UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CELLCO PARTNERSHIP D/B/A
VERIZON WIRELESS
Petitioner,

v.

BRIDGE AND POST, INC.,
Patent Owner

Case IPR2018-00321
Patent No. 9,659,314

PATENT OWNER'S NOTICE OF APPEAL

Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

Notice is hereby given, pursuant to 37 C.F.R. § 90.2(a)(1), that Patent Owner Bridge and Post, Inc. ("Patent Owner" or "Bridge and Post") hereby timely appeals under 35 U.S.C. §§ 141, 142, and 319 to the United States Court of Appeals for the Federal Circuit from the Final Written Decision entered on June 19, 2019 (Paper No. 27), and from all underlying orders, decisions, rulings, and opinions.

In accordance with 37 C.F.R. § 90.2(a)(3)(ii), Bridge and Posts states that the issues for appeal include, but are not limited to: (i) whether the Board erred in finding that claims 1–21 of U.S. Patent No. 9,659,314 (the "'314 patent") were unpatentable under 35 U.S.C. § 103; (ii) the Board's claim constructions or failure to construe any terms; (iii) any findings or determinations supporting or related to the aforementioned issues as well as other issues decided adversely to Patent Owner in any order, decisions, rulings, or opinions.

A copy of the Final Written Decision is attached hereto.

Simultaneous with this submission, a copy of this Notice of Appeal is being filed with the Patent Trial and Appeal Board. In addition, a copy is being

electronically filed with the Clerk's Office for the United States Court of Appeals for the Federal Circuit (via CM/ECF), along with the required docketing fee.

Furthermore, a copy of this Notice of Appeal is being served on Petitioners Cellco Partnership D/B/A Verizon Wireless.

Dated: August 21, 2019

Respectfully submitted,

By */Lauren N. Robinson/*

Lauren N. Robinson, Lead Counsel
Reg. No. 74,404
Denise M. De Mory
(*Pro Hac Vice*)
Christina M. Finn
(*Pro Hac Vice*)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-351-7248
Facsimile: 415-426-4744
lrobinson@bdiplaw.com
ddemory@bdiplaw.com
cfinn@bdiplaw.com

Attorneys For Patent Owner

CERTIFICATE OF SERVICE

The undersigned hereby certifies that, in addition to being filed electronically through the Patent Trial and Appeal Board's End to End System (PTAB E2E), the foregoing PATENT OWNER'S NOTICE OF APPEAL was served by Express Mail, tracking number EE 117669049 US, August 21, 2019, with the Director of the United States Patent and Trademark Office, at the following address:

Office of the General Counsel
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, Virginia 22313-1450

In addition, the undersigned certifies that a copy of the foregoing Notice of Appeal, along with the required docket fee, was filed on August 21, 2019, with the Clerk's Office for the United States Court of Appeals for the Federal Circuit through the Court's CM/ECF filing system.

The undersigned certifies pursuant to 37 C.F.R. § 42.6(e) that a true copy of the foregoing PATENT OWNER'S NOTICE OF APPEAL has been served in its entirety on August 21, 2019, by electronic mail on the Petitioners via its attorneys of record:

Jay I. Alexander
jalexander@cov.com

Peter P. Chen
pchen@cov.com

Verizon-BridgePost-IPR@cov.com

By */Lauren N. Robinson/*
Lauren N. Robinson, Lead Counsel
Reg. No. 74,404
Denise M. De Mory
(*Pro Hac Vice*)
Christina M. Finn
(*Pro Hac Vice*)
BUNSOW DE MORY LLP
701 El Camino Real
Redwood City, CA 94063
Telephone: 650-351-7248
Facsimile: 415-426-4744
lrobinson@bdiplaw.com
ddemory@bdiplaw.com
cfinn@bdiplaw.com

Attorneys For Patent Owner

Trials@uspto.gov
Tel: 571-272-7822

Paper 27
Entered: June 19, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CELLCO PARTNERSHIP D/B/A
VERIZON WIRELESS
Petitioner,

v.

BRIDGE AND POST, INC.,
Patent Owner.

Case IPR2018-00321
Patent 9,659,314 B2

Before JONI Y. CHANG, BARBARA A. PARVIS, and KEVIN C. TROCK, *Administrative Patent Judges*.

TROCK, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. § 318(a) and 37 C.F.R. § 42.73

I. INTRODUCTION

Cellco Partnership d/b/a Verizon Wireless ("Petitioner") filed a request for *inter partes* review of claims 1–21 (the "challenged claims") of U.S. Patent No. 9,659,314 B2 (Ex. 1001, "the '314 patent"). Paper 1 ("Pet."). Bridge and Post, Inc. ("Patent Owner") filed a Preliminary Response. Paper 6 ("Prelim. Resp."). We instituted *inter partes* review of all the challenged claims and all the grounds raised in the Petition. Paper 7.

Patent Owner filed a Response (Paper 11, "Resp.") and Petitioner filed a Reply (Paper 19, "Reply"). A hearing was held on March 8, 2019, a transcript of which has been entered into the record. Paper 26 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6(b). This Final Written Decision is issued pursuant to 35 U.S.C. § 318(a). We base our decision on the preponderance of the evidence. 35 U.S.C. § 316(e); 37 C.F.R. § 42.1(d). Having reviewed the arguments of the parties and the supporting evidence, we find that Petitioner has demonstrated by a preponderance of the evidence that each of the challenged claims is unpatentable.

A. The '314 Patent[1]

The '314 patent relates to a system and method of tagging network traffic with relevant user demographic and location information for facilitating the delivery of directed media. Ex. 1001, 3:29–32. A tag processing module within a router device coupling a client computer to a destination site served by a server computer intercepts a request from a

[1] The parties both address the priority date of the '314 patent in their briefing. *See* Pet. 11; Resp. 9–12. At the oral hearing, however, the parties agreed that it was not necessary for the Board to address this issue. *See* Tr. 5:7–12, 24:22–25:6.

client computer to a server computer over a network. *Id.* at 3:32–35. The tag processing module determines a unique device identifier corresponding to the client computer, generates a local user identifier for the client computer by performing a one-way hashing operation on the unique device identifier, derives demographic and location (geographic) information for a user of the client computer, generates a request identifier associated with the intercepted request by encrypting the local user identifier, demographic information and geographic location information in an alphanumeric string, and embeds the alphanumeric string in an extensible field of a packet within the request to generate a tagged request identifier. *Id.* at 35–45. The destination site receives the alphanumeric string comprising the tagged request identifier and transmits a request to a tag-related processing service to decode the request identifier. *Id.* at 45–49. In response to the request, the tag-related processing service provides the corresponding location and demographic information to the destination site. *Id.* at 49–51. Using this information, the destination site, or any associated ad partner or other supplemental content provider can serve directed ads or messages through the destination site to the client computer. *Id.* at 51–54.

B. Challenged Claims

Petitioner challenges claims 1–21 of the '314 patent. Claims 1, 20, and 21 are independent and are similar—one principal difference being that claims 20 and 21 recite steps of the claimed method occurring at a server and a network routing device, respectively. Claim 1 is illustrative of the method steps.

> 1. [1.0] A method for improving the selection of media for delivery to a targeted user of a client computing device, comprising:

> [1.1] determining user information for a user;
> [1.2] generating a user identifier for the user from the determined user information;
> [1.3][2] tagging, with a network routing device, network traffic that is bound for a destination site,
> [1.4] the tagging including: generating a request identifier by encrypting the user identifier in an alphanumeric string, and adding the request identifier to the network traffic to generate tagged network traffic;
> [1.5] transmitting the tagged network traffic to the destination site;
> [1.6] receiving from a requester associated with the destination site a decode request to decode the tagged network traffic;
> [1.7] decoding the tagged network traffic to obtain the user identifier;
> [1.8] retrieving stored user information associated with the user identifier; and
> [1.9] transmitting the stored user information to the requester.

Ex. 1001, 17:16–38 (bracketing and numbering added).

C. Applied Evidence

Petitioner relies upon the following references:

(1) International Patent Publication WO 00/73876 A2, Dec. 7, 2000 ("Harada") (Ex. 1004);

(2) International Patent Publication WO 2006/081680, Aug. 10, 2006 ("Roker") (Ex. 1005);

---

[2] Patent Owner's numerical designations and recitations of claim 1's limitations, specifically the subheadings 1.3–1.5 shown on page 27 of the Response, vary from the designations and recitations used in the Petition and the Institution Decision. In this Final Written Decision, for purposes of consistency and clarity, we use the same numerical designations and recitations used in the Petition and the Institution Decision.

(3) U.S. Patent Application Publication No. 2005/0172154 A1, Aug. 4, 2005 ("Short") (Ex. 1006);

(4) International Patent Publication WO 00/67450, Nov. 9, 2000 ("Parekh") (Ex. 1007);

(5) International Publication WO 00/67092, Nov. 9, 2000 ("Mathai") (Ex. 1008); and

(6) Microsoft Product Activation for Windows XP, Nov. 29, 2001 ("Microsoft") (Ex. 1009).

Petitioner also relies on the Declarations of Mr. Stephen Gray. (Exs. 1010, 1037).

Patent Owner relies on the Declaration of Mr. Steve Smoot. (Ex. 2002).

D. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability:

Challenged Claims	**Basis**	**References**
1–7, 10–11, 14–16, 20–21	§ 103(a)	Harada, Roker
12–13	§ 103(a)	Harada, Roker, Short
8–9, 17–18	§ 103(a)	Harada, Roker, Parekh
19	§ 103(a)	Harada, Roker, Mathai
11	§ 103(a)	Harada, Roker, Microsoft

II. DISCUSSION

A. Claim Construction

The instant Petition was filed on December 18, 2017, prior to the effective date of the rule change that replaces the broadest reasonable interpretation ("BRI") standard. *See Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board*, 83 Fed. Reg. 51,340 (Oct. 11, 2018) (final rule) ("This rule is effective on November 13, 2018 and applies to all IPR, PGR and CBM petitions filed on or after the effective date."). We, therefore, apply the BRI standard in this proceeding.

Under this standard, claim terms in an unexpired patent are given their broadest reasonable construction in light of the specification of the patent in which they appear. 37 C.F.R. § 42.100(b) (2017). Claim terms are generally given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007). Only those terms that are in controversy need be construed, and only to the extent necessary to resolve the controversy. *See Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999).

Petitioner does not assert that any claim term in the '314 patent requires construction beyond its plain and ordinary meaning. Pet. 5. Patent Owner concurs. Resp. 9. Nonetheless, Patent Owner raises a claim construction issue implicitly in its argument with respect to limitation 1.9, that the cited references do not teach or suggest "transmitting" under the plain meaning of that term as it would be understood by one of ordinary skill in the art. *See* Resp. 37–40 (citing Ex. 2002 ¶¶ 89–94).

