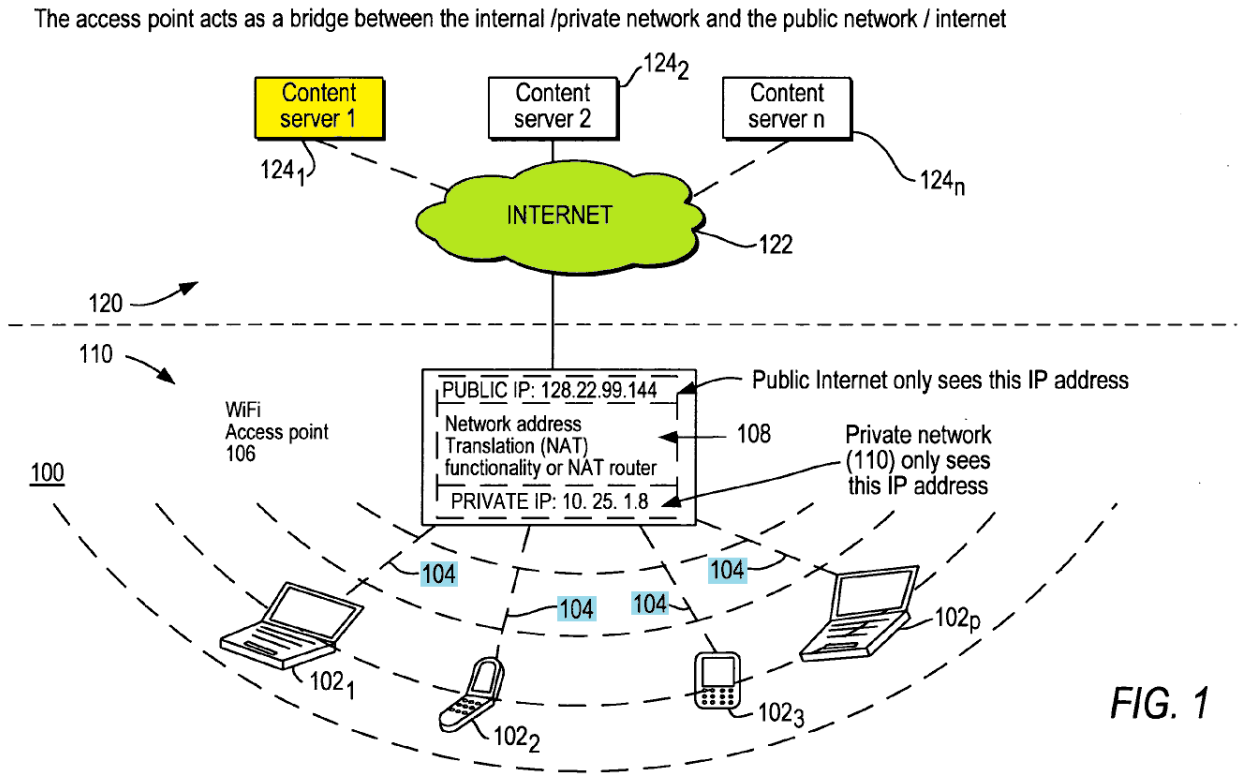
125. Finally, each mobile device has also separately accessed the Internet "**during a predetermined period of time via a common IP address**," as claimed. This is because, as explained for claim 1(a) above, the IP address of the access point **106**, based on well-known and industry-standard DHCP techniques, would have been a dynamically-assigned IP address with a "lease" time during which the address remains valid. (Sitaraman, 3:42-51.) "Once the lease expires, the IP address can be 'recycled' and given to another machine." (Sitaraman, 3:49-51.)

126. Under the proposed combination, therefore, mobile devices **102** accessing the Internet via access point **106** would have accessed during "**a predetermined period of time via a common IP address**," *i.e.*, the lease time for the dynamic IP address used by access point **106**. This period of time is

"**predetermined**" because it was based on the lease time provided by the DHCP server when it first assigned the dynamic IP address to access point **106**, which was determined before any of the mobile devices **102** in Baig could have logged into the content server via that access point. Accordingly, when "**the two or more Internet-accessing electronic devices have separately accessed the Internet through a router of the LAN**," they would have done so during that predetermined lease period in which the dynamic IP address of access point **106** was valid. In fact, I note that the '878 patent describes the claimed "**predetermined period of time**" by expressly alluding to these well-known DHCP lease time techniques. ('878, 4:22-26 ("The assignment of the IP address usually expires after a predetermined period of time, at which point the DHCP client and server renegotiate a new IP address from the DHCP server's predefined pool of IP addresses.").)

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

127. Baig also satisfies this limitation, as shown again in Figure 1:



(Baig, Fig. 1 (highlighting added).) As discussed above, Figure 1 shows each content server **124** (one of which I have heighted as an example), connected to the public Internet **122**, and makes clear that the content server ("**the computer system**") is connected to local network **104** (via access point **106**) through the Internet **122**, but the content server is outside of local network **104**. As Baig explains: "[T]he mobile devices **102** form a 'local network' **104** with the access point **106**, while everything outside of (i.e., external to) the hotspot **110**, i.e., all servers & computers residing on the public Internet, is considered the 'public' network **120**." (Baig, ¶0043; Baig Provisional, 0011.) Baig therefore discloses that "**the computer system determining the association in part (a) is outside the LAN and is**

connected to the LAN through the Internet."

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

128. This final limitation of claim 1 is disclosed by Baig, in combination with **Hahn**. As explained, after a user logs into the content server using its mobile device **102** ("**a first of the associated Internet-accessing electronic devices**"), the content server in Baig ("**the computer system**") places the mobile device **102** in a vicinity-based group with other mobile devices connected to the same hotspot/access point. (Baig, *e.g.*, ¶¶0038 ("The VSCP identifies a group of users at a wireless hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."), 0052 ("The server **224**… identif[ies] 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**."); Baig Provisional, 0010, 0012-0013.) As explained in detail below, this in turn will result in a transmission of information to the second mobile device ("**an automatic action with respect to**

a second of the associated Internet-accessing electronic devices").

129. As discussed, Baig discloses a technique of creating a vicinity-based group of users whose mobile devices are connected via the same access point IP address (and thus connected to the same local area network). (Baig, *e.g.*, ¶¶0038 ("The VSCP identifies a group of users at a wireless hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."), 0052 ("The server **224**… identif[ies] 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**."); Baig Provisional, 0010, 0012-0013.)

130. As mentioned for above, after a user is logged-in, the user is taken to a webpage as shown in Figure 6 that shows, among other things, a list **606** of other users connected to the same hotspot:

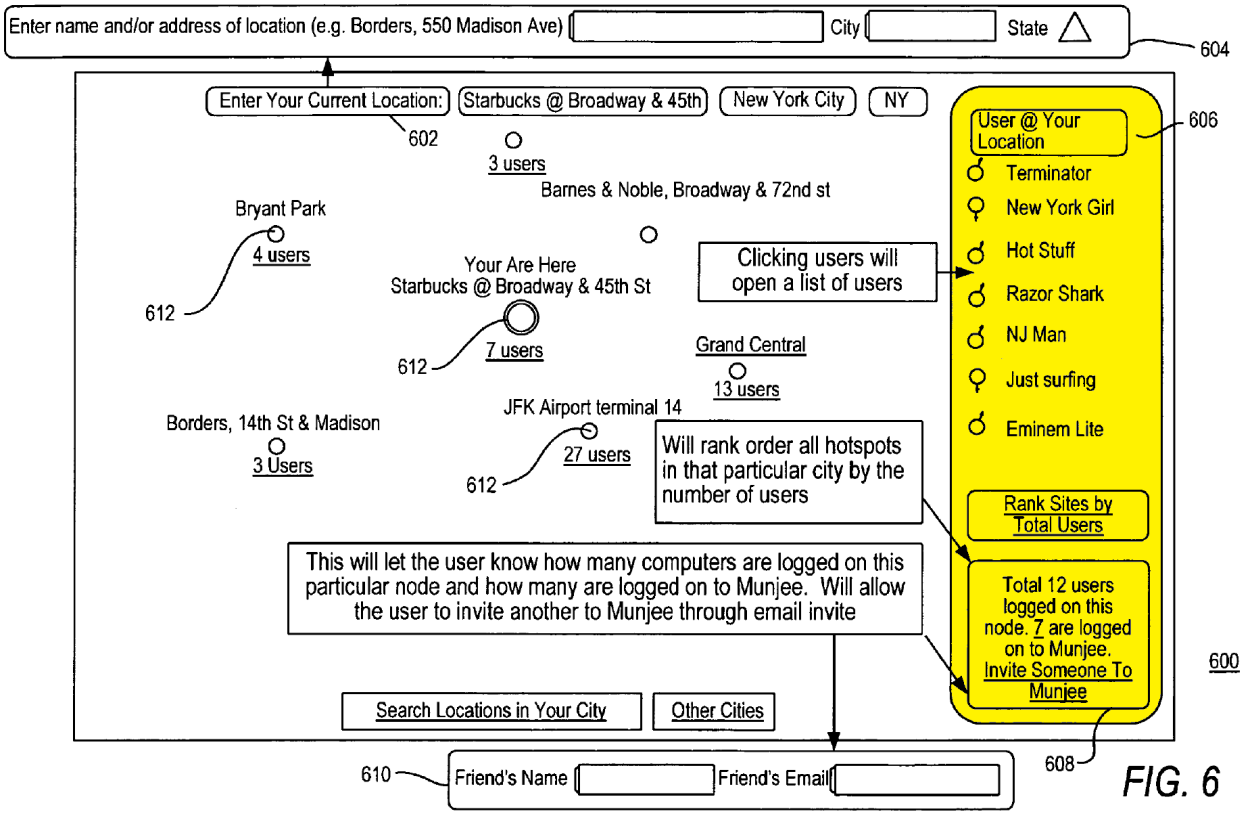


FIG. 6

(Baig, Fig. 6 (highlighting added); Baig, ¶0074 ("As described above, once a user registers on the web page illustrated in FIG. 5, and then logs into the VCSP website on the home page as illustrated in FIG. 4, the server **224** presents the web page illustrated in FIG. 6 to the user on his/her mobile device **102**."); Baig Provisional, 0017.) The key part of the webpage here is list **606** shown in highlighting above, which "displays a list **606** of other users at the present hotspot **110**." As shown, the list includes the names of seven other users who are logged-on (*e.g.* "Terminator," "New York Girl"), and the list further shows, for each name, either a male or female

♂ Terminator
♀ New York Girl
♂ Hot Stuff

gender symbol. The gender symbols are clear from Figure 6 above, but the version of Figure 6 in the incorporated-by-reference provisional (shown in part at right) shows them more clearly. (Baig Provisional, Fig. 6.)