At oral argument, Petitioner's counsel proposed that "transmitting" be construed as "the communication of data between two different entities, but not required to be different pieces of hardware." Tr. 8:20–23. Patent Owner's counsel countered at oral argument that its proposed construction for "transmitting" was "to convey information between entities that are independent and separate by wire or wirelessly." Tr. 25:17–18.

Indeed, Patent Owner's expert, Mr. Smoot, testifies that a person of ordinary skill in the art "would have understood that the plain and ordinary meaning of 'transmitting' is to convey information between entities that are independent and separate by wire or wirelessly," and cites to examples in the '314 patent purportedly showing transmission of stored user information between separate components. Ex. 2002 ¶¶ 89–91.

Petitioner's expert, Mr. Gray, disagrees with Mr. Smoot. Mr. Gray testifies, "a [person of ordinary skill in the art] would have viewed the movement of data within a computer to involve 'transmitting,' as that is how the term has been used in prior art patents." Ex. 1037 ¶ 8 (citing Ex. 1039 ¶ 7; Ex. 1040 ¶ 53). In the context of the '314 patent, Mr. Gray testifies, "a [person of ordinary skill in the art] would not have understood 'transmitting' to exclude communications within a computer or server." *Id.*

Mr. Gray also testifies,

> nothing in the '314 Patent requires "transmitting" to occur between separate components on the network. In fact, the '314 Patent teaches the opposite, because it discloses that the invention "can be implemented through any suitable unitary or distributed combination of hardware, software, and/or firmware." Ex. 1001, 4:47–50, 15:57–16:17. This teaches that rather than requiring separate components on the network, the invention could

> instead be implemented in a "unitary" system, or could be only "software, and/or firmware." Ex. 1001, 4:47–50, 15:57–16:17.

Ex. 1037 ¶ 10.

We must be careful not to read a particular embodiment appearing in the written description into the claim if the claim language is broader than the embodiment. *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993). Although "understanding the claim language may be aided by the explanations contained in the written description, it is important not to import into a claim limitations that are not a part of the claim." *SuperGuide Corp. v. DirecTV Enters., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004).

Here, limitation 1.9 recites, "transmitting the stored user information to the requester." This limitation does not state expressly that the stored user information must move between independent and separate entities or components, only that the "stored user information" be "transmit[ed]" "to the requester." Neither party has pointed to an express definition for "transmitting" in the '314 patent.

The '314 patent does, however, state that, "the components of the system can be implemented through any suitable unitary or distributed combination of hardware, software, and/or firmware." Ex. 1001, 4:47–50. The '314 patent also explains that "[t]hroughout the following description, the terms 'component,' 'module,' or 'process' may be used interchangeably to denote a hardware circuit, software program, or combination hardware/software structure that is configured to perform a particular task." *Id.* at 4:39–43. Based upon this explanation, the term "component," as used by the '314 patent, may indeed refer to a software program.

The '314 patent goes on to state that,

> the systems and methods disclosed herein may be embodied in various forms including, for example, a data processor, such as a computer that also includes a database, digital electronic circuitry, firmware, software, or in combinations of them. Further, while some of the disclosed implementations describe components such as software, systems and methods consistent with the present invention may be implemented with any combination of hardware, software and/or firmware.

Id. at 15:59–67.

Consistent with this expressed flexibility for implementing the claimed invention, the '314 patent specification does not always require the requester associated with the destination site (e.g., a web server) to be a separate component of physical hardware from a tag-related process (TRP) that decodes a request. For example, the specification describes an embodiment in which the web server and the TRP may be co-located on the same computer, even though the TRP is described as a "separate process." *See e.g.*, Ex. 1001, 10:28–41, Fig. 2. Patent Owner's expert, Mr. Smoot, agreed with this understanding at his deposition. *See* Ex. 1038, 21:24–23:15.

Limitation 1.9, as written, is broader than the meaning proposed by Patent Owner, i.e., that "transmitting" means to convey information between entities or components that are independent and separate. Limitation 1.9 is also broader than the examples and embodiments in the '314 patent cited by Mr. Smoot to support his proposed meaning of "transmitting."

Importing a limitation requiring independent and separate entities or components into the claim is not appropriate, especially where, as here, the

'314 patent expressly states that "the components of the system can be implemented through any suitable unitary or distributed combination of hardware, software and/or firmware," and that "[t]he processes disclosed herein are not inherently related to any particular computer, network, architecture, environment, or other apparatus, and may be implemented by a suitable combination of hardware, software, and/or firmware." Ex. 1001, 4:47–50, 16:8–12.

Moreover, patent publications at the relevant time used the term "transmitting" to refer to the movement of data within a computer. *See* Ex. 1037 ¶ 8 (citing Exs. 1039, 1040). Thus, Patent Owner's proposed construction of "transmitting" to require independent and separate entities is inconsistent with the broadest reasonable interpretation of the term in light of the entire disclosure of the '314 patent as would be understood by one of ordinary skill in the art. Accordingly, we decline to adopt Patent Owner's proposed construction of "transmitting." Instead, we adopt Petitioner's proposed construction that a person of ordinary skill in the art reading the claims of the '314 patent in light of the entire specification would understand the term "transmitting" to mean "the communication of data between two different entities, but not required to be two different pieces of hardware."

B. Principles of Law on Obviousness

Section 103(a) forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." In *Graham v. John Deere Co. of Kansas City*, 383

U.S. 1, 13 (1966), the Court set out a framework for applying the statutory language of § 103: under § 103, the scope and content of the prior art are to be determined; differences between the prior art and the claims at issue are to be ascertained; and the level of ordinary skill in the pertinent art resolved.

The Supreme Court has made clear that we apply "an expansive and flexible approach" to the question of obviousness. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 415 (2007). Whether a patent claiming the combination of prior art elements would have been obvious is determined by whether the improvement is more than the predictable use of prior art elements according to their established functions. *Id.* at 417. To reach this conclusion, however, requires more than a mere showing that the prior art includes separate references covering each separate limitation in a claim under examination. *Unigene Labs., Inc. v. Apotex, Inc.*, 655 F.3d 1352, 1360 (Fed. Cir. 2011). Rather, obviousness requires the additional showing that a person of ordinary skill at the time of the invention would have selected and combined those prior art elements in the normal course of research and development to yield the claimed invention. *Id.*

C. Level of Ordinary Skill

In determining whether an invention would have been obvious at the time of the invention, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham*, 383 U.S. at 17. "The importance of resolving the level of ordinary skill in the art lies in the necessity of maintaining objectivity in the obviousness inquiry." *Ryko Mfg. Co. v. Nu-Star, Inc.*, 950 F.2d 714, 718 (Fed. Cir. 1991).

In our Institution Decision, we found that a person of ordinary skill in the art in the field of the '314 patent is a person with a degree in computer or

electrical engineering, computer science, or an equivalent degree, with at least two years of experience in network applications or client-server class computing systems in a web-based environment, and some familiarity with online advertising. Paper 7, 8.

In its Response, Patent Owner argues that a better definition would be "an associate's or bachelor's degree in computer or electrical engineering, computer science, or an equivalent degree, training, or experience, with at least two years of experience in network engineering and network applications engineering in a web-based environment." Resp. 8 (citing Ex. 2002 ¶ 36). Patent Owner argues that its proposed definition "captures that the subject matter of the claims relates to network architecture as well as network applications engineering." *Id.* Petitioner does not address specifically Patent Owner's argument in its Reply.

We are persuaded by Patent Owner's argument concerning the level of ordinary skill in the art. Accordingly, we adopt Patent Owner's proposed description that a person of ordinary skill in the art at the time of the invention would have had an associate's or bachelor's degree in computer or electrical engineering, computer science, or an equivalent degree, training, or experience, with at least two years of experience in network engineering and network applications engineering in a web-based environment.

D. Asserted References

1. Harada (Ex. 1004)

Harada teaches a data transfer method performed at a proxy server, which includes intercepting a data request from a client computer that is directed to a target server, encrypting profile information, augmenting the data request by adding the encrypted profile information to the data request,

and sending the augmented data request to the target server. Ex. 1004, Abstract. Figure 2 of Harada, reproduced below, shows a network.

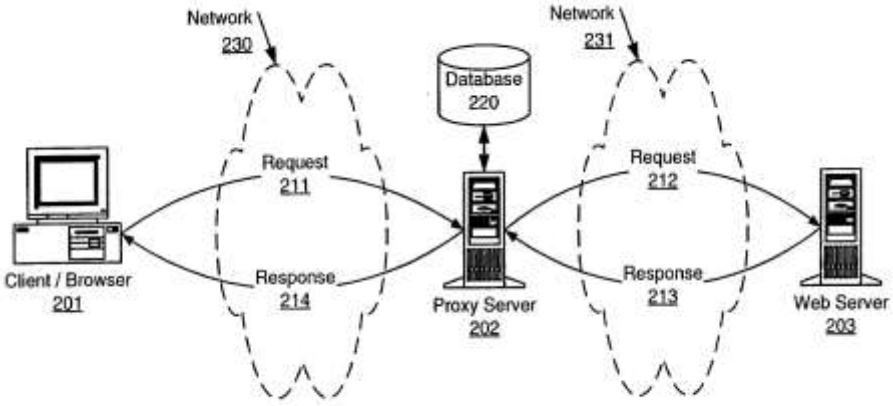

Fig. 2

As shown in Figure 2 of Harada, data request 211 from client 201 to web server 203 is intercepted at proxy server 202. According to Harada, the user profile information is stored first at proxy server 202 in database 220. *Id.* at 5:13−15. When HTTP data request 211 is received by proxy server 202 from client/browser 201, the user profile information from database 220 is encapsulated in request 212 by adding HTTP headers containing the user profile information to the headers received in request 211, and then request 212 is forwarded to web server 203. *Id.* at 5:15−19. The header fields may include encrypted user profile data. *Id.* at 6:25–27. Extraction of user profile data may include decryption of the data so that the extracted user profile data can be used to generate or customize data sent in response to the proxy server for forwarding to a user or client computer. *Id.* at 7:5–8. For example, a tourist information web server may customize a page based on

user profile data specifying a browser user's age and interest. *Id.* at 7:8–9.

2. Roker (Ex. 1005)

Roker teaches a system and method for providing "Internet content that is personalized and therefore more relevant to the individual user." Ex. 1005, 4:11−13. Figure 1 of Roker is shown below.

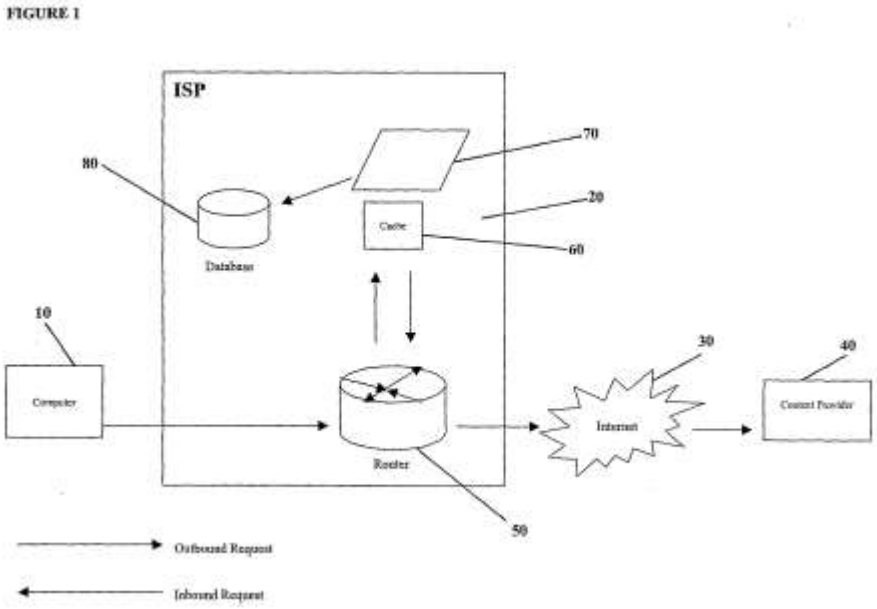

Figure 1 of Roker shows that users operate a browser on computer 10 and use service provider 20 to access Internet 30. *Id.* at 7:18−8:2. Service provider 20 includes router 50 for directing messages between computer 10 and Internet 30, and network device server 70 that accesses database 80 to obtain information about the user of computer 10. *Id.* Database 80 contains personal information about users, such as the user's name, address, billing information, and user preferences. *Id.* at 8:3–5. Network device 70 functions to strategically place "tailored" communications and advertising content into a user's Internet browser. *Id.* at 8:14–16. Network device 70 can collect and interpret user-specific information and encode and encapsulate that information in an outgoing HTTP request, decode

information at the content provider 20's server(s), and select, modify or manufacture content in real-time for presentation to individually targeted users. *Id.* at 8:28–9:3.

The system safely stores personal information about the user and encrypts such information when adding it to an outgoing message. *Id.* at 11:2–7. The system can associate unique subscriber identification of a user as stored in database 80 with the bidirectional HTTP data stream (both requests and responses) transparently, in real-time and add, remove or block selected information in the HTTP stream. *Id.* at 11:20–24. The HTTP request can be enriched with the addition of encoded user attribute information, stored in database 80, in the form of additional HTTP headers. *Id.* at 11:25–27. The user attribute information itself can be sent to the content provider 40, or an encoded key can be sent to content provider 40 instead; this encoded key useful only to the intended recipient (the specific content provider 40). *Id.* at 12:4–6.

3. Parekh (Ex. 1007)

Parekh, entitled *Systems and Methods for Determining, Collecting, and Using Geographic Locations of Internet Users*, is directed to determining a geographic location of an Internet user. Ex. 1007, Abstract. Figure 1 of Parekh is shown below.

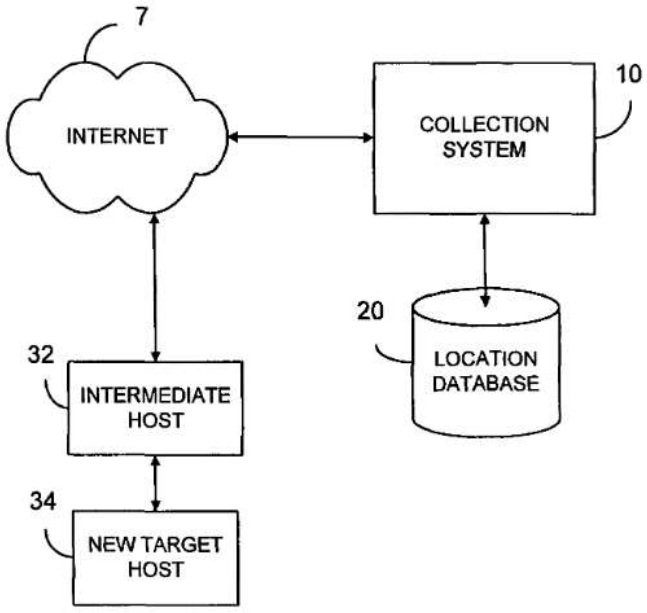

Figure 1 of Parekh, shown above, illustrates a network having a collection system. Ex. 1007, 7. The method involves determining if the host is on-line, determining ownership of the host name, and then determining the route taken in delivering packets to the user. *Id.* at Abstract. Based on the detected route, the method proceeds with determining the geographic route based on the host locations and then assigning a confidence level to the assigned location. *Id.* A system collects the geographic information and allows web sites or other entities to request the geographic location of their visitors. *Id.* The database of geographic locations may be stored in a central location or, alternatively, may be at least partially located at the web site. *Id.* With this information, web sites can target content, advertising, or route traffic depending upon the geographic locations of their visitors. *Id.* Through web site requests for geographic information, a central database tracks an Internet user's traffic on the Internet whereby a profile can be generated. In addition to this profile, the central database can store visitor's preferences as to what content should be delivered to an IP address, the

available interface, and the network speed associated with that IP address. *Id.*

4. Microsoft (Ex. 1009)

Microsoft is a technical market bulletin entitled, *Technical Details on Microsoft Product Activation for Windows XP*. Its purpose is to help customers and partners better understand the technologies used by product activation. Ex. 1009, 4. In particular, it describes how to identify computers in order to prevent piracy of Windows XP software. For retail software, computers would be identified based on identifiers associated with their hardware components, such as the "MAC address" associated with a network adapter. *Id.* at 7. These hardware identifiers would be "hashed" "through a one-way mathematical transformation" so that the "resultant hash value cannot be backwards calculated to determine the original values" "in order to maintain the user's privacy." *Id.* at 6.

5. Short (Ex. 1006)

Short is entitled, *Systems and Methods for Providing Digital Content and Caller Alerts to Wireless Network-Enabled Devices.* Short notes that more and more digital content is being delivered online over private and public networks, such as intranets, the Internet, cable television networks, telephone networks, and digital radio networks. Ex. 1006 ¶ 2. Short explains there is a need for systems and methods for enabling the content owner or provider to deliver digital content tailored to the preferences of the user (i.e., the intended audience) to the client device. *Id.* ¶ 6. Short explains the systems and methods of the invention provide user-selected digital content, such as music, video, games, etc. in a secure manner, over a wireless network, such as a cellular telephone network or satellite network,

in a substantially seamless and uninterrupted fashion as the user (with a mobile client device) moves about within the network, thereby facilitating, for example, custom-programmable on-demand content. *Id.* ¶ 7. Short also describes various illustrative embodiments that employ systems and methods for digital rights management (DRM) of digital content (e.g., audio data, music data, image data, video data, tactile data, text data, software, other digital data, or a combination thereof) distributed over a network, such as an intranet or the Internet, in either a wired or wireless fashion. *Id.* ¶ 60.

6. Mathai (Ex. 1008)

Mathai, entitled *Method and System for Providing Personalized Online Services and Advertisements in Public Spaces*, is directed to a method and system for providing personalized and integrated online services for communications and commercial transactions both in private and public venues. Ex. 1008, Abstract. The invention provides personalized information that is conveniently accessible through a network of public access stations, which are enabled by a personal system access card. *Id.* The invention also provides advertisers the opportunity to directly engage actual and potential user-consumers with selected advertising or marketing content based on each user's profile and usage history. *Id.*

E. Analysis

1. Patent Owner's General Assertions

Patent Owner makes two general assertions that Petitioner has failed to carry its burden of establishing that the challenged claims are unpatentable. These assertions are: 1) "Petitioner fails to conduct the vital step, required by *Graham*, of identifying the differences between the claimed subject matter and the prior art" (Resp. 22); and 2) "Petitioner [has

not] demonstrated that a [person of ordinary skill in the art] would have been motivated to combine the cited references to arrive at the challenged claims" (Resp. 12).

With respect to Patent Owner's general assertion that Petitioner has failed to identify the differences between the claimed subject matter and the prior art, we disagree with Patent Owner's assertions for the reasons set forth *infra*, where we consider the arguments and evidence with respect to each of the challenged claims and their respective limitations. *See, e.g.*, limitation 1.4, *infra*. Although important, the focus of an obviousness analysis is not merely on the differences between the claimed invention and the prior art. *Hybritech, Inc. v. Monoclonal Antibodies, Inc.*, 802 F.2d 1367, 1379–80 (Fed. Cir. 1986). There may be, in fact, only a single difference. *See Ryko*, 950 F.2d at 717. The question to be answered is whether the claimed invention as a whole would have been obvious to one of ordinary skill in the art at the time of the claimed invention. *Litton Indus. Prods., Inc. v. Solid State Sys. Corp.*, 755 F.2d 158, 164 (Fed. Cir. 1985). When the evidence is viewed in this light, Patent Owner's arguments are unpersuasive.

With respect to Patent Owner's assertion that Petitioner fails to demonstrate that a person of ordinary skill in the art would have been motivated to combine the cited references to arrive at the challenged claims, we also disagree with Patent Owner. For example, with respect to the combination of Harada and Roker, Petitioner argues,

> *Roker* provides a POSA with the motivation and the means to securely and uniquely identify a user and/or a user's device in the system of *Harada*. For example, *Roker* teaches that it is desirable to encrypt the information about the user where that information will leave a service provider's network

> because such information may be intercepted along its path of travel to other destinations.
>
> *Roker* also teaches that a static IP address is useful as an identifier, both for a user and for the user's device. Implementing "these features in *Harada* would improve *Harada's* method by allowing more secure and effective tailoring of content based on user profile information. Ex. 1010 ¶ 75.

Pet. 21.

Based on the arguments and evidence presented by Petitioner discussed in detail *infra*, we are persuaded that Petitioner has shown sufficiently that one of ordinary skill in the art would have been motivated to combine the references in the manner Petitioner has proposed.