131. List **606** of other 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 ("In FIG. 7, the Chat tab **706** is shown as being selected (highlighted), and displaying a text conversation between two or more users. In one embodiment, the list **606** of users at the present hotspot is shown on the right side of the display screen."); Baig Provisional, 0019.)

132. The transmission and display of list **606** as disclosed in Baig discloses and renders obvious claim 1(d). Baig discloses "**with the computer system**," *i.e.*, with the content server, "**using the association determined in part (a)**," the association based on the first and second mobile devices being connected to the same hotspot/access point, **"tak**[ing] **an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices**," *i.e.*, sending list **606** as part of a webpage to the second mobile device.

133. Let's take 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 was already connected and currently viewing the webpage of Figure 6 or Figure 7 on their mobile device (**the second device**), with both users connected via the same access point as discussed. In this scenario, after "Terminator" logged in, the content server would have sent the webpage to the second device including list **606**, showing that "Terminator" was now part of the vicinity-based group. This would have resulted in an "**action with respect to a second of the associated Internet-accessing electronic devices**," because the second device would have received and displayed "Terminator" on list **606** when displaying the webpage shown in Figure 6 or Figure 7. (Baig, ¶¶0076 ("The web page **600** also displays list **606** of other users at the present hotspot **110**."), 0080 (same, Fig. 7); Baig Provisional, 0018-0019.)

134. I note that the claim further requires taking "**automatic**" action, and Baig is unclear as to the timing with respect to display of list **606**. For example, it is unclear how list **606** in Figure 6 gets updated or refreshed on the second device when a new user joins using the same access point/hotspot. For this reason, I have relied on Baig in further combination with **Hahn** for the "**automatic**" issue. I will discuss Hahn in a separate discussion below.

135. Turning back to Baig, the action taken with respect to the second device was also the result of "**utiliz**[ing] **user profile information associated with the**

device identifier of a first of the associated Internet-accessing electronic devices and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices." This is because, as explained above, list **606** that was transmitted to and displayed on the second device identifies the gender of the other logged-in users. For "Terminator" who is logged in using the first device using our example above, list **606** includes a gender symbol ("♂") indicating that he is male. The transmission and display of list **606** to the second device is thus the result of "**utilizing user profile information**," because it includes gender information of "Terminator," who has connected using the first device having the access point IP address as discussed above ("**associated with the device identifier of a first of the associated Internet-accessing electronic devices**"). The mapping of gender information to "**profile data**" is consistent with the '878 patent, which broadly describes profile data as including "demographic or behavioral information," such as information "concerning the user's characteristics or activities." ('878, 6:7-12.) The gender of "Terminator" clearly qualifies as a user profile information including at least "**demographic data**" that was "**collected**" via the first device. (Baig, ¶¶0093 ("As users register online on the VCSP website, profile information about our users, such as age, gender, occupation, interests and the like are requested during the registration process and securely stored by the

VCSP **202**."), 0096 ("For example, each user enters age and gender information, among other information in their profiles at the time of registration."), 0070 & Fig. 5 (explaining that new user registration form includes "Gender" field **508** to collect gender information from new user); Baig Provisional, 0022, 0017.)

136. Although claim 1(d) requires only requires one of "**demographic**" or "**behavioral**" profile information, Baig discloses a second way in which the transmission and display of list **606** on the second device was the result of "**behavioral**" information collected via the first device. The '878 broadly defines "**behavioral**" information as including any a wide variety of previous action by the user/subscriber, including "and any other form of previous subscriber activity." ('878, 4:49-57.) Similarly, Baig discloses behavioral information in the form of action by the user indicating that they wish to be visible to other users. (Baig, *e.g.*, ¶¶0081 ("A link **720** can also be provided to remove [the user's] concealment (i.e. invisibility) to other users."), 0124 ("All users who are logged on can see the other users in the chat-room, unless a user options out from being visible to other users."); Baig Provisional, 0019, 0027.) The transmission and display of list **606** is thus the result of utilizing profile information including "**behavioral information**," because list **606** transmitted to the second device will only include "Terminator" (who is connected using access point IP address associated with the first device), if

"Terminator" took an action allowing himself to be visible to other users. Stated another way, the fact that "Terminator" appeared in list **606** sent to the second device is the result of his activity/behavior, *i.e.*, indicating that "Terminator" selected link **720** "to remove [his] concealment (i.e. invisibility) to other users." (Baig, ¶0081; Baig Provisional, 0019.)

137. Baig also discloses taking the claimed action "**using the device identifier of the second of the associated Internet-accessing electronic devices**." 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 logged into the content server using the device identifier of the second device, *e.g.*, the cookie as explained in claim 1(a)(i). As explained previously, the cookie is used under the proposed combination to allow the content server to identify the mobile device as being logged in – a prerequisite to display of the web page in Figure 6 that includes list **606**. (Baig, ¶0073 ("[O]nce a user… logs into the VCSP website on the home page as illustrated in FIG. 4, the server **224** presents the web page illustrated in FIG. 6 to the user on his/her mobile device **102**."); Baig Provisional, 0017.) Because logging into the content server is a necessary prerequisite – and direct cause – of the transmission of list **606** to the second device for display (the "**action**"), the transmission occurred "**using**" at least

the cookie assigned to the second device. Additionally, as explained for claim 1(a)(i), the "**device identifier**" under the proposed combination with Laidlaw is used as a key to locate the session table associated with the second device. (Laidlaw, ¶0016.) That session table, as explained, further includes the IP address of the access point used by the second device to connect to the content server –a necessary piece of information for content server to send information to the second device. The ability to send the webpage with list **606** to the second device, in other words, relies and thus uses the cookie ("**device identifier**") of the second device.

138. As mentioned briefly above, claim 1(d) further requires that the claimed action be "**automatic**," and Baig is unclear as to whether the "**automatic**" requirement is met. For example, consider again the example scenario above 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 such as "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 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. (*See* Baig, ¶¶0076 ("The web page **600** also displays list **606** of other users at the present hotspot **110**."); 0038 ("The VSCP identifies a group of users at a wireless

hotspot based upon their common public IP address and interconnects them, thereby creating a vicinity-based user group."); Baig Provisional, 0018, 0010.)

139. But it is not clear from Baig when (or how) list **606** is updated when, for example, new users connect to the hotspot. For example, is list **606** updated automatically or does the mobile device user have to do something (such as press the "refresh" button on the web browser) to cause the display of list **606** to update?

140. But this omission from Baig does not present any obstacle to finding claim 1 obvious. 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 or removed from the access point vicinity group.

141. This is confirmed by **Hahn** (**EX1008**), a 1996 textbook describing basic and well-known features of conventional web technologies. As Hahn explains, conventional webpages do not automatically change after display:

> **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, referred to as "CLIENT PULL," involves the web browser automatically requesting that the page be reloaded at periodic intervals, for example every 30 seconds. (*Id.*) The second technique, which Hahn refers to as a "SERVER PUSH," involves the server automatically sending new data to the client without the web browser having to make a request. (*Id.*)

142. Both of the techniques in Hahn independently qualify as "**automatic**," as they occur without requiring user action. With respect to CLIENT PULL, Hahn explains that "the client program (your browser) is told to 'pull' information from the server <u>without your intervention</u>." (Hahn, p.0048.) Although the client in CLIENT PULL periodically issues a request to reload the page, the update is still "automatic" because both the client request and the server response occur without user action. The SERVER PUSH technique is similarly automatic, except that it does not even require the client to issue a request. (*Id.*)

143. ***Manner, Rationale, and Motivation to Combine (Baig with Laidlaw and Sitaraman)***: It would have been obvious to adapt the automatic update techniques of Hahn to the system based on the Baig-Laidlaw-Sitaraman combination, predictably resulting in the content server being adapted to

automatically send 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. Under the proposed combination and building on the scenario described above, therefore, when user "Terminator" connects to the access point and logs into the website using the first device, the content server would **automatically** send an updated version of Figure 6 or Figure 7 – with an updated list **606** – to the second device for display.

144. This would have been true under both the CLIENT PULL or SERVER PUSH techniques in Hahn. For the CLIENT PULL technique, the web browser on the second device would have periodically and automatically requested reloading of the webpage without user action, predictably resulting in the content server transmitting an updated webpage (with an updated list **606** showing "Terminator") to the second device for display. For the SERVER PUSH technique, the content server would simply have transmitted an updated webpage after "Terminator" joined the access point and/or logged onto the website. Either implementation would have rendered obvious "**tak**[ing] **an automatic action with respect to a second of the associated Internet-accessing electronic devices**," because in both cases, the updated webpage is automatically (without user action) sent to the second device reflecting the addition of "Terminator" to the group. An ordinarily skilled artisan

would have found this combination straightforward.

145. As noted previously for claim 1(a), Baig is closely analogous to the ’878 patent. Hahn is also an analogous reference in the same field of the ’878 patent of providing online access to information (such as websites) over the Internet and/or local networks. Hahn would also have been reasonably pertinent to a number of problems facing the inventors, including how to automate an electronic transmission based on the claimed indicia. For example, Hahn would have been reasonably pertinent to the inventors in implementing a technique for automatically transmitting information after it has been determined that the first and second devices were connected to the same local network.

146. An ordinarily skilled artisan would have been amply motivated to combine. 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**) would have frequently changed. As discussed above, Baig expressly contemplates that new users could have been added to vicinity groups when additional mobile devices

connect to an access point and login to the website – and this could have occurred frequently. The system in Baig, for example, is designed to work with mobile devices that connect to access points at locations where users commonly gather for short periods of time, such as a coffee shop or airport terminal. (Baig, *e.g.*, ¶¶0039 (STARBUCKS coffee shop), 0078 (JFK airport terminal); Baig Provisional, 0010, 0018.) An ordinarily skilled artisan would thus have been motivated to adapt the website of Baig to incorporate the automatic update techniques of Hahn so users have up-to-date information about users in the vicinity group as shown in list **606**.

147. Hahn provides a further motivation to combine by explaining that its automatic update techniques are suitable for "web-based talk facilities," in which users send messages back and forth with other users. (Hahn, pp.0048-0049, 0070.) Baig discloses such a system by disclosing, for example, the ability of users to chat with other users in a vicinity group. (Baig, *e.g.*, Fig. 7, ¶¶0080-0082; Baig Provisional, 0019.) The automatic update techniques in Hahn would have provided a clear benefit to Baig of providing a user with an automatically-updated list **606** to provide an up-to-date identification of other users with whom the user can communicate.