2. Obviousness over Harada and Roker - Independent Claims 1, 20, and 21

Claims 1, 20, and 21 are independent and similar—one principal difference being that claims 20 and 21 recite steps of the claimed method occurring at a server and a network routing device, respectively. Petitioner relies on the combination of Harada and Roker to teach the limitations of the independent claims, claim 1 being illustrative.

a. 1.0 "A method for improving the selection of media for delivery to a targeted user of a client computing device"

With respect to claim 1's preamble, Petitioner asserts that "*Harada* intercepts a data request from a client computer to a target web server at a proxy server, adds encrypted profile information to the data request, decrypts and extracts the profile information at the web server and uses the profile information to generate a response." Pet. 22 (citing Ex. 1004, 2:28–3:25). Petitioner argues that Harada's "extracted profile information is used

'to generate or customize data sent in response 213 to the proxy server for forwarding as a response 214 to a user or client computer (step 425).'" *Id.* For example, Petitioner argues, "a tourist information web server may customize a page based [on] user profile data specifying a browser user's age, and interest." *Id.* (quoting Ex. 1004, 7:3–9; *see also* Ex. 1010 ¶ 76).

Petitioner also argues that Roker "tailor[s] … content to an audience of a single user." *Id.* (citing Ex. 1005, 5:3–6). Petitioner argues that in Roker, "[a] network device intercepts a request from a user to a content provider, accesses personal information related to the user and alters the request by 'the addition of encoded relevancy tags.'" *Id.* (quoting Ex. 1005, 5:15–16). Petitioner also argues that in Roker, "the content provider . . . may decode said relevancy tags and send a response [back]." *Id.* (quoting Ex. 1005, 5:16–17). In one embodiment, Petitioner argues, Roker's "relevancy data embedded in HTTP header tags may be used to 'make preferable advertisement choices by a destination host web publisher.'" *Id.* (quoting Ex. 1005, 19:14–16; *see also* Ex. 1010 ¶ 77).

Patent Owner does not address specifically Petitioner's arguments and evidence with respect to claim 1's preamble. *See* Resp. 23–39.

We agree with Petitioner that Harada describes using extracted profile information to customize data sent in response to a proxy server for forwarding to a user, and that Roker describes a network device intercepting a request from a user, accessing personal information about the user, and altering the request by adding relevancy tags.

We find, therefore, that the combination of Harada and Roker teaches or suggests the recited "method for improving the selection of media for delivery to a targeted user of a client computing device" of claim 1, and to

the extent the limitation is recited similarly in claims 20 and 21.

b. 1.1 "determining user information for a user"

With respect to the recited limitation, "determining user information for a user," Petitioner argues that "*Harada* [teaches] determining three types of 'user information' for a user." Pet. 23. Petitioner argues that "*Harada* retrieves previously stored user profile information from database 220 associated with proxy server 202." *Id.* (citing Ex. 1004, 5:8–17, Fig. 2). Petitioner explains that the "user profile is selected from database 220 based on identifying information associated with a particular computer or user of that computer." *Id.* (citing Ex. 1004, 6:5–21). Petitioner argues that such profile information "may include information such as a username, zip code, or age group associated with the user." *Id.* (citing Ex. 1004, 6:20–25).

Petitioner argues that "*Harada* also [teaches] 'user information' in the form of name and password information submitted by the client computer to a POP [point of presence] or login server." *Id.* (citing Ex. 1004, 6:9–11). Petitioner further argues that Harada's "POP or login server may send 'network connection information unique to that user (such as a unique combination of TCP/IP address and port number) to the proxy server 202 where it is stored in a database 220.'" *Id.* (quoting Ex. 1004, 6:11–15; *see also* Ex. 1010 ¶ 79).

Petitioner similarly argues that Roker teaches determining user information for a user by "accessing a database containing personal information related to the user." *Id.* (quoting Ex. 1005, 5:11–12; *see also* Ex. 1010 ¶ 80). Petitioner notes that Roker defines such personal information as "information about a user personal to that user, including name, address, contact information, preferences, and financial, familial and

professional information." *Id.* at 24 (quoting Ex. 1005, 7:7–8).

Patent Owner does not contest specifically Petitioner's arguments and evidence that Harada and Roker teach the recited "determining user information for a user," but instead addresses Petitioner's arguments and evidence with respect to the "user identifier" recited in limitation 1.2, which we address below. *See* Resp. 23–27.

We agree with Petitioner that Harada describes a user profile selected from a database identifying information associated with a particular user that may include information such as a username, zip code, or age group associated with the user. We also agree with Petitioner that Roker describes accessing a database containing personal information related to a user, such as name, address, contact information, and personal preferences.

We find, therefore, that the combination of Harada and Roker teaches or suggests the recited "determining user information for a user" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

c. 1.2 "generating a user identifier for the user from the determined user information"

With respect to the recited limitation "generating a user identifier for the user from the determined user information," Petitioner argues Harada teaches generating a user identifier for the user from the determined user information, as claimed, in at least two ways, and Roker teaches a third way. Pet. 24–26.

Petitioner first argues Harada adds profile information about the user to a data request from the user. *Id.* at 24 (citing Ex. 1004, 2:30–3:2). Petitioner explains that in Harada, the particular user profile information included in a data request is "selected based on an identity of a client computer user or a browser user." *Id.* (quoting Ex. 1004, 4:7–9). Petitioner

explains that in Harada, field 304 contains a "UserName=JohnDoe" identifier. *Id.* (citing Ex. 1004, 4:7–9). Petitioner argues that a person of ordinary skill in the art would recognize the inserted "UserName" is based on the determined user information because this variable is included in the user profile information retrieved from database 220 using network connection information. *Id.* (citing Ex. 1004, 6:14–29; Ex. 1010 ¶¶ 81–82).

Petitioner's second argument is that Harada teaches "web server 503 can store received profile data in a local database for future request processing purposes," and may return a shortcut token to proxy server 502. *Id.* at 25 (quoting Ex. 1004, 12:17–19). Petitioner argues proxy server 502 may add the shortcut token to a subsequent request 518 in place of the "full" user profile data sent in request 514 to reduce the amount of data that needs to be transferred in subsequent request 518. *Id.* (citing Ex. 1004, 12:19–21). Petitioner argues that a person of ordinary skill in the art "would have recognized the shortcut token added to subsequent data requests from the user as a second form of 'user identifier for the user from the determined user information,' as claimed," because "the fact that the shortcut token can be 'database query information' suggests the use of a query string or key based on the determined user information because that is the most straightforward way to link the shortcut token to the correct stored profile." *Id.* (quoting Ex. 1010 ¶ 84).

Thirdly, Petitioner argues that Roker also teaches this limitation because a user can be identified with "a code unique to the permitted user (subscriber) profile," such as a "billing or accounting code of the service provider," or "a static IP address used by the service provider to identify their customers." *Id.* at 26 (quoting Ex. 1005, 16:10–16). Petitioner further

argues a person of ordinary skill in the art "would have had reason to substitute Roker's method of identifying the user by static IP address or billing code for Harada's UserName or shortcut token because Roker teaches that the "nature of the identification method is arbitrary as it is often a unique method used by each service provider's network." *Id.* (citing Ex. 1010 ¶ 85; Ex. 1005, 16:10–16).

Patent Owner argues "neither the UserName nor the shortcut token meets the 'user identifier' limitation of Elements 1.1 and 1.2."[3] Resp. 25. Patent Owner argues, "the UserName cannot meet the "user identifier" limitation because it is not encrypted, but is instead sent unencrypted to the destination site." *Id.* Patent Owner also argues, "the 'shortcut token' . . . cannot be the 'user identifier' because . . . the 'shortcut token' is actually generated by the destination site after all 'user information' is already stored at the destination site. Thus, there would never be any need for any of Elements 1.6 through 1.9 to ever be performed." *Id.*

Patent Owner further argues, "in *Roker*, this 'code unique to the permitted user (subscriber) profile' is never transmitted to the destination site and hence it cannot constitute the 'user identifier' of the claim, which is encrypted and added to the network traffic transmitted to the destination site in Element 1.3." *Id.* at 26. Patent Owner goes on to argue that Petitioner's proposed substitution of Roker's code unique for Harada's UserName would not be sufficient because it would still be transmitted unencrypted. *Id.* at 27. Patent Owner argues similarly that substituting Roker's code unique for Harada's shortcut token likewise fails because the shortcut token originates

[3] Contrary to Patent Owner's statement, "user identifier" is not recited in limitation 1.1.

in the destination site. *Id.*

Patent Owner's argument that "the UserName cannot meet the 'user identifier' limitation because it is not encrypted" is not persuasive because limitation 1.2 does not recite or require encryption. Rather, limitation 1.2, recites "generating a user identifier for the user from the determined user information," and Patent Owner does not contest that Harada's UserName is generated from determined user information. Claim 1 recites "encrypting" in limitation 1.4, which we address *infra*.

Patent Owner's argument that Harada's shortcut token cannot be the "user identifier" recited in limitation 1.2 because it is never transmitted to the destination site is also unpersuasive because limitation 1.2 does not specify or restrict where the "user identifier" must be generated. Claim 1 recites "destination site" in limitations 1.3, 1.5, and 1.6, which we address *infra.*

Patent Owner's arguments with respect to the use of Roker's "code unique," i.e., that it "is never transmitted to the destination site," any substitution for Harada's UserName "would still remain unencrypted," and the substitution of the "code unique" for the shortcut token would still "originate[] solely in the destination site," are similarly unpersuasive for the same reasons articulated *supra*. Arguments with respect to encryption and the destination site are addressed *infra*.

We agree with Petitioner that Harada describes a UserName based upon the identity or name of a user as well as a shortcut token used in place of a full user profile. We also agree with Petitioner that Roker describes identifying a user with a unique code such as a static IP address.

We find, therefore, that the combination of Harada and Roker teaches

or suggests the recited "generating a user identifier for the user from the determined user information" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

d. 1.3 "tagging, with a network routing device, network traffic that is bound for a destination site"

With respect to the recited limitation "tagging, with a network routing device, network traffic that is bound for a destination site," Petitioner argues Harada teaches tagging network traffic bound for a destination site by encapsulating, at a proxy server, user profile information from a database into a HTTP request that is forwarded by the proxy server to a web server, and by inserting a shortcut token into subsequent requests. *Id.* (citing Ex. 1004 5:15–19, 12:17–23, Fig. 5). Petitioner argues that this encapsulation process is "tagging" because "*Roker* explains that targeting parameters in an HTTP header are known as 'relevancy tags' and thus would be created in a 'tag process.'" *Id.* at 26–27 (quoting Ex. 1005, 7:11–13, 15:10; *see also* Ex. 1010 ¶¶ 86–87).