148. An ordinarily skilled artisan would have perceived no technological obstacle to the proposed combination, and would have had more than a reasonable

expectation of success. The automatic update techniques in Hahn were already well-known by the time Hahn was published in 1996, and thus would have been considered entirely trivial by April 2007. For example, the industry standard for the Hypertext Markup Language (HTML), the language used to encode webpages, provides a specific "refresh" metatag for specifying a timing interval (such as every 10 seconds) in which the webpage will be automatically reloaded. Both the CLIENT PULL and SERVER PUSH techniques in Hahn could have been implemented using conventional techniques.

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

149. As explained for claim 1, each of the devices connected to the LAN is a "**mobile device**." (Baig, ¶0042 ("Referring to FIG. 1, a block diagram is shown illustrating how <u>one or more mobile devices</u> **102** at a public WiFi hotspot 110 interact with the public network **120**."); Baig Provisional, 0010-0011.) It would also have been obvious that each mobile device would have been connected "**only intermittently**" to the LAN. As explained for claim 1, the claimed "**LAN**" corresponds to the local private network **104** shown in Figure 1, in which each mobile device **102** is connected using the same access point/hotspot. It would have been obvious that each mobile device would have been connected only

intermittently; as explained for claim 1(d), because access points/hotspots may be located where users commonly gather for short periods of time, such as coffee shops or airport terminals. (Baig, *e.g.*, ¶¶0039 (coffee shop), 0078 (airport terminal); Baig Provisional, 0010, 0018.) It would have been obvious that after users leave this location – for example move to a location outside the range of the WiFi hotspot – they would no longer be connected to the LAN. (Baig, ¶0052 (noting that "the range of wireless communications for any given hotspot is limited…"); Baig Provisional, 0013.) It would also have been obvious that a user may have frequented a location having a WiFi hotspot (such as a coffee shop), thus resulting in the mobile device of that user being connected to that hotspot/access point only intermittently.

150. This is further confirmed by disclosures in Baig in which the system keeps track of the number of logged-in users at particular times of the day, *e.g.* by hourly increments, thus further confirming that mobile devices may be connected to the LAN only intermittently. (Baig, ¶¶0114-0115, Figs. 14-15; Baig Provisional, 0025-0026.) It therefore would have been obvious that the first mobile device, as with every other mobile device connected through the current hotspot/access point, "**is connected to the LAN only intermittently**," as claimed.

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

151. As fully explained for claim 1(a) above, the "**device identifier**" for the first and second mobile device **102**, based on the combination of Baig and Laidlaw, would have been a cookie that stores the session token provided to the mobile device **102** by the content server. (Laidlaw, ¶¶0006, 0016.) It would also have been obvious (and basic knowledge of an ordinarily skilled artisan) that the cookie would have been "**readable by the computer system**," *i.e.*, by the content server of Baig under the proposed combination. The whole purpose of a cookie, in fact, is to be subsequently passed back from a client device to a server so the server can read the cookie to identify and recognize the client device. (Laidlaw, *e.g.*, ¶0006 ("A cookie is a sequence of binary information… which the client system <u>sends back to the web server with each subsequent request</u>…. A <u>web application may inspect the value of cookies</u>, and search for cookies that it previously issued in order to determine that a given web request is from a user who had previously been sent a cookie.").)

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

152. It would also have been obvious, and basic knowledge of an ordinarily skilled artisan, that the cookie would have been "**stored, in a member of the first**

device," as claimed. As Laidlaw explains, "[a] cookie is a sequence of binary information that a web server may send to a client system, and which the client system sends back to the web server with each subsequent request…." (Laidlaw, ¶0006.) It would have been obvious that a client system, such as mobile device **102**, would have stored the cookie in memory in order to be able to send it "back to the web server with each subsequent request" (*id.*). Conversely, if a cookie was not stored, the client system would not be able to "remember" it for inclusion in subsequent requests. Indeed, it was basic knowledge of ordinarily skilled artisans that cookies were stored on the computer of the web browser. (*See* Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0026 ("A cookie is a text that can be <u>written to a text file on the user's hard drive</u> when visiting a Web site. In most cases, that text will be a unique string, allowing the person to be identified.").) It also would have been obvious that storage of the cookie in the memory of the first device would have occurred "**using the computer system**," *i.e.*, the content server, because it was the content server that initially sent the cookie to the mobile device **102** for storage there so it could be included in subsequent requests to the server. (Laidlaw, ¶0006.)

153. It would also have been obvious that the claimed storing occurs "**automatically**." Under the proposed combination, after the user has logged in to

the content server, the content server would have created the session token and place it into a cookie. (Laidlaw, ¶0016 ("When the user authenticates at a login screen, the session token is placed into a cookie.").) Nothing in Laidlaw suggests (let alone requires) user intervention in any aspect of the creation of the cookie, or the transmission of the cookie to the client device for storage. This is also consistent with the well-known behavior of cookies. It was well-known to that a cookie was stored "**automatically**" on a client computer in response to receipt of the cookie by the client computer. Storage of cookies is so automatic and transparent, in fact, that users often had no idea that they even existed. For example, Zeff reports of complaints by some in the press that cookies can "invade privacy by clandestinely placing a file on the user's hard drive," which is the reason web browsers provide optional settings that enable users to disallow storage of cookies from websites. (Robbin Zeff et al., *Advertising on the Internet* (2d ed. 1999) (**EX1011**), p.0027.)[4]

154. Finally, the fact that each mobile device **102** would have logged into the content server (such as by the user entering a username and password) does not

[4] The automatic nature of cookie storage is also the reason why jurisdictions in Europe and some states within the United States now require that websites obtain user consent prior to storing cookies locally on visitor computers. This has resulted in the now-ubiquitous (and oftentimes annoying) "Allow Cookies?" prompts that appear on a large number of websites today.

diminish my conclusion with respect to the "**automatically**" limitation. The fact that storage of the cookie may have been preceded by user action is irrelevant because the actual claimed storage of the cookie occurred without user intervention. This is consistent with the '878 patent, which explains that a cookie can be stored in response to numerous types of preceding user actions, for example to "store a username used by the user to access a site," as well as to store "previous searches conducted at the site, or pages viewed or visited at the site, by the computer user." ('878, 6:49-54.)

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

155. It would also have been obvious that the session token/cookies for the first and second mobile device **102** ("**device identifiers**") would have included no personally identifiable information. Laidlaw describes an exemplary session token in the form of a sequence of 128 bits of data that "contains three elements: random data, a UNIX time stamp, and an incremental token ID," which is concatenated together then encrypted. (Laidlaw, ¶0032.) Laidlaw explains that the "UNIX timestamp" is typically represented as the number of seconds since January 1, 1970, which was well-known, and the "token ID" is simply "an integer whose value increments by a predetermined amount every time the system generates a new ID."

(*Id.*) None of this data, either before or after encryption, includes any personally identifiable information pertaining to any user. The data, in fact, is entirely independent of the identity of the user or its characteristics.

6. Independent Claim 13

156. Claim 13 is substantially similar to claim 1 except written as a computer system claim, as shown by the table below (common language shown in underlining):

Claim 1	Claim 13
1. A method for identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the method comprising:	13. A computer system comprising at least one hardware server computer, wherein the computer system is programmed and connected to perform a method of identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the method comprising:
(a) with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:	(a) with the computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:

(i) a device identifier;	(i) a device identifier;
(ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and	(ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and
(iii) at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;	(iii) at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;
(c) wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and	(c) wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and
(d) with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices.	(d) with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices.

157. Claim 13 is thus obvious for the same reasons as claim 1. As with claim 1, the "**computer system**" for claim 13 corresponds to a content server in Baig, which qualifies as "**at least one hardware server computer**," which is "**programmed and connected to perform**" the method of claim 13. Baig explains

that the content server includes a processor, memory and support circuitry ("**hardware server**") that stores and executes computer programs for carrying out the disclosed techniques. (Baig, *e.g.*, ¶¶0052 ("The [content] server **224** includes at least one processor, memory and support circuitry for running programs that, for example, 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**."), 0053 ("The at least one server **224** further includes programs and data for hosting a website of the VCSP **202**."); Baig Provisional, 0013.) The hardware server in Baig, under the proposed combination, would therefore have been programmed to perform each of the steps of claim 13.

7. Claims 14 and 19

158. Dependent claims 14 and 19 are substantially similar to claims 2 and 10, respectively, except that they depend from claim 13 instead of claim 1. This is confirmed by the table below (common language shown in underlining):

Claim 2	**Claim 14**
2. <u>The</u> method <u>of claim</u> **1** <u>wherein the first device comprises a mobile device that is connected to the LAN only intermittently</u>.	14. <u>The</u> computer system <u>of claim</u> **13** <u>wherein</u> the computer system is programmed to perform the method even when <u>the first device comprises a mobile device that is connected to the LAN only intermittently</u>.
Claim 10	**Claim 19**

10. The method of claim **1** wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device.	19. The computer system of claim **13** wherein the computer system is programmed to perform the method even when the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device.

159. Claims 14 and 19 are thus obvious for the same reasons as claims 2 and 10, discussed above.

8. Independent Claim 22

160. Claim 22 is substantially similar to claim 1 and claim 13 except written as an "**article**" claim, as shown by the table below (common language shown in underlining):

Claim 1	Claim 22
1. A method for identifying an association among multiple electronic devices of a group of devices connected through a common local area network (LAN) and using the association for cross-device action, the method comprising:	22. An article comprising a tangible data storage medium that is not a transitory propagating signal encoding computer-readable instructions that, when applied to a computer system comprising at least one hardware server computer, instruct the computer system to perform a method comprising:
(a) with a computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about	(a) with the computer system, determining an association between device identifiers of two or more Internet-accessing electronic devices based on electronically stored association-detection information about

Claim 1	Claim 22
a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:	a plurality of Internet-accessing electronic devices, wherein the stored association-detection information for each of the plurality of Internet-accessing electronic devices includes:
(i) a device identifier;	(i) a device identifier;
(ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and	(ii) at least one dynamically assigned IP address assigned to a modem that connects a router of the LAN to the Internet; and
(iii) at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;	(iii) at least one timestamp specifying a time when the Internet-accessing electronic device accessed the Internet via the router of the LAN;
(b) wherein determining the association in part (a) is done by using the stored association-detection information to determine that the two or more Internet-accessing electronic devices have separately accessed the Internet through a router of the LAN during a predetermined period of time via a common IP address;	(b) wherein determining the association in part (a) is done by using the stored association-detection information to determine that the two or more Internet-accessing electronic devices have separately accessed the Internet through a router of the LAN during a predetermined period of time via a common IP address;
(c) wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and	(c) wherein the computer system determining the association in part (a) is outside the LAN and is connected to the LAN through the Internet; and
(d) with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising	(d) with the computer system, using the association determined in part (a) to utilize user profile information associated with the device identifier of a first of the associated Internet-accessing electronic devices, and comprising

Claim 1	Claim 22
behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices.	behavioral or demographic data collected via the first of the associated Internet-accessing electronic devices, to take an automatic action with respect to a second of the associated Internet-accessing electronic devices using the device identifier of the second of the associated Internet-accessing electronic devices.

161. Claim 22 is thus obvious for the same reasons as claim 1 and claim 13. As explained for claim 13, the "**computer system**" corresponds to a content server in Baig, which qualifies as "**at least one hardware server computer**," which is "**programmed and connected to perform**" the method of claim 13. Baig explains that the content server includes a memory for storing computer programs for carrying out its techniques. (Baig, *e.g.*, ¶¶0052 ("The [content] server **224** includes at least one processor, memory and support circuitry for running programs that, for example, 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**."), 0053 ("The at least one server **224** further includes programs and data for hosting a website of the VCSP **202**."); Baig Provisional, 0012-0013.) The claimed "**article comprising tangible data storage medium that is not a transitory propagating signal encoding computer-readable instructions**," corresponds in Baig to the

memory for storing computer programs for carrying out the techniques of Baig. (*Id.*) It would have been obvious that the programs in Baig would have included computer-readable instructions that, under the proposed combination, would have been used to carry out each of the steps of claim 22.

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

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

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

163. The only aspect of claim 3 that was not covered by my analysis of claim 1(d) was the last clause, in which the behavioral data would have been collected "**when the first device is not connected to the LAN**." But this further feature adds nothing of patentable significance.

164. It would have been obvious to anyone who had used a public WiFi hotspot as of April 2007, or was familiar with WiFi generally, that mobile devices **102** in Baig could have been moved out of the range of a particular hotspot/access point, and into the range of another hotspot/access point. (Baig, ¶0052 (noting that "the range of wireless communications for any given hotspot is limited…"); Baig Provisional, 0013.) Baig itself confirms that use of WiFi hotspots had skyrocketed in parks, cafes, bookstores, airports, and other public places. (Baig, ¶0037; Baig Provisional, 0009.) It thus would have been obvious that a mobile device **102** in Baig could have logged into a content server using a first access point/hotspot at a first location (such as an airport), and later logged into the content server using a second and different access point/hotspot at a second location (such as coffee shop), with each access point/hotspot having a <u>different</u> IP address and thus each <u>defining</u> a different local area network (LAN). (Baig, ¶0043 ("Thus, the mobile devices **102** at the hotspot **110** form a local network **104** with the access point **106**."); Baig Provisional, 0011; *see also* Bergs, U.S. Patent Application Publication No. 2005/0175181 A1 (EX1012), ¶0004 ("Moreover, a change from one hotspot to another hotspot involves changing the IP address.").)

165. It therefore would have been obvious, applying this example to claim 3, that the <u>first</u> device user could have <u>previously</u> made its selection regarding

visibility to other users while accessing a first access point/hotspot (for example at an airport) – as Baig explains, by choosing to "remove their concealment (i.e., invisibility) to other users." (Baig, ¶0081; Baig Provisional, 0019.) That first device user could then have moved to the current access point/hotspot (for example at a coffee shop), and then logged into the content server from there.

166. As a result, when both the first and second users are logged into the content server from the current access point/hotspot, when transmission of the list **606** in Figure 6 to the mobile device of the second user ("**the action**") occurs, it would have been based on "**behavioral data collected via the first device at a time when the first device is not connected to the LAN**," *i.e.*, because the first user's visibility selection (which was used to determine whether list **606** will identify the first device user) was collected via the first device while previously connected to the airport access point/hotspot.

167. But one final issue warrants further discussion. My example above assumes that the content server in Baig would have stored or otherwise remembered the first device user's visibility selection made at the first access point/hotspot, such that the selection would later be applicable when first device user logs into the content server from the second access point/hotspot. Baig explains that when users register, "profile information about our users, such as age, gender, occupation,

interests and the like are requested during the registration process and securely stored by the VCSP **202**." (Baig, ¶0094; Baig Provisional, 0022.) But Baig itself does not indicate, one way or another, whether the user's visibility selection is one of the pieces of information stored as part of the user profile. Nevertheless, retaining the user's visibility selection would have been obvious in further view of **Xu**.

168. Xu discloses a system similar to Baig for creating virtual communities that allow users to share resources such as websites, software, chat channels, discussion threads, or any other type of resource. (Xu, 10:24-31, 11:41-46.) Xu discloses a similar feature of allowing users to be made aware of the presence of other users in a virtual community. (Xu, 19:32-36.) But like Baig, users in Xu choose whether or not they wish to be visible to other members of the community, and this information can be persistently stored in a global database. (*Id.*) For example, "[u]sers have full control over their own privacies and securities in the global user database. For example, he can choose to sign in anonymously or be invisible to others, whatever mode he chooses." (Xu, 27:32-35.) With respect to the "global user database," it "is used to keep all individual users' information, for example, its identifier and current status such as whether it is online or offline." (Xu, 26:5-7.) "User preferences such as privacy, security settings can also be stored there. For example, the system uses them to determine if the user should be anonymous or

invisible to the rest of the community." (Xu, 26:13-15.)

169. As applied to Baig, therefore, it therefore would have been obvious to adapt the content server in Baig to store the user's visibility setting as part of its privacy settings, for example in a user database, such that the user's visibility preference would have been applicable even if the user logs out and later logs in to the content server, including from a different hotspot/access point. As a result, under the proposed combination using the example above, the first device user's visibility selection which was connected to the first access point/hotspot would have been preserved and used, when the first device user logs into the content server using the current access point/hotspot, to determine whether list **606** will identify the first device user.

170. Xu is an analogous reference in the same field of providing online access to information (such as websites) between multiple devices over the Internet. Xu would also have been reasonably pertinent to a number of problems facing the inventors, including how to collect and later use behavioral information that was collected from a first device user in deciding what information to present to a second device user.

171. An ordinarily skilled artisan would have been motivated to combine in order to give users in Baig greater control over their own privacy when interacting

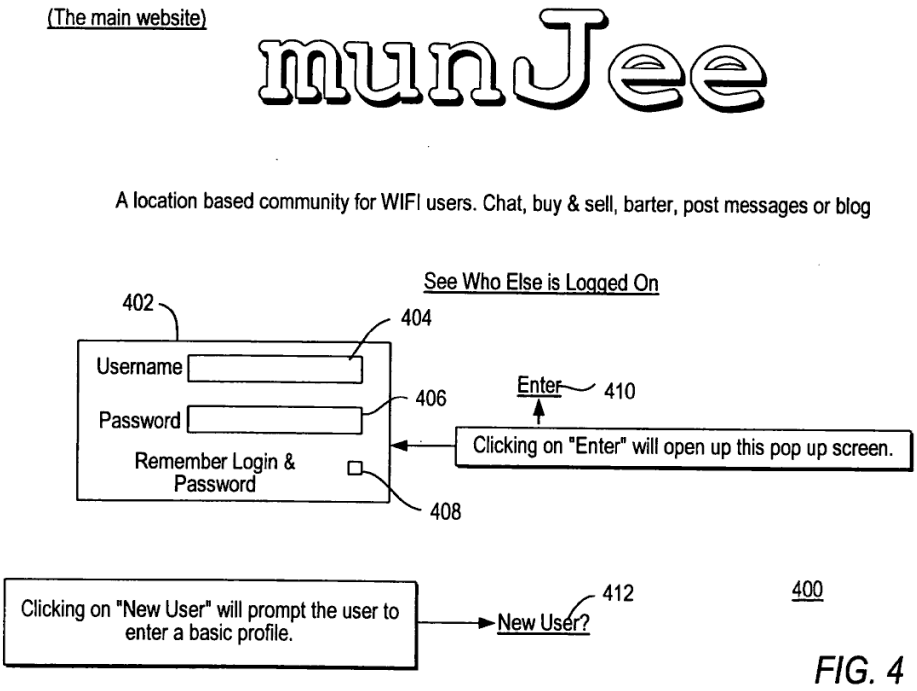
with the content server. Xu provides an express motivation to combine by explaining that its privacy and security settings give the user "full control over their own privacies and securities in the global user database. For example, he can choose to sign in anonymously or be invisible to others, whatever mode he chooses." (Xu, 27:32-35.) For example, a user who wishes to remain invisible would only need to make a selection once. Because that information would have stored (for example in a global database), the user need not reset the visibility setting each time the user logs in. This provides a further convenience to the user, and more consistency in application of the user's preferences. It also would have been obvious that a mobile device user in Baig could have logged into the VCSP in Baig multiple times, including through different hotspots/access points at different physical locations. It thus would have been beneficial for the content server to store (and thus be able to apply) the user's visibility preference from one login to the next, as Baig does for other registration information. (Baig, ¶0093 ("As users register online on the VCSP website, profile information about our users, such as age, gender, occupation, interests and the like are requested during the registration process and securely stored by the VCSP **202**."); Baig Provisional, 0022.)

172. An ordinarily skilled artisan would have had at least a reasonable expectation of success. The ability of users to access multiple access points/hotspots

was a built-in capability of conventional WiFi technology. The ability to store the user's visibility preference in Baig, and use it in subsequent logins to the content server, would have been trivially simple to implement using conventional techniques. As noted, Baig explains that the system already stores profile information about users "such as age, gender, occupation, interests and the like are requested during the registration process," which is "securely stored by the VCSP **202**." (Baig, ¶0094; Baig Provisional, 0022.) The ability to further store the visibility selection of the first device user would have involved nothing more than storing an additional value in its user profile.

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

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



(Baig, Fig. 4.)