Patent Owner does not contest specifically Petitioner's arguments and evidence that Harada's encapsulating, at a proxy server, user profile information from a database into a HTTP request that is forwarded by the proxy server to a web server, and inserting a shortcut token into subsequent requests, teaches the recited "tagging," especially in light of Roker's explanation that targeting parameters in an HTTP header are known as relevancy tags. *See* Resp. 27–31.

We agree with Petitioner that Harada describes tagging network traffic bound for a destination site by encapsulating, at a proxy server, user profile information from a database into a HTTP request that is forwarded to a web server, and also describes inserting a shortcut token into subsequent

requests. We also agree with Petitioner that Roker explains that targeting parameters in an HTTP header are known as relevancy tags and would be created in a tag process.

We find, therefore, that the combination of Harada and Roker teaches or suggests the recited "tagging, with a network routing device, network traffic that is bound for a destination site" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

e. 1.4 "the tagging including: generating a request identifier by encrypting the user identifier in an alphanumeric string, and adding the request identifier to the network traffic to generate tagged network traffic"

With respect to the recited limitation "the tagging including: generating a request identifier by encrypting the user identifier in an alphanumeric string, and adding the request identifier to the network traffic to generate tagged network traffic," Petitioner argues that a person of ordinary skill in the art would have had reason to generate a request identifier by encrypting user identifiers as shown by the combined teachings of Harada and Roker. Pet. 27.

Petitioner argues Harada teaches that certain user profile information is encrypted and placed in field 305 of the HTTP header. *Id.* (citing Ex. 1004, 6:20–27). Petitioner concedes that Harada does not explicitly disclose encrypting the UserName inserted into field 304, but Petitioner argues a person of ordinary skill in the art would have had reason to encrypt the identifying information in field 304 (or additional fields) because: (a) Harada teaches that "field 305 may include encrypted user profile data" using its SecureData protocol (*id.* quoting Ex. 1004, 6:25–26, 8:3–22); (b) Roker teaches that "the request can be further intercepted along its path,"

making it "preferable to use" encryption (*id.* (quoting Ex. 1005, 12:4–10)); and (c) "substituting encrypted user profile information for unencrypted user profile information would provide the predictable result that user profile information would be transmitted from the proxy server to the content provider in encrypted" form where it could be used, "in a more secure fashion, to customize and target content to the user based on the encrypted information" (*id.* at 27–28 (quoting Ex. 1010 ¶ 88)).

Petitioner further argues that a person of ordinary skill in the art "would have recognized that Harada teaches encrypting data as an alphanumeric string because it consists of 'letters A through Z, numbers 0 through 9, punctuation marks, and symbols that can be entered from the keyboard,'" *Id.* at 28 (quoting Ex. 1010 ¶ 89; Ex. 1020, p.17 (defining "alphanumeric characters")).

Petitioner also argues that Harada teaches that a shortcut token may be sent in encrypted form. *Id.* (citing Ex. 1004, 13:11–13, Fig. 5). Petitioner argues that a shortcut token is a "user identifier" as claimed. *Id.* Petitioner argues that a person of ordinary skill in the art would have understood that "*Harada* teaches or suggests encrypting the shortcut token 'in an alphanumeric string' because *Harada* teaches (a) the importance of encrypting the shortcut token when it is sent from the website to the proxy server (*id.*, 12:24–13:15), and (b) a mechanism for encrypting the shortcut token in an alphanumeric string in an HTTP request; namely, the 'SecureData Protocol.'" *Id.* at 28–29 (citing Ex. 1004, 6:24–29, Fig. 3; Ex. 1010 ¶ 90).

Petitioner also argues that Roker teaches the use of various user identifiers such as accounting codes or a static IP address that enables a

"persisten[t]" profile to be applied "across all out-bound and in-bound data packets." *Id.* at 29 (quoting Ex. 1005, 16:17–20). Petitioner argues a person of ordinary skill in the art would have had reason to include these identifiers in a request because of Roker's teaching, that Harada teaches including a user identifier in a request (Ex. 1004, Fig. 3B), and including the user identifier would enable the content provider to avoid showing duplicate ads to a user (Ex. 1029, at 1:22–27). *Id.* (citing Ex. 1010 ¶ 91). Petitioner also argues a person of ordinary skill in the art would have had reason to encrypt these identifiers because Roker teaches "it is often preferable to use" encoded user attribute information because the "request can be further intercepted along its path." *Id.* (quoting Ex. 1005, 11:25–12:10).

Patent Owner argues, "the alleged user identifier of *Roker* is never inserted into the network traffic, much less in an encrypted form." Resp. 28. Although Patent Owner concedes "[c]ertain user profile information from *Harada* is encrypted and inserted into the network traffic . . . the UserName (which is the alleged user identifier) is not encrypted when it is transmitted." Harada, Patent Owner argues, "specifically teaches not to encrypt the UserName." *Id.* at 28–29.

Patent Owner also argues that Harada's use of a shortcut token does not meet the limitation because its use would eliminate the need for limitations 1.6–1.8 (reciting the receiving, decoding, and retrieving steps), because the shortcut token in Harada is generated by the destination site. *Id.* at 29; *see also id.* at 25–26.

Patent Owner further argues that Roker's accounting codes or static IP address are not sufficient because they are related to "a profile internal to the service provider's network—not transmitting a user identifier to a

destination site, encrypted or otherwise." *Id.* at 29–30. Patent Owner argues, although "*Roker* disclosed that the network modifies network traffic in various ways . . . even if *Roker's* modifications were tags, *Roker* never discloses tagging network traffic with "a code unique to the permitted user (subscriber) profile." *Id.* at 30. If anything, Patent Owner argues, "*Roker* teaches away from transmitting the 'a code unique to the permitted user (subscriber) profile' in any fashion and certainly not for the claimed use of tagging network traffic, particularly given that the code could relate to internal billing or other accounting practices." *Id.*

Patent Owner's arguments that Petitioner's proposed combination of Roker and Harada fails because the "user identifier of *Roker* is never inserted into the network traffic, much less in an encrypted form," and Harada "specifically teaches not to encrypt the UserName," are unpersuasive.

The Supreme Court noted in *KSR*, "[a] person of ordinary skill is also a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 421. In many cases, "a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id.* at 420. "[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *Id.* at 417.

Here, Petitioner's expert, Mr. Gray, provides testimony that a person of ordinary skill in the art would have had reason to encrypt the UserName, including Harada's encryption of user information in other fields, Roker's teaching that a request can be intercepted along its path making it preferable

to use encryption, and a person of ordinary skill understanding that "substituting encrypted user profile information for unencrypted user profile information would provide the predictable result that user profile information would be transmitted from the proxy server to the content provider in encrypted, rather than unencrypted, form." Ex. 1010 ¶ 88. Harada also teaches use of SecureData protocol for encryption. *See* Ex. 1004, 6:26–27, 7:29–8:9.

Patent Owner's "teaching away" argument with respect to Harada's use of unencrypted data for the UserName is also unpersuasive. *See* Resp. 28–29 ("*Harada* . . . specifically teaches not to encrypt the UserName"). Teaching away requires a reference to "criticize, discredit, or otherwise discourage investigation into the claimed invention." *Meiresonne v. Google, Inc.*, 849 F.3d 1379, 1382 (Fed. Cir. 2017). Nothing in Harada criticizes, discredits, or otherwise discourages encrypting all of the information in a header. The HTTP header shown in Fig. 3B of Harada is merely "exemplary." Ex. 1004, 5:4.

Moreover, Harada states expressly that "Field 304 *may* include unencrypted user profile data ("UserName=John_Doe, ZipCode=60609, ParentalControl=YoungTeen), while field 305 *may* include encrypted user profile data." *Id.* at 6:24–26. The particular use of the word *may* suggests that use of encrypted or unencrypted user profile data is permissive, not required, in these fields. Such suggested permissive use of encryption does not "criticize, discredit, or otherwise discourage" the use of encryption for the UserName as Patent Owner appears to argue.

Patent Owner's argument with respect to Harada's use of a shortcut token, i.e., that it would eliminate the need for limitations 1.6–1.8 because

the shortcut token in Harada is generated by the destination site, is similarly unpersuasive.[4] Claim 1 does not specify where the user identifier must be generated. In Harada, after the shortcut token is generated, it is sent to the proxy server 502, which tags subsequent requests 518 with the shortcut token rather than using the full user profile data. Ex. 1004, 12:18–20. The shortcut token can be "an index value, database query information, file name, other pointer data, or an arbitrary value generated by the web site 503 and used to reference the stored user profile data." *Id.* at 12:21–23; Ex 1010 ¶ 83.

In those requests, the token is processed in the same manner as the UserName; namely, the shortcut token-tagged request is passed from the IIS or Netscape server software to proxy data exchange filter software, the shortcut token is decoded, and relevant stored user information made available to the IIS or Netscape web server software, thus not rendering limitations 1.6–1.8 superfluous as Patent Owner argues. *See, e.g.*, Ex. 1004, 7:14–24, 12:9–23; Ex. 1010 ¶¶ 96, 98–100; Ex. 1037 ¶ 16.

Patent Owner's arguments with respect to the use of Roker's accounting codes and static IP address are not persuasive either. Roker explains that the identifiers can be used to create a persistent profile to be applied "across all out-bound and in-bound data packets," not merely network-internal packets as Patent Owner argues. *See* Ex. 1005, 16:17–20; Ex. 1010 ¶ 91. Roker's described use of accounting codes and static IP

[4] We note that Patent Owner states, "[t]he differences between the challenged claims and *Harada* and *Roker* are not a reordering of steps." Resp. 14; s*ee also* Resp. 37 ("This is not a case where the cited art discloses each and every step of the challenged claims, but simply does so out of order.").

address does not "criticize, discredit, or otherwise discourage investigation" and thus does not amount to teaching away as Patent Owner argues.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited "tagging including: generating a request identifier by encrypting the user identifier in an alphanumeric string, and adding the request identifier to the network traffic to generate tagged network traffic" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

f. 1.5 "transmitting the tagged network traffic to the destination site"

With respect to the recited limitation "transmitting the tagged network traffic to the destination site," Petitioner argues Harada teaches that, after proxy server 202 "forms the modified HTTP request 212 containing the user profile data," the "modified request 212 may then be forwarded by the proxy server for receipt at a web site (steps 404 and 421)." Pet. 30 (quoting Ex. 1004, 6:27–29; *see also id.* 9:2–3, 12:7–9; Fig. 5; Ex. 1010 ¶ 94). Petitioner also argues that Roker teaches transmitting modified HTTP requests. *Id.* at 31 (citing Ex. 1010 ¶ 95).