174. Baig shows a home page **400** that allows the user to "log in for accessing the VCSP website and services." (Baig, ¶0068; Baig Provisional, 0016.) Baig explains that once a user registers and "then logs into the VCSP website on the home page as illustrated in FIG 4, the server **224** presents the web page illustrated in FIG. 6 to the user on his/her mobile device **102**." (Baig, ¶0074; Baig Provisional, 0017.) The web page in Figure 6 is shown below:

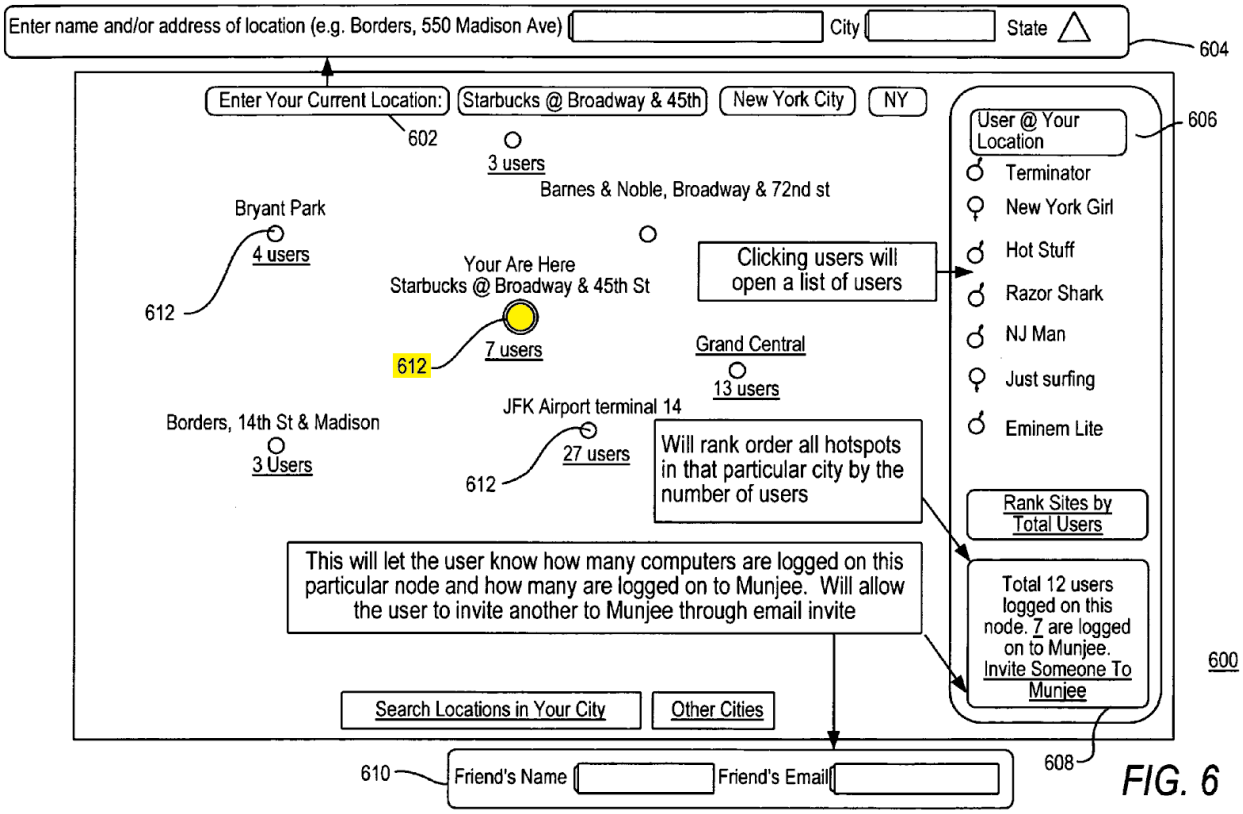


FIG. 6

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

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

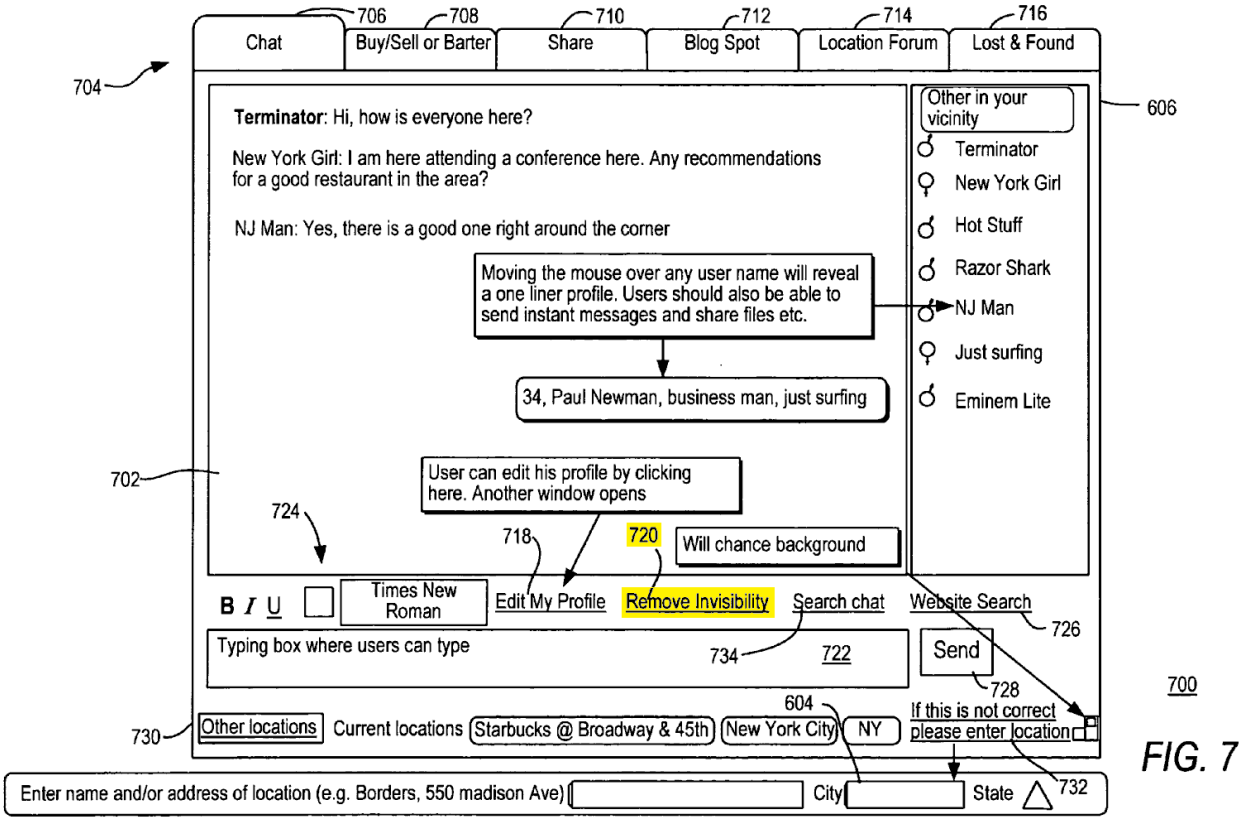


FIG. 7

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

176. Figure 7 shows a web page **700** with a number of options for the selected hotspot, including chat **706**, and also included list **606** identifying users at the current hotspot. As shown in highlighting, the web page also includes a link **720** that allows the user to decide to become visible to other users. (Baig, ¶0081 ("A link **720** can also be provided to remove their concealment (i.e., invisibility) to other users."); Baig Provisional, 0019.) Link **720**, as discussed for claim 1(d), provides the mechanism for collecting behavioral information from the first device user, *i.e.*, the user's decision to become visible to other users.

177. The behavioral information under the proposed combination was therefore collected "**as a result of redirection of the first device from an online site visited by the first device**," under at least two theories. First, as the sequence discussed above makes clear, the user was only able to reach web page **700** of Figure 7 – which allowed the user to specify their visibility preference – as a result of being redirected from the VCSP website ("**an online site visited by the first device**"), first from the login page **400** (Fig. 4) to web page **600** (Fig. 6), and then from web page **600** (Fig. 6) to web page **700** (Fig. 7). In each of these cases, the user's web browser was redirected from one page to another. These redirections, either individually or collectively, qualify as "**redirection of the first device from an online site visited by the first device**," and the behavioral information was collected "**as a result of**" either of both of these redirections because redirection was an essential step in the causal chain allowing the user to access web page **700** and thus activate link **720**. Stated differently, but for the redirection in Baig, the behavioral information would not have been collected because the user would not have been able to activate link **720**, and thus, the content server would not be able to collect and store and retain the user's visibility selection. The behavioral information was also collected "**while the first device is not connected to the LAN**," because as explained in the scenario described for claim 3, it would have been collected when

the first device user was logged into the content server from a previous and different access point/hotspot, *i.e.*, an earlier LAN different from the current LAN mapped to the "**the LAN**" as claimed. As explained previously, under the combination with Xu, the user's visibility setting would have been saved and thus applicable when the first device later connected to "**the LAN**" through the current access point **106** and logged into the content server from that network.

178. As a second and alternative way to find the claimed "**redirection**," Baig describes the option to remove the user's concealment as "**link 720**," which appears on the webpage **700** in Figure 7 above in underlining typical of conventional web hyperlinks. As was well-known to ordinarily skilled artisans, a "link" in the context of a webpage refers to a user interface option associated with a URL that the browser web accesses if the user activates the link. (Hahn, 0035 ("A nice way to think about links is to imagine that underneath each link lies a URL. Thus, each time you select a link, it is as if your browser looks under the link, finds the URL, and does whatever is necessary to fetch the information to which the URL points.").) In this case, when the mobile device user in Baig clicks on link **720** on web page **700**, this causes "**a redirection**" of the browser to a URL associated with the link, which informs the server that the user has changed their visibility setting. The behavioral information was thus collected "**as a result of**" the redirection in this instance because it was the

redirection via the URL associated with link **720** that notified the server of the user action to change their visibility preference.

179. Finally, I note that it appears that each of the web pages described above (*i.e.* **400** (Fig. 4), **600** (Fig. 6), **700** (Fig. 7)) is part of the VSCP website provided by the content server. But nothing in claim 4 requires redirection to a different website; the claim only specifies redirection "**from an online site**," and does not place limits on the redirected-to site. Moreover, nothing in the term "**redirection**" requires different sites; in fact redirection was a basic and fundamental feature of web programming in which a web page could cause the user's browser to redirect to another address identified by any arbitrary URL, which could have pointed to a web page on the same or different website. In fact, it was common for websites to redirect users to different pages within the same website (and sometimes the same page to cause reloading of the page), similar to the examples in Baig above.

3. Claims 15-16

180. Claims 15-16 are substantially similar to claims 3-4, addressed above as shown in the table below (common language shown in underlining):

Claim 3	Claim 15
3. The method of claim **2** wherein the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via	15. The computer system of claim **14** wherein the computer system is programmed to utilize in part (d) of the method user profile information

the first device at a time when the first device is not connected to the LAN.	associated with the device identifier that comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN.
Claim 4	**Claim 16**
4. The method of claim **3** wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN.	16. The computer system of claim **15** wherein the computer system is programmed to receive the behavioral data collected via the first device as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN.

181. As shown, other than minor rearranging of language from claims 3-4 for corresponding computer system claims 15-16, there are no material differences. Claims 15-16 are therefore obvious for the same reasons as claims 3-4.

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

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

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

182. Claims 6 and 7 are closely related and thus will be discussed together. Baig discloses a vicinity-based community service that includes, in addition to the

features described for **Ground 1**, an advertising service in which advertisers can target advertisements to users at a particular hotspot based on (among other things) demographic information such as age and gender. (Baig, ¶¶0095 ("The VCSP **202** can also provide an option to the advertisers to restrict their ads only to individuals under/over a certain age, or of a certain gender at a particular geographical area."), 0093 ("Advantageously, the advertisers can target the audience of a particular hotspot according to the profile, e.g., age/gender etc. of the users and/or a particular time of the day."), Baig Provisional, 0022.) Advertisements are selected based on a competitive bidding system. (Baig, ¶0062; Baig Provisional, 0015.) As Baig further explains, "[t]he winner of the bidding contest receives exclusive rights to advertise on the VCSP website for the selected hotspot at a particular time of day, for example between 6-8 pm to female end-users who are 18-25 years old at a particular location." (Baig, ¶0104; Baig Provisional, 0024.)

183. Baig therefore discloses actions, in addition to the automatic actions described for claim 1, actions further comprising "**selecting an advertisement, from among a plurality of possible advertisements**" (claim 7), and "**causing the selected advertisement to be directed to the second device**" (claim 8), with the "**advertisement**" corresponding to an advertisement selected for delivery to the second device based on a winning bid. The advertisement is selected from "**among**

a plurality of possible advertisements," *i.e.*, the available advertisements including those from other advertisers entities who participated in the bidding contest. The selection is, as noted, is based on user profile information of the second device user, such the users age and/or gender. And as explained for claim 1(d), these actions would have been "**automatic**" because the advertisement would have been selected and delivered to the second device via the automatic website update techniques described in Hahn, as discussed. Alternatively, the advertisement could have been selected and delivered to the second device automatically, as part of the webpage (Figure 6) sent to the second device, upon the second device user logging on to the content server. (Baig, Fig. 6, ¶0074; Baig Provisional, 0017.)

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

185. Gerace discloses a system for targeted advertising based on a "user profile" for an end user, who can include user demographic information. (Gerace, ¶¶0008-0009, 0083, 0062.) A key feature of Gerace, for purposes of claims 6-7, is its ability to deduce demographic information for a user profile (such as age and

gender) even if the user has not provided such information. "When not provided by the user," Gerace explains, "the system may forecast demographic information for a user based on relationships with other users and/or group members," for example, "average age of friends is assumed to be the end-users age, dominant gender of friends is assumed to be gender of the end-user," and so forth. (Gerace, ¶0010.) Gerace further explains:

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

(Gerace, ¶0083.) The user profile, which includes the assumed demographic information, can then be used to target and display adds to the user. (Gerace, ¶0055 ("The present invention forms and maintains user profiles **17** (**FIG**. **2***h*) based on information received from end-users and information deduced by end-user activity as users of system **100**. The present invention employs the user profiles **17** in

targeting ad campaigns.”).)

186. Gerace therefore discloses selecting an advertisement to display to a user based, at least in part, on a portion of the user profile of at least one other user, such as the age or gender of other users detected in the user’s activities.

187. ***Manner, Rationale, and Motivation to Combine (Ground 1 Prior Art with Gerace)***: It would have been obvious to combine the prior art for **Ground 1** with Gerace. The combination would have predictably resulted in the vicinity-based community system of Baig as described for **Ground 1**, with the further ability to select and deliver advertisements to the second device user, “**based at least in part on at least a portion of the user profile information associated with the device identifier of the first device**,” *i.e.*, based at least in part on demographic profile information of the first device user, such as its age and/or gender.

188. For example, if the second device user in Baig did not provide demographic profile information such as age and/or gender, the system in Baig would have deduced this information for the second device user based on the profile information of other users, which could have included at least the first device user based on (among other things) its relationship with the second device user, common activities and behaviors, or simply the fact that the two are connected to the same access point/hotspot. These deduced characteristics, in turn, would have then been

used in selecting advertisements for delivery to the second device based, at least in part, on the age and/or gender profile information of the first device user.

189. I note that, in a real-world implementation of the proposed combination, the profiles of yet additional users (beyond the first user) may have also been used to deduce profile information for the second device user. But this presents no issue for the proposed combination because the claim only requires the selection to be based "**at least in part**" on "**a portion**" of the first device user's profile information, and thus does not preclude the system from also taking profile information of other users into account in deducing demographic characteristics.

190. Gerace is an analogous reference in the same field of Internet-based advertising and would have been reasonably pertinent to problems facing the inventor. For example, Gerace's disclosures would have been pertinent in describing techniques for using user profile information to select advertisements for deliver to a user, including how to use user profile information associated with another user in making the advertisement selection.

191. An ordinarily skilled artisan would have been motivated to combine. To begin with, it would have been obvious to an ordinarily skilled artisan that users of the system of Baig may have felt reluctant to provide their age and/or gender information, and thus may have declined to do so. Baig acknowledges as much by

making clear that, in one embodiment, user entry of age and gender information is an optional for user registration. (Baig, ¶¶0070 & Fig. 4 (showing that registration user entry fields also including Gender field **508** and Age field **514**), 0071 ("Preferably, <u>some or most of the entry fields</u> [for registration] <u>are optional</u>, such that only the user name field **502** and password related fields **504** and **506** are mandatory for registration."), Baig Provisional, 0017.) The techniques in Gerace would thus have provided a clear benefit to the proposed combination by allowing the system of Baig – in those cases where the second device user elected not to provide their age or gender (or both) – to deduce those characteristics and use them in selecting an advertisement for delivery to the second device. And although the deduced age and gender of the second device user may not always be 100% accurate, of course, these deduced characteristics are preferable to having no demographic information at all relating to the second user. When compared to having no information at all about these characteristics, for example, the deduced characteristics would have increased the likelihood of selecting an advertisement for the second device user that was relevant and interesting to that user.

192. An ordinarily skilled artisan would have perceived no technological obstacle to the proposed combination, and would have had more than a reasonable expectation of success. Targeted advertising techniques and techniques for

collecting and using user profile information were already well-known. The underlying technology in Gerace is not complex, and an ordinarily skilled artisan could have implemented the proposed combination, including the disclosures from Gerace discussed above, using conventional techniques and without undue experimentation.

3. Claims 17-18

193. Claims 17-18 are substantially similar to claims 6-7, addressed above as shown in the table below (common language shown in underlining):

Claim 6	Claim 17
6. The method of claim **1** wherein the automatic action comprises selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device.	17. The computer system of claim **13** wherein the automatic action that the computer system is programmed to take comprises selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device.
Claim 7	**Claim 18**
7. The method of claim **6** wherein the automatic action comprises causing the selected advertisement to be directed to the second device.	18. The computer system of claim **17** wherein the automatic action that the computer system is programmed to take comprises causing the selected advertisement to be directed to the second device.

194. As shown, other than minor rearranging of language from claims 6-7 for corresponding computer system claims 17-18, there are no material differences.

Claims 17-18 are therefore obvious for the same reasons as claims 6-7.

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

1. Claim 11: "The method of claim 1 wherein"

195. Claim 11 is little more than an amalgam of limitations recited in other dependent claims addressed above, including claims 2-7 and 10. Accordingly, claim 11 is obvious based on the same grounds applicable to those claims.

(a) "(i) the first device comprises a mobile device that is connected to the LAN only intermittently,"

196. Claim 11(i) is substantially identical to claim 2, and thus, would have been obvious for the same reasons based on **Ground 1**.

(b) "(ii) the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN,

197. Claim 11(ii) is substantially identical to claim 3, and thus, would have been obvious for the same reasons based on **Ground 2**.

(c) "(iii) wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN, and"

198. Claim 11(iii) is substantially identical to claim 4, and thus, would have been obvious for the same reasons.

(d) "(iv) the automatic action comprises (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device."

199. Claim 11(iv) is substantially identical to claims 6 and 7, and thus, would have been obvious for the same reasons based on **Ground 3**.

2. Claim 12: "The method of claim 11 wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device."

200. As explained for claim 10, the device identifiers under the proposed combination contain no personally identifiable information pertaining to any user.

3. Claims 20-21 and 23

201. Claims 20-21 and 23 are substantially similar to claims 11-12 discussed above, except that they depend from a different independent claim as shown below (with common language shown in underlining):

Claim 11	Claim 20
11. <u>The</u> method <u>of claim</u> **1** <u>wherein</u> (i) <u>the first device comprises a mobile device that is connected to the LAN only intermittently</u>, (ii) <u>the user profile information associated with the device identifier</u> <u>utilized</u> <u>in part (d)</u> <u>comprises behavioral data collected via the first device at a time when the first device is</u>	20. <u>The</u> computer system <u>of claim</u> **13** (i) <u>wherein</u> the computer system is programmed to perform the method even when <u>the first device comprises a mobile device that is connected to the LAN only intermittently</u>; (ii) wherein the computer system is programmed to <u>utilize in part (d)</u> of the method <u>user</u>

not connected to the LAN, (iii) wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN, and (iv) the automatic action comprises (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device.	profile information associated with the device identifier that comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN; (iii) wherein the computer system is programmed to receive the behavioral data collected via the first device as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN; and (iv) wherein the automatic action that the computer system is programmed to take comprises (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device.
Claim 12	**Claim 21**
12. The method of claim **11** wherein the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device.	21. The computer system of claim **20** wherein the computer system is programmed to perform the method even when the device identifiers of the first device and the second device include no personally identifiable information pertaining to a user of the first device or the second device.
Claim 11	**Claim 23**
11. The method of claim **1** wherein	23. The article of claim **22** wherein the computer-readable instructions further cause the computer system

(i) the first device comprises a mobile device that is connected to the LAN only intermittently,	(i) to perform the method even when the first device comprises a mobile device that is connected to the LAN only intermittently;
(ii) the user profile information associated with the device identifier utilized in part (d) comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN,	(ii) to utilize in part (d) of the method user profile information associated with the device identifier that comprises behavioral data collected via the first device at a time when the first device is not connected to the LAN;
(iii) wherein the behavioral data collected via the first device is received at the computer system as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN, and	(iii) to receive the behavioral data collected via the first device as a result of redirection of the first device from an online site visited by the first device while the first device is not connected to the LAN; and
(iv) the automatic action comprises (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device.	(iv) to take automatic action comprising (A) selecting an advertisement, from among a plurality of possible advertisements, based at least in part on at least a portion of the user profile information associated with the device identifier of the first device, and (B) causing the selected advertisement to be directed to the second device.

202. As shown above, the only differences between claims 11-12 and claims 20-21 and 23 are not material, and amount to minor adjustments intended to provide system and article counterparts to claims 11-12. These claims are thus obvious for the same reasons as claims 11-12 provided above.