Patent Owner does not appear to address specifically Petitioner's arguments and evidence with respect to this limitation. In its Response, Patent Owner references limitation 1.5 as "adding the request identifier to the network traffic to generate tagged network traffic," but this is description is inconsistent with limitation 1.5 ("transmitting the tagged network traffic to the destination site") as argued by the Petitioner (Pet. 30–31) and addressed by the Board in the Decision on Institution (Paper 7, 18). To the extent Patent Owner's arguments that "the alleged user identifier of Roker is never inserted into the network traffic," and Roker "references a profile internal to

the service provider's network—not transmitting a user identifier to a destination site," (*see* Resp. 29–30) might apply to transmitting tagged network traffic to the destination site, Patent Owner's arguments are unpersuasive as discussed *supra*.

We agree with Petitioner that Harada's description that, after proxy server 202 forms modified HTTP request 212 containing the user profile data, modified request 212 may then be forwarded by the proxy server for receipt at a web site (steps 404 and 421), along with Roker's description of transmitting modified HTTP requests, teaches or suggests "transmitting the tagged network traffic to the destination site" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

g. 1.6 "receiving from a requester associated with the destination site a decode request to decode the tagged network traffic"

With respect to the recited limitation "receiving from a requester associated with the destination site a decode request to decode the tagged network traffic," Petitioner argues Harada teaches that when the web server receives a request, "the request can be passed to proxy data exchange filter software that can extract the added fields," and "decrypt the session key and the user profile information" to "make the user profile information available to web server applications." Pet. 31 (quoting Ex. 1004, 12:9–12).

Petitioner argues Harada teaches that "the request 212 is passed to the proxy data exchange filter by the IIS or Netscape server software" associated with an "IIS or Netscape server web site." *Id.* (quoting Ex. 1004, 7:22–24). Petitioner also argues a person of ordinary skill would have understood that Harada's exchange filter software would "receiv[e]" a "decode request" from "a requester associated with the destination site" (e.g., Harada's IIS or

Netscape server software) "to decode the tagged network traffic," as claimed, because Harada "teaches that the tagged request is 'passed' from the server software to the exchange filter in order for the exchange filter to decode the tagged request." *Id.* at 31–32 (quoting Ex. 1004, 7:14–23; *see also* Ex. 1010 ¶ 96).

Additionally, Petitioner argues Roker teaches that "encrypt[ed]" profile information ("Caller ID content") is sent "with the user's communications to content provider 40's website (or to a third party to decode the content)," similar to two decoding options in the '314 patent. *Id.* at 32 (quoting Ex. 1005, 11:11–15; *see also* Ex. 1001, 10:12–41). Petitioner argues this teaches or suggests that a server associated with the web site (i.e., the claimed "requestor associated with the destination site") sends a decode request to a third party because: (a) it was well known that web servers would often send information directly to discrete third-party ad servers, which would then deliver targeted ads; and (b) Roker does not suggest an alternate mechanism for how the third party would receive a request to decode content. *Id.* at 32 (citing Ex. 1013, 36; Ex. 1034, 24:3–67; Ex. 1014, 4:5–24; *see also* Ex. 1010 ¶ 97). For example, Petitioner argues, Roker suggests use of an "advertising network, or advertising server, who can more precisely deliver the optimal advertisement opportunity." *Id.* (quoting Ex. 1005, 18:22–23). This ad server, Petitioner argues, would use "embedd[ed] relevancy data [in] HTTP header tags" to "make preferable advertisement choices." *Id.* (quoting Ex. 1005, 19:14–16; Ex. 1010 ¶ 97).

Patent Owner argues that Harada does not teach "receiving from a requester associated with the destination site a decode request," because Harda is describing "one software component of the disclosed web server

'passing' a request to the proxy exchange filter software within the same hardware component, and Petitioner never identifies the claimed "decode request." Resp. 31–33. Moreover, Patent Owner argues, because the destination site already has the "stored user information," Harada makes this step superfluous. *Id.* at 34.

Patent Owner also argues that Petitioner's reliance on Roker's sending Caller ID content is misplaced because the decoding options relied on by Petitioner in the '314 patent "relate[] solely to an exemplary embodiment where the TRP receives and processes the decode request and then extracts user information corresponding to the request identifier for transmission back to the destination site or requestor." Resp. 34–35. Patent Owner also argues Petitioner's Roker theory relies on user information being extracted or utilized information that is already included in the network request as an (improper) stand-in for a decode request having been received. *Id.* at 35.

Patent Owner's arguments are not persuasive. Patent Owner's arguments with respect to Harada are based on the notion that the claims require distinct or separate components or equipment to effectuate the steps of the claims. For example, Patent Owner's expert, Mr. Smoot, testifies that "receiving and transmitting equipment to enable the delivery of information . . . are explicitly required by the plain language of the claim limitations," and "the tag-related processing component (TRP) is . . . separate from the destination site or requestor that generates and transmits the decode request," and that "the 'decode request' is received by a component that is separate from the requestor." Ex. 2002 ¶¶ 79–81.

As we explained, *supra*, with respect to claim construction, the '314 patent notes that the invention "can be implemented through any suitable

unitary or distributed combination of hardware, software and/or firmware." Ex. 1001, 4:47–50, 15:57–16:17. The claims do not specify whether the "requester" is hardware or software or whether the decoding function must be in a separate physical location. Indeed, the '314 patent describes an embodiment where communications occur between software programs operating on the same computer. Ex. 1001, 10:28–42.

We credit Mr. Gray's testimony that a person of ordinary skill in the art would have understood Harada's exchange filter software as receiving a request to decode network traffic from Harada's IIS or Netscape server software because Harada explains that the tagged request is passed from that server software to the exchange filter in order for the exchange filter to decode the request. Ex. 1010 ¶ 96.

We also agree with Petitioner that Roker describes encrypted user information (Caller ID content) sent either to "content provider 40's web site (or to a third party to decode the content), where the Caller ID content is examined, decisions made, and then return content is sent from the web site back to the user's computer 10." Ex. 1005, 11:11–15. This description suggests a server associated with the web site sends a decode request to a third party to obtain decoded user identifying information to enable the provision of custom content to the user, which is similar to the embodiment described in the '314 patent. Ex. 1001, 10:12–52, Fig. 4; Ex. 1010 ¶¶ 97–98, 101.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited "receiving from a requester associated with the destination site a decode request to

decode the tagged network traffic" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

h. 1.7 "decoding the tagged network traffic to obtain the user identifier"

With respect to the recited limitation "decoding the tagged network traffic to obtain the user identifier," Petitioner argues Harada and Roker teach an exchange filter and third party, respectively, that receives decode requests when the web server receives modified HTTP requests. Pet. 33. Petitioner argues a person of ordinary skill would have understood that both references teach or suggest the claimed "decoding the tagged network traffic to obtain the user identifier" because in both references, the decoded user profile information is sent or made available to the server computer or content provider so that it can provide customized return content either alone or in connection with the third-party advertisement server. *Id.* (citing Ex. 1004, 12:9–16; Ex. 1005, 11:11–19, 13:12–22; Ex. 1010 ¶ 98). Petitioner argues a person of ordinary skill would have understood that the decoded form of the "user identifier" (e.g., UserName or shortcut token) would be included within the information obtained from the decoding process because both references utilize decoded user identifying information extracted from the modified data request to determine what custom content to deliver to the user in response to the user's data request. *Id.* (citing Ex. 1004, 6:27–7:9, 12:12–23; Ex. 1005, 5:15–17, 8:20–9:3, 11:11–15, 13:13– 17; Ex. 1010 ¶ 99).

Patent Owner argues that "what is being decoded in Roker is not the tagged network traffic consisting of the encrypted user identifier (the claimed request identifier), but rather the user information (which was sent with the original transmission, again obviating the need[] for these later

steps)." Resp. 36. Patent Owner argues that it does not make sense for such a request to be implied, "because the cited passage of *Roker* contemplates that ***the user information has already been provided to the destination site***" and "[t]here is no need for the destination site or a requester associated with the destination site to send a decode request to decode the tagged network traffic." *Id.* Claimed method steps 1.7–1.9 are unnecessary in Roker, Patent owner argues, because "the destination site **already has access to the user information**." *Id.* at 36–37.

Patent Owner argues the same holds true for the portions of Harada relied on by Petitioner. *Id.* at 37. Patent Owner argues Harada's shortcut token "is only used for subsequent communications where the destination site already has the user information, making the claimed method steps 1.6–1.9 superfluous. *Id.* at 37.

Patent Owner's argument with respect to Roker is unpersuasive because it ignores Roker's explanation that information used to tag the HTTP request may be encoded (Ex. 1005, 13:14–16), and Caller ID content (i.e., the "request identifier") may be sent to "a third party to decode the content," *I(id.* at 11:11–15). Mr. Gray testifies that a person of ordinary skill in the art would have understood sending encoded tagged network traffic from the web server to the third party ad server as a request to decode the encoded tagged information. Ex. 1010 ¶ 97. Mr. Gray explains that it was well known at the time that web servers would often send information directly to discrete third-party ad servers, which would then deliver targeted ads. *Id.* (citing Ex. 1013, 36; Ex. 1014, 4:5–24; Ex. 1034, 24:3–67). Mr. Gray also explains Roker suggests use of an "advertising network, or advertising server, who can more precisely deliver the optimal advertisement

opportunity," and the third-party ad server would use "embedd[ed] relevancy data [in] HTTP header tags" to "make preferable advertisement choices." Ex. 1005, 18:22–23, 19:14–16.

Patent Owner's argument with respect to Harada is also unpersuasive. Harada explains "[w]hen request 514 is received by the web server 503, the request can be passed to proxy data exchange filter software that can extract the added fields 304–205 from the request 514, decrypt the session key and the user profile information contained in fields 304–205, and make the user profile information available to web server applications." Ex. 1004, 12. Mr. Gray explains that a person of ordinary skill in the art would have understood that the decoded user profile information is sent or made available to the server computer so that it can provide customized return content. Ex. 1010 ¶ 98.

Mr. Gray also explains that a person of ordinary skill in the art would have understood that the decoded form of the "user identifier" (e.g., UserName or shortcut token) would be included within the information obtained from the decoding process because it utilizes the decoded user identifying information extracted from the modified data request to determine what custom content to deliver to the user in response to the user's data request. *Id.* ¶ 99. Harada's shortcut token is obtained from the decoding process to retrieve the corresponding database entry. Ex. 1004, 1212–23.