VI. ENABLEMENT OF THE PRIOR ART

203. My Declaration above has relied upon disclosures from Baig, Laidlaw, Sitaraman, Hahn, Xu, and Gerace, to show that the challenged claims would have been obvious. In my opinion, the disclosures from the prior art that I have cited throughout this Declaration were sufficiently detailed to have enabled an ordinarily skilled artisan to make and use the proposed combination in the manner detailed above, without undue experimentation. For example, with respect to Baig (the primary reference for all grounds), it discloses techniques for identifying and grouping users/devices connected to the same local area network, *i.e.*, by identifying devices connecting through a common IP address, and providing online services to users in those groups. These techniques do not involve new or complex technologies, but rather, rely on existing technologies that were widely used and understood. For example, the ability to use IP addresses to identify devices was well-known decades before the April 2007 priority date. There was also a wealth of publicly-available information about how to implement networking technologies using IP addresses, including Request for Comment (RFC) documents, freely-available source code for networking protocols and applications, among other resources. The techniques from Baig that I cite in my Declaration could have been implemented using conventional programming techniques.

204. With respect to Laidlaw and Sitaraman, which I have cited for basic techniques of storing session information and dynamically-assigned IP addresses (including DHCP), which were also well-known long before April 2007. Indeed, the portions of Sitaraman (filed in 1998) cited above come from its "Background" discussion of the prior art. An ordinarily skilled artisan could have implemented the techniques discussed in Laidlaw and Sitaraman, including session management and DHCP, using conventional programming techniques.

205. With respect to Hahn, as I explained in connection with claim 1(d), the automatic web page update techniques in Hahn were already well-known by the time Hahn was published in 1996, and thus would have been considered entirely trivial by April 2007. For example, the industry standard for the Hypertext Markup Language (HTML), the language used to encode webpages, provided a specific "refresh" metatag for specifying a timing interval (such as every 10 seconds) in which the webpage will be automatically reloaded. An ordinarily skilled artisan could have implemented the automatic web page update techniques discussed in Hahn using conventional programming techniques.

206. And with respect to Xu and Gerace, which I have cited for certain dependent claims, the relied-upon disclosures could also have been readily implemented by an ordinarily skilled artisan. My Declaration relies on Xu for the

unremarkable proposition that it would have been obvious to store a user's visibility preference (for example as part of the user's stored profile information), which would have been trivially easy to implement. My Declaration cites Gerace for techniques of assuming or deducing profile information for a user based, among other things, on activities of other users. These techniques could likewise have been implemented using known programming techniques. Accordingly, with respect to each of the prior art combinations set forth in Grounds 1-4, the disclosures in the prior art references were sufficiently detailed, in light of the knowledge of an ordinarily skilled artisan, to have enabled an ordinarily skilled artisan to make and use the proposed combinations without undue experimentation. For the same reason, as I have explained throughout this Declaration, an ordinarily skilled artisan would have had at least a reasonable expectation of success in making and using the proposed combinations in the manner described in my Declaration.

VII. NO SECONDARY CONSIDERATIONS OF NONOBVIOUSNESS

207. As explained in **Part III.B**, I understand that "secondary considerations" may be used as indicia of nonobviousness, provided that any such consideration has a nexus to the invention claimed. I understand from Petitioner's counsel that Patent Owner in the related district court litigation has not yet identified any evidence related to secondary considerations with a nexus to the claimed

invention. Nor am I aware of information, such as commercial success, unexplained results, long felt but unsolved need, industry acclaim, simultaneous invention, copying by others, skepticism by experts in the field, and failure of others, suggesting that the claims addressed in this Declaration are not obvious. To the extent Patent Owner later provides information it claims relates to secondary considerations, I reserve the right to supplement my analysis and opinions to comment on it.

VIII. CONCLUSION

208. In signing this Declaration, I recognize that the Declaration will be filed as evidence in a contested case before the Patent Trial and Appeal Board of the United States Patent and Trademark Office. I also recognize that I may be subject to cross-examination in this proceeding. If required, I will appear for cross-examination at the appropriate time. I reserve the right to offer opinions relevant to the invalidity of the challenged claims and/or offer testimony in support of this Declaration.

209. I hereby declare that all statements made herein of my own knowledge are true and that all statements are made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001.

Dated: August 4, 2023

Respectfully submitted,

Christopher M. Schmandt
Winchester, MA

EXHIBIT A

Christopher Schmandt
4 Longfellow
Winchester, MA 01890
+1-617-230-4257

Education

M.I.T., Master of Science, Visual Studies (Computer Graphics), 1980

M.I.T., Bachelor of Science, Computer Science, 1978

Professional Experience -- MIT

Media Laboratory, Principal Research Scientist, 1985-2018 (retired)
Director, Living Mobile Research Group (formerly Speech + Mobility)

Architecture Machine Group, Research Associate, 1980-1984

Architecture Machine Group, Research Assistant, 1979-1980

Architecture Machine Group, Graphics Programmer, 1977-1979

Departmental Undergraduate Research Opportunities Program Coordinator, 1984-2018

Laboratory Intellectual Property Committee 2001-2016, chair 2002-2009

Departmental Committee on Graduate Studies, 1996-2001, 2007-2018

Sponsored Research Activities

Alerting and Mobile Messaging, Digital Life Consortium, MIT Media Lab, 1997-2018

Acoustical Cues to Discourse Structure, National Science Foundation, Principal Investigator, 1995-1998

Parsing Radio, News in the Future Consortium, MIT Media Lab, 1993-1999

Desktop Audio, SUN Microsystems, Inc., Principal Investigator, 1989-1996

Voice Interaction in Hand Held Computers, Apple Computer, Principal Investigator, 1991-1993

Voice Interfaces for Network Services, AT&T, Principal Investigator, 1989-1991

Back Seat Driver, NEC, Principal Investigator, 1988-1991

Acoustic and Visual Cues for Speech Recognition, DARPA, co-Principal Investigator, 1986-1988

Personal Computers and Telephony, NTT Public Corporation, Principal Investigator, 1984-1989

Home Telecomputing, Atari, Inc., Principal Investigator, 1983

Testifying legal engagments within the last five years, representing party in italics

- *Microsoft* v. SpeakWare, 2019
- *Bumble Trading LLC* v. Match Group LLC, 2019
- *Tile Inc.* v. Cellwitch Inc, 2019
- Blackberry Ltd v. *Facebook, Inc* 2020
- *EROAD Ltd* v. PerDiem Co, 2020
- *Snap Inc.* v. SRK Technology LLC, 2020
- *Shopify Inc* Ltd v. Express Mobile Inc, 2020
- Express Mobile Inc, v *Wix Ltd* 2020
- *Motorola Mobility LLC* v. Ironworks patents, LLC. 2021
- Express Mobile Inc, v *GoDaddy Inc* 2021
- *Bumble Trading LLC* v. Kinectus, LLC. 2021
- *Tile, Inc* v. Linquet Technologies, Inc. 2021
- *Facebook, Inc.* v. Palo Alto Research Center, Inc. 2021
- *Unified Patents, LLC* v.Gesture Technology Partners, LLC. 2021
- Quantum Metric, Inc v.*Content Square Isreal, Ltd.* 2021
- *Meta Platforms Inc.* v.AlmondNet, Inc 2022
- *Apple Inc.* v.Zentian Limited 2022
- *Google LLC* v. Mira Advanced Technoogy Systems Inc 2022
- *Google LLC and Youtube LLC* v. Robocast, Inc 2023
- *Google LLC* v. Adnexus 2023

Professional Experience -- Intellectual Property

Co-inventor on U.S. Patents

- 5,177,685 for "Automobile navigation system using real time spoken driving instructions"
- 6,728,348 for "System for storing voice recognizable identifiers using a limited input device such as a telephone key pad"
- 6,937,986 for "Automatic dynamic speech recognition vocabulary based on external sources of information"
- 7,098,776 for "Methods and apparatus for vibrotactile communication"
- 7,392,280 for "Method for summarization of threads in electronic mail"
- 7,738,637 "Interactive voice message retrieval"
- 7,443,283 for "Methods and apparatus for connecting an intimate group by exchanging awareness cues and text, voice instant messages, and two-way voice communications"
- 7,865,560 for "System for summarization of threads in electronic mail"
- 8,121,653 for "Methods and apparatus for autonomously managing communications using an intelligent intermediary"
- 8,135,128 for "Animatronic creatures that act as intermediaries between human users and a telephone system"

Co-inventor on U.S. Patent Applications

- 20020076009 "International dialing using spoken commands"
- 20030023688 "Voice-based message sorting and retrieval method"
- 20030081738 "Method and apparatus for improving access to numerical information in voice messages"
- 20030144846 "Method and system for modifying the behavior of an application based upon the application's grammar"
- 20030158903 "Calendar bar interface for electronic mail interaction"

Publications
Most publications can be found at http://www.media.mit.edu/speech/publications
or http://living.media.mit.edu/publications

Field Study of a Tactile Sound Awareness Device for Deaf and Hard of Hearin Users ISWC 2020. (with D. Jain, B. Chiu, S. Goodman, L. Findlater, J. Froehlich)

SkinMorph: Texture-Tunable On-Skin Interface Through Thin, Programmable Gel ISWC 2018. (with Cindy Kao, M. Banforth, D. Kim)

Technical Interventions to Detect, Communicate, and Deter Sexual Assault. ISWC 2017. (with Manisha Mohan)

Exploring Interactions and Perceptions of Kinetic Wearables. DIS 2017. (with Cindy Hsin-Liu Kao, D. Ajilo, O. Anilionyte, A. Dementyev, I. Choi and S. Follmer)

Leveraging User-made Predictions to Help Understand Personal Behavior. MobileHCI 2017. (with Miriam Greis, Tilman Dangler and Albrecht Schmidt)

Rovables: On-Body Robots as Mobile Wearables. UIST 2016. (with Cindy Hsin-Liu Kao, A. Dementyev, I. Choi, D. Ajilo, M. Xu, and S. Follmer)

DuoSkin: Rapidly Prototyping On-Skin User Interfaces Using Skin-Friendly Materials. ISWC 2016. (with Cindy Hsin-Liu Kao, Christian Holz, Asta Roseway, and Andres Calvo)

Immersive Terrestrial Scuba Diving Using Virtual Reality (with Dhruv Jain, Misha Sra, Jingru Go, Rodrigo Margues, Raymond Wu and Justin Chiu) Proceedings, UIST 2016

Expanding social mobile games beyond the device screen (with Misha Sra) Journal of Personal and Ubiquitous Computing, 2015

NailO: Fingernails as an input surface (with Cindy Hsin-Liu Kao, Artem Dementyev, Joseph Paradiso) CHI 2015

Mugshots: A mug display for front and back stage social interaction in the workplace (with Cindy Hsin-Liu Kao) TEI (Tangible and Embedded Interfaces) 2015

Mime: compact, low power 3D gesture sensing for interactionwith head mounted displays (with Andrea Colaco, Ahmend Kirmani, Hye Soo Yang, Nan-Wei Gong, and Vivek Goyal) Proceedings of UIST 2013.