As noted *supra*, Harada's token is processed in the same manner as the UserName, i.e., the shortcut token-tagged request is passed from the IIS or Netscape server software to proxy data exchange filter software, the shortcut token is decoded, and relevant stored user information made

available to the IIS or Netscape web server software, thus not rendering limitations 1.6–1.8 superfluous, as Patent Owner argues. *See* Ex. 1004, 7:14–24, 12:9–23; Ex. 1010 ¶¶ 96, 98–100; Ex. 1037 ¶ 16.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited "decoding the tagged network traffic to obtain the user identifier" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

i. 1.8 "retrieving stored user information associated with the user identifier"

With respect to the recited limitation "retrieving stored user information associated with the user identifier," Petitioner argues Harada's "web server 503 can store the received profile data in a local database for future request processing purposes." Pet. 33 (quoting Ex. 1004, 12:17–23). Petitioner argues a person of ordinary skill reading Harada would understand that the user profile information stored at the web server is "retrieved" in response to subsequent requests using the shortcut token, enabling delivery of targeted content by "mak[ing] the user profile information available to web server applications." *Id.* at 33–34 (quoting Ex. 1004, 12:9–12, Fig. 5; *see also* Ex. 1010 ¶ 100).

Patent Owner argues that Petitioner's theory with respect to limitation 1.8 ignores that claimed method steps 1.6 and 1.7, "***do not occur at all*** in either *Harada* or *Roker*." Resp. 37. Patent Owner argues the cited art describes "fundamentally different approaches than the approach of the challenged claims," and "simply does not teach or suggest certain elements at all." *Id.*

We disagree with Patent Owner. Harada describes specifically, "web server 503 can store the received profile data in a local database for future

request processing purposes." Ex. 1004, 12:17–23. Mr. Gray testifies that a person of ordinary skill in the art would understand that the user profile information stored at the web server is retrieved in response to subsequent requests using the shortcut token, enabling delivery of targeted content by "mak[ing] the user profile information available to web server applications." Ex. 1010 ¶ 100 (quoting Ex. 1004, 12:12). Patent Owner's argument that claimed method step 1.8 is not taught by the prior art because the prior art does not teach steps 1.6 and 1.7 does not address specifically Petitioner's arguments and evidence that the prior art teaches step 1.8.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited "decoding the tagged network traffic to obtain the user identifier" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

j. 1.9 "transmitting the stored user information to the requester"

With respect to the recited limitation "transmitting the stored user information to the requester," Petitioner argues that in Harada, after the proxy exchange filter software decrypts the session key and user profile information contained in fields 304–305, or the shortcut token, the user profile information is made "available to web server applications" (i.e., "transmitted" to the "requester") by a number of "data exchange techniques." Pet. 35 (quoting Ex. 1004, 12:9–15). Petitioner argues a person of ordinary skill would have understood "these web server applications to be part of the IIS or Netscape server software because they provide content that the server software delivers to the requesting user." *Id.* (quoting Ex. 1010 ¶ 102). Petitioner also argues that in Roker, either the content provider (the "requester") or the third-party ad server, in response to

the content provider, examines the encrypted Caller ID content, which contains anonymized user personal information and makes decisions about the return content to be sent back to the user's computer. *Id.* (citing Ex. 1005, 11:1–10, 11:11–15; *see also* Ex. 1010 ¶ 103).

Patent Owner argues that Harada's proxy exchange filter software making data "available to" software on the very same web server is not "transmitting the stored user information to the requester" under the plain meaning of those terms. Resp. 38. Patent owner argues a person of ordinary skill in the art "would not interpret Harada's 'mak[ing] available' on the same server as 'transmitting.'" *Id.* (citing Ex. 2002 ¶¶ 89–93).

Patent Owner also argues that Petitioner's reference to "a number of 'data exchange techniques'" undercuts its argument that Harada teaches or suggests "transmitting the stored user information to the requester." *Id.* Patent Owner argues that the examples provided in Harada indicate that data is not being "transmitted" under the plain meaning of the term. *Id.* at 39. In particular, Patent Owner argues, "placing [data] in shared memory" indicates that data is not being transmitted. *Id.* (citing Ex. 2002 ¶ 93). Patent Owner further argues that under Petitioner's theory, user information is not being transmitted to a requester associated with the destination site, which Patent Owner argues, is the claimed "requester." *Id.*

With respect to Roker, Patent Owner argues, "[t]ransmission of content to a user is not 'transmitting the stored user information to the requester,' particularly where Petitioner has identified the "requester" here and in prior elements [sic] as the content provider." *Id.* at 40.

With respect to Patent Owner's argument that Harada is not transmitting data to the requester, Petitioner points out that the web server

applications in Harada to which the user profile information is made available would have been "a part of the IIS or Netscape server software because they provide content that the server software delivers to the requesting user." Reply 13–14; Ex. 1010 ¶ 102.

To the extent Patent Owner is making an implicit claim construction argument that a person of ordinary skill in the art "would not interpret Harada's 'mak[ing] available' on the same server as 'transmitting,'" this argument is not persuasive based upon our claim construction analysis, *supra,* that "transmitting" means "the communication of data between two different entities, but not required to be two different pieces of hardware."

With respect to Roker, Patent Owner argues transmission of content to a user is not "transmitting the stored user information to the requester," because the Petitioner has identified the "requester" here as the content provider. Roker explains, however, that "the third party ad server, in response to the content provider, examines the encrypted Caller ID content … and makes decisions about the return content to be sent back to the user's computer." Ex. 1005, 11:1–15; Ex. 1010 ¶ 103. Where the ad server makes those decisions, the content is transmitted first to the content provider (i.e., the requester), and then back to the user's computer, which satisfies limitation 1.9 ("transmitting the stored user information to the requester"). Ex. 1010 ¶ 103.

We are persuaded by Petitioner's arguments and evidence that the combination of Harada and Roker teaches or suggests the recited "transmitting the stored user information to the requester" of claim 1, and to the extent the limitation is recited similarly in claims 20 and 21.

Summary of Claim 1

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests all the recited limitations of claim 1.

k. Limitations 20.3 and 20.8

As noted *supra*, one of the differences between independent claim 20 and independent claim 1 is that claim 20 recites the method steps occurring at a server. Claim 20 reads as follows:

> 20. [20.0] A method for improving the selection of media for delivery to a targeted user, comprising:
> [20.1] determining, at a server, user information for a user;
> [20.2] generating, at the server, a user identifier for the user from the determined user information;
> [20.3] receiving, at the server from a requester associated with a destination site, a decode request to decode tagged network traffic,
> [20.4] wherein the tagged network traffic was transmitted to the destination site from a network routing device, and wherein the network routing device had tagged intercepted network traffic to create the tagged network traffic,
> [20.5] the tagged network traffic including a request identifier comprising the user identifier encrypted in an alphanumeric string;
> [20.6] decoding, at the server, the tagged network traffic to obtain the user identifier;
> [20.7] retrieving, at the server, stored user information associated with the user identifier; and
> [20.8] transmitting, at the server, the stored user information to the requester.

Ex. 1001, 18:42–61.

As discussed *supra*, we found that Petitioner's arguments and

evidence with respect to the combination of Harada and Roker taught or suggested the recited limitations of claim 20 to the extent those limitations were recited similarly by claim 1.

With respect to the recited "server" of claim 20, Petitioner argues that the server is taught by Harada's web server 503. *See* Pet. 50–53 (citing, e.g., Ex. 1004, 12:9–12, Fig. 5).

In response to Petitioner's arguments and evidence with respect to claim 20, Patent Owner argues,

> [f]or Element 20.3, just as for Element 1.6, Petitioner's theories do not meet the plain meaning of the claim language. Here, Petitioner relies only on *Harada*, including referring back to discussion of *Harada* for Element 1.6. *See* Petition, 51–52. But here again, *Harada's* disclosure of proxy data exchange filter software on a web server "passing" data from web server software on that same web server does not meet the plain meaning of "receiving, from a requester associated with the destination site, a decode request to decode tagged network traffic." *See also* Ex. 2002 ¶ 96.
>
> For Element 20.8, Petitioner again relies only on *Harada*, and refers back to discussion of *Harada* for Element 1.9. *See* Petition, 53. For the same reasons discussed there, Petitioner's *Harada* theory does not meet the plain language of Element 20.8. *Harada's* proxy exchange filter software making data "available to" software on the very same web server is not "transmitting the stored user information to the requester" under the plain meaning of Element 20.8. *See also* Ex. 2002 ¶ 97. Here, unlike in Element 1.9, Petitioner explicitly mentions the example "data exchange techniques," including "storing it in a database" and "placing it

> in shared memory," but these examples again serve only to reiterate that the data is not being "transmitted" under the plain meaning of that term. Ex. 2002 ¶¶ 93, 97.

Resp. 41–42.

Petitioner points out in its Reply that "the exchange filter software in Harada's web server receives a decode request from the IIS/Netscape web server software (the requestor associated with the destination site). This configuration is within the '314 patent's contemplation of a "unitary … combination of hardware, software and/or firmware." Reply 16 (citing Ex. 1001, 4:48–50).

We agree with Petitioner. Patent Owner does not contest Petitioner's evidence that Harada teaches the recited "server" of claim 20. Instead, with respect to limitations 20.3 and 20.8, Patent Owner relies on the same arguments made with respect to the plain and ordinary meaning of the term "transmitting" recited in claim 1. As with claim 1, Patent Owner is attempting to incorporate a limitation from the specification into the claim, i.e., "transmitting" requires moving information between independent and separate entities or components, even though such a limitation is not recited expressly in the claim. Patent Owner's argument with respect to claim 20 is unpersuasive for the same reasons we discussed *supra* with respect to claim 1.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited limitations of claim 20.

l. Limitation 21.6

Claim 21 differs from claims 1 and 20 in that the method steps of

claim 21 recite a "network routing device." Claim 21 reads as follows:

> 21. [21.0] A method for improving the selection of media for delivery to a targeted user, comprising:
> [21.1] determining, by a network routing device, user information for a user;
> [21.2] generating, by the network routing device, a user identifier for the user from the determined user information;
> [21.3] tagging, with the network routing device, network traffic that is bound for a destination site,
> [21.4] the tagging including: generating a request identifier by encrypting the user identifier in an alphanumeric string, and adding the request identifier to the network traffic to generate tagged network traffic; and
> [21.5] transmitting, by the network routing device, the tagged network traffic to the destination site,
> [21.6] the destination site receiving stored user information from a server after the destination site transmitted a decode request to a server to decode the tagged network traffic.

Ex. 1001, 18:62–19:12.

As discussed *supra*, we found that Petitioner's arguments and evidence with respect to the combination of Harada and Roker taught or suggested the recited limitations of claim 21 to the extent those limitations were recited similarly by claim 1.

With respect to the recited "network routing device," of claim 21, Petitioner argues the "network routing device" is taught by Harada's "proxy server" 502 or Roker's "network device" 70, in the combination of Harada and Roker. *See* Pet. 53–58 (citing, e.g., Ex. 1004, 5:8–17, Fig. 2; Ex. 1005, 5:11–12, Fig. 1).