Spotz: A location-based approach to self-awareness (with Misha Sra) Proceedings of Persuasive 2013.

Setting the stage for interaction: A tablet application to augment group discussion in a seminar class (with Drew Harry and Eric Gordon) Proceedings of CSCW 2012.

Indoor Location Sensing using Geo-Magnetism (with Jaewoo Chung, Matt Donahoe, Ig-Jae Kim, Pedram Razavai and Micaela Wiseman) Proceedings of International Conference on Mobile Systems, Applications, and Services (Mobisys) 2011.

My second bike: a TV-enabled social and interactive riding experience (with Jaewoo Chung, Kuang Xu, Andrea Colaco, and Victor Li) Proceedings of IEEE Communications and Networking Conference, Jan 2010.

Going my way?: User-aware route planner (with Jaewoo Chung) Proceedings CHI 2009.

Globetoddler: Designing for remote interataction between preschoolers and their traveling parents (with Paulina Modlitba) CHI 2008 Extended Abstracts

Are we there yet? - a temporally aware media player (with Matt Adcock and Jaewoo Chung), Australian User Interface Conference (AUIC) 2008

Physical embodiments for mobile communication agents (with Stefan Marti), UIST 2005

Giving the caller the finger: collaborative responsibility for cellphone interruptions (with Stefan Marti) Extended Abstracts, CHI 2005

Active Messenger: email filtering and delivery in a heterogeneous network (with Stefan Marti) Human-Computer Interaction Journal (HCI) Volume 20 (2005)

WatchMe: communication and awareness between members of a closely-knit group (with Natalia Marmasse) Proceedings of Ubicomp 2004

An audio-based personal memoroy aid (with S. Vemuri, W. Bender, S.Tellex and B. Lassey) Proceedings of Ubicomp 2004

Improving speech playback using time-compression and speech recognition (with Sunil Vemuri, Philip DeCamp, and Walter Bender) Proceedings of CHI 2004

Impromptu: managing networked audio applications for mobile users (with Kwan Lee, Jang Kim, and Mark Ackerman), Proceedings of MobiSys 2004

TalkBack: a conversational answering machine (with Vidya Lakshmipathy and Natalia Marmasse) Proceedings of UIST 2003

``ListenIn'' to domestic environments from remote locations (with Gerardo Vallejo) Proceedings of the 2003 International Conference on Auditory Display (ICAD)

Safe & Sound: a wireless leash (with Natalia Marmasse) Extended Abstracts, Proceedings of CHI 2003

Mediated voice communication via mobile IP (with Jang Kim, Kwan Lee, Gerardo Vallejo, and Mark Ackerman), Proceedings of UIST 2002.

The Audio Notebook: Paper and pen interaction with structured speech (with Lisa Stifelman and Barry Arons), Proceedings of CHI 2001

Synthetic News Radio (with Keith Emnett) IBM Systems Journal, Vol. 39 Nos. 3-4, pp. 646-659, 2000.

Everywhere messaging (with Natalia Marmasse, Stefan Marti, Nitin Sawhney, and Sean Wheeler) IBM Systems Journal, Vol. 39 Nos. 3-4, pp. 660-677, 2000.

Location-aware information delivery wth comMotion (with Natalia Marmasse), Proceedings of the Second International Symposium on Handheld and Ubiquitous Computing, pp. 157-171, Springer, 2000.

Nomadic Radio: Scalable and contextual notification for wearable audio messaging (with Nitin Sawhney), Proceedings of CHI 1999.

Speaking and listening on the run: Design for wearable audio computing (with Nitin Sawhney), Proceedings of International Symposium on Wearable Computing, 1998.

Audio Hallway: A virtual acoustic environment for browsing, Proceedings of UIST 1998.

Dynamic Soundscape: Mapping time to space for audio browsing (with Minoru Kobayashi), Proceedings of CHI 1997.

CLUES: Dynamic personalized message filtering (with Matt Marx), Proceedings of CSCW 1996.

Using acoustic structure in a hand-held audio playback device (with Deb Roy), IBM Systems Journal, Vol 35, Nos. 3 and 4, 1996.

Mailcall: Message presentation and navigation in a nonvisual environment (with Matt Marx), Proceedings of CHI 1996

AudioStreamer: Exploiting simultaneity for listening (with Atty Mullins), short paper, CHI 1995.

Multimedia momadic services on today's hardware, IEEE Network, September/October 1994.

Putting people first: Specifying proper names in speech interfaces (with Matt Marx), proceedings of UIST 1994.

Chatter: A conversational learning speech interface (with E. Ly) AAAI Workshop on Intelligent Multi-Media Multi-Modal Systems, 1994.

Voice Communication with Computers: Conversational Systems. New York: Van Nostrand Reinhold. 1994.

Capturing, structuring, and representing ubiquitous audio (with D. Hindus and C. Horner), ACM Transactions on Information Systems, Vol. 11, No. 4, October 1993.

Speech Recognition Architectures for Multimedia Environments, (with E. Ly and B. Arons), Proceedings of the 1993 AVIOS Conference, September 1993.

Phoneshell: the Telephone as Computer Terminal, Proceedings of the ACM Multimedia Conference, August 1993.

Voicenotes: A Speech Interface for a Hand-Held Voice Notetaker (with L. Stifelman, B. Arons, and E. Hulteen), Proceedings of INTERCHI'93, April 1993.

From Desktop Audio to Mobile Access: Opportunities for Voice in Computing, book chapter in Advances in Human-Computer Interaction, Vol. 4, H.R. Hartson and D. Hix editors. 1992.

Ubiquitous Audio: Capturing Spontaneous Collaboration (with D. Hindus), Proceedings of CSCW'92, November 1992.

Integrating Audio and Telephony in a Distributed Workstation Environment (with S. Angebranndt, R. Hyde, D. Luong, and N. Siravara), Proceedings of the Summer 1991 USENIX Conference, June 1991.

Augmenting a Window System with Speech Input (with M. Ackerman and D. Hindus), Computer, IEEE Computer Society, Vol. 23, No. 8, August 1990.

Observations on Using Speech Input for Window Navigation (with D. Hindus, M. Ackerman, and S. Manandhar), Proceedings, Human-Computer Interaction, Interact '90, IFIP, August 1990.

Phonetool: Integrating Telephones and Workstations (with S. Casner), Proceedings, GLOBECOM '89, IEEE Communications Society, November 1989.

Desktop Audio (with B. Arons), UNIX Review, October 1989.

Synthetic Speech for Real Time Direction-Giving (with J. Davis), IEEE Transactions on Consumer Electronics, IEEE, September 1989.

The Back Seat Driver: Real Time Spoken Driving Instructions (with J. Davis), Proceedings, IEEE Vehicle Navigation and Information Systems Conference, IEEE, Toronto, Canada, September 1989.

An Audio and Telephone Server for Multi-media Workstations (with M. McKenna), Proceedings, Second IEEE Conference on Workstations, IEEE, Palo Alto, CA., 1988.

Employing Voice Back Channels to Facilitate Audio Document Retrieval, Proceedings, ACM Conference on Office Information Systems (COIS), Santa Clara, CA, 1988.

Conversational Telecommunications Environments, Proceedings, Second International Conference on Human-Computer Interaction, 1987.

Understanding Speech Without Recognizing Words, Proceedings, American Voice Input/Output Society Conference, AVIOS, 1987.

A Robust Parser and Dialog Generator for a Conversational Office System (with B. Arons and C. Simmons), Proceedings, American Voice Input/Output Society Conference, AVIOS, Palo Alto, CA, 1987.

Integrated Messages and Network Services for a Personal Workstation, IEEE Workshop on Telematics and Message Handling Systems, IEEE, 1986.

Voice Interaction in an Integrated Office and Telecommunications Environment, Proceedings, American Voice Input/Output Society Conference, AVIOS, San Francisco, CA, 1985.

Voice Communication with Computers, book chapter in Advances in Human-Computer Interaction, H. R. Hartson ed., 1985.

Speech Synthesis Gives Voiced Access to an Electronic Mail System, Speech Technology, Vol. 2, No. 3, Aug/Sept 1984.

A Conversational Telephone Messaging System (with B. Arons), IEEE Transactions on Consumer Electronics, IEEE, Vol CE-30, August 1984.

Phone Slave: A Graphical Telecommunications Interface (with B. Arons), Proceedings, Society for Information Display International Symposium, SID, San Francisco, CA, June 1984.

Input/Display Registration in a Stereoscopic Workstation, Displays, April 1984.

Remote Access to Voice and Text Messages, Proceedings, American Voice Input/Output Society Conference, AVIOS, Washington D.C., 1984.

Fuzzy Fonts: Analog Models Improve Digital Text Quality, Proceedings, National Computer Graphics Association Conference, Chicago, IL, 1983.

Greyscale Fonts Designed From Video Signal Analysis, Society of Applied Learning Technology, Houston, TX, 1983.

Spatial Input/Display Correspondence in a Stereoscopic Computer Graphic Work Station, Proceedings, ACM/SIGGRAPH, Detroit, MI, 1983.

A Programmable Virtual Vocabulary Speech Processing Peripheral (with W. Bender), Proceedings, American Voice Input/Output Society Conference on Voice Data Entry Systems Applications, AVIOS, 1983.

The Intelligent Voice Interactive Interface (with E. A. Hulteen), Proceedings, Human Factors in Computer Systems, National Bureau of Standards/ACM, Gaithersburg, MD, 1982.

Interactive Three-Dimensional Computer Space, Proceedings, SPIE Conference on Processing and Display of Three-Dimensional Data, SPIE, San Diego, CA, 1982, Vol. 367.

Speech Communications, a Systems' Approach, Proceedings, American Voice Input/Output Society Conference on Entry Systems Applications, 1982.

Voice Interaction: Putting Intelligence into the Interface, Proceedings, IEEE International Conference on Cybernetics and Society, IEEE, Seattle, WA, 1982.

The Intelligent Ear: A Graphical Interface to Digital Audio, Proceedings, IEEE International Conference on Cybernetics and Society, IEEE, Atlanta, GA, 1981.

Soft Typography, Information Processing 1980, IFIPS, S. Lavington ed., North-Holland Publishing Co., 1980.