In response to Petitioner's arguments and evidence with respect to

claim 21, Patent Owner argues,

> [f]or Element 21.6, Petitioner again relies on its argument that *Harada's* disclosure of user information being "made available" by techniques such as "storing it in a database" or "placing it in shared memory," this time to argue that this meets the requirement of "the destination site receiving stored user information from a server." For *Roker*, Petitioner argues that the limitation is met because "the content provider examines the encrypted Caller ID content, which contains anonymized user personal information." Neither of these examples teaches or suggests "receiving" by the destination site under the plain meaning of Element 21.6.
>
> Further, at a higher level, Petitioner's theories for Element 21.6 ignore the fundamental differences between the approaches of *Harada* and *Roker* and the challenged claims. As discussed above, *Harada* and *Roker*, in contrast to the challenged claims, provide the user information to the destination site in the first communication—obviating any need for the subsequent decode request from the destination site or associated requester or transmission of stored user information to the destination site or associated requester. Petitioner's theories for Element 21.6 ignore these differences.

Resp. 42–43 (internal citations omitted).

In its Reply, Petitioner argues,

> Patent Owner's arguments regarding limitation 21.6 purport to rely on the "plain meaning" of this limitation, but Patent Owner never explains what that meaning is. Patent Owner does not make any arguments different from its previous argument respecting limitation 1.9 and its general argument that *Harada* and *Roker* do not rely on multiple communications. Those arguments should be

> rejected for the reasons articulated previously. The website in Roker receives decoded user-identifying information that enables the provision of customer content to the user after sending a request to the third party to decode the information.

Reply 16–17.

Patent Owner does not contest Petitioner's evidence that Harada and Roker teach the recited "network routing device" of claim 21. Instead, with respect to limitations 21.6, Patent Owner argues that Harada and Rocker do not teach or suggest "receiving" by the destination site under the plain meaning of the limitation. Patent Owner cites to paragraph 98 of the Smoot declaration as support for this argument (*see* Resp. 42), but paragraph 98 does not provide a plain meaning for "receiving" by the destination site. *See* Ex. 2002 ¶ 98.

Patent Owner's other argument with respect to limitation 21.6, that Petitioner's combination of Harada and Roker "obviate[s] any need for the subsequent decode request from the destination site or associated requester or transmission of stored user information to the destination site or associated requester," is essentially the same argument Patent Owner made with respect to claim 1, which we found unpersuasive in our discussion, *supra*.

Based on the arguments and evidence of record, we find the combination of Harada and Roker teaches or suggests the recited limitations of claim 21.

3. Obviousness over Harada and Roker - Dependent Claims 2–7, 10–11, 14–16

a. Claim 2

Dependent claim 2 reads as follows:

> 2. The method of claim 1, wherein the request identifier comprises a key that provides access to a set of stored user information.

Ex. 1001, 17:39–41.

With respect to claim 2, Petitioner argues,

> *Harada* discloses that "[p]rofile information may be encrypted at the proxy server using a session key as an encryption key, and may be decrypted at the target server using the same session key. The session key may be determined by the proxy server and sent to the target server using a public key 15 cryptography algorithm and a public key associated with the target server." Ex. 1004, 4:11–15. "The public key encrypted session key" may "be placed in the request message 212." *Id.*, 8:15–16. *Harada* discloses an example of a session key included in field 305 of the HTTP header in Fig.3B. *Id.*, 10:15–24, Fig. 3B. Ex. 1010 ¶ 104. The session key "provides access to a set of stored user information," as claimed, because "[w]hen the web server 203 has received the encrypted session key and user profile data, the web server 203 can decrypt its session key by using the public key cryptography algorithm and the web server's private key. The web server 203 may then decrypt the user profile information using the decrypted session key." *Id.*, 8:17–20. A POSA would have understood that this profile information was "a set of stored information," as claimed, because it was stored both on the proxy server in a database and in memory on the content server. Ex. 1010 ¶ 105.

Pet. 35–36.

Petitioner further argues a person of ordinary skill in the art,

> would have understood that the shortcut token added to subsequent data requests from the user could similarly be encrypted to further protect the privacy of the user information and that the

> encrypted shortcut token would provide access to a set of stored user profile information in a database on the server. Ex. 1004, 12:17–13:15; Ex. 1010 ¶ 106.

Pet. 36.

With respect to dependent claim 2, Patent Owner argues. "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of Harada and Roker. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2−7, 10−11, and 14−16]." Resp. 43.

Patent Owner's argument with respect to claim 2 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes the use of a session key that can be decrypted to provide access to the encrypted user profile information. We are persuaded by Petitioner's evidence and arguments that a person of ordinary skill in the art would have understood that, by using the session key in this manner, Harada is obtaining access to profile information, which is a set of stored information. We are also persuaded that a person of ordinary skill in the art would have understood that Harada's shortcut token could similarly be encrypted to further protect the privacy of the user information and that the encrypted shortcut token would provide access to a set of stored user profile information in a database on the server.

We, therefore, find that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, wherein the request identifier comprises a key that provides access to a set of stored user information."

b. Claim 3

Dependent claim 3 reads as follows:

> 3. The method of claim 1, wherein the stored user information associated with the user identifier includes: previously determined demographic information related to the user, previously determined geographic information related to the user, or previously determined user determining user preferences.

Ex. 1001, 17:42–47.

With respect to claim 3, Petitioner argues,

> *Harada* discloses that the stored user information may include demographic and geographic information about the user such as the user's age group and zip code. Ex. 1004, 6:20–25. *Roker* similarly discloses demographic and geographic information about the user, as well as user preferences, such as "address, contact information, preferences, and financial, familial and professional information." Ex. 1005, 7:7–8, 8:5–7, *see also id.*, 5:15 ("The personal information may include user preferences.").
>
> A POSA would have understood that this information must have been "previously determined" because the methods of both *Harada* and *Roker* must rely on user profile information collected a priori to target content to the user based on demographic, geographic or preference information. *See, e.g.*, Ex. 1004, 2:22–24 (referring to "query [to] a user for data… for data storage and input"). Ex. 1010 ¶ 107. In addition, a POSA would have understood *Roker's* reference to "preferences" to be "user determining user preferences" because the purpose of storing user preferences in *Roker* is to use that information to help identify the user with sufficient precision to target content such as advertising to that user. Ex. 1010 ¶ 108 (citing Ex. 1005, 4:7–9).

Pet. 37.

With respect to dependent claim 3, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of Harada and Roker. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 3 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes the stored user information may include demographic and geographic information about the user such as the user's age group and zip code and that Roker describes demographic and geographic information about the user as well. We are persuaded by Petitioner's evidence and arguments that a person of ordinary skill in the art would have understood that this information was previously determined. We are also persuaded that a person of ordinary skill in the art would have understood that Roker's preferences would be user determining preferences.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, wherein the stored user information associated with the user identifier includes: previously determined demographic information related to the user, previously determined geographic information related to the user, or previously determined user determining user preferences."

c. Claim 4

Dependent claim 4 reads as follows:

> 4. The method of claim 1, further comprising maintaining, or updating, or both, the stored user information.

Ex. 1001, 17:48–49.

With respect to claim 4, Petitioner argues,

> *Roker* discloses that a user's profile may be updated automatically in response to a prompt from a third-party system. Ex. 1005, 21:24–25. Stored user information also may be updated in response to a prompt to the user, such as a prompt to the user to update his or her credit card information. *Id.*, 22:23–24. Ex. 1010 ¶ 109.
>
> *Harada* discloses a "Flush" operation in which proxy server 502 is directed to discard a specified shortcut token or all such tokens and a web server may be directed to discard stored user profile data associated with one or all shortcut tokens. Ex. 1004, 13:20–24. "This directive may be used by a web server 503 or proxy server 502 that is performing a reset operation." *Id.*, 13:24–26. A POSA would have understood that the flushing operation disclosed by *Harada* is a form of "maintaining, or updating … stored user information," as claimed, because the removal of existing data is one common way of maintaining and/or updating data. *Harada* further discloses that the web server can issue a "SendFull" directive, which asks the proxy server to "send 'full' user profile data (rather than a shortcut token)." Ex. 1004, 14:1–3.
>
> A POSA "would have understood this disclosure to teach or suggest updating the profile with the full profile." Ex. 1010 ¶ 110. A POSA would have had reason to maintain and update the stored user information in the combination of *Harada* and *Roker* in view of these teachings "because doing so would ensure better precision and flexibility in targeting content such as advertisements to users while avoiding redundancy and reducing errors, which is an object of both" references. Ex. 1010

> ¶ 111 (citing Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26).

Pet. 37–39.

With respect to dependent claim 4, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of Harada and Roker. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 4 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Roker describes that a user's profile may be updated automatically in response to a prompt. We also agree with Petitioner that Harada describes discarding a stored user profile data associated with shortcut tokens. We are persuaded by Petitioner's evidence and arguments that Harada's flushing operation is a form of maintaining, or updating stored user information. We are also persuaded that a person of ordinary skill in the art would have had reason to maintain and update the stored user information in the combination of Harada and Roker in view of these teachings.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, further comprising maintaining, or updating, or both, the stored user information."

d. Claim 5

Dependent claim 5 reads as follows:

> 5. The method of claim 1, wherein the determining user information includes: determining demographic information related to the user,

> determining geographic information related to the user, and determining user preferences.

Ex. 1001, 17:50–55.

With respect to claim 5, Petitioner argues,

> *Harada* discloses that the stored user information may include demographic and geographic information about the user such as the user's age group and zip code, as well as the user's "interest[s]." Ex. 1004, 6:20–25, 7:5–9. *Roker* similarly discloses demographic and geographic information about the user, as well as user preferences, such as "address, contact information, preferences, and financial, familial and professional information." Ex. 1005, 7:7–8, 8:5–7, *see also id.*, 5:15 ("The personal information may include user preferences."). A POSA would have combined *Roker's* user preferences with *Harada's* content targeting system "because it would improve the precision and efficiency of content tailoring." Ex. 1010 ¶ 112.
>
> [A] POSA would have understood that this information must have been "determin[ed]" because the methods of both *Harada* and *Roker* must rely on user profile information collected a priori to target content to the user based on demographic, geographic or preference information. A POSA further would have understood that common methods for determining demographic and geographic information about a user, and user preferences, existed at the time, including "forms" filled out by users to obtain needed targeting data. Ex. 1010 ¶ 112 (citing Ex. 1004, 7:9–13).

Pet. 39–40.

With respect to dependent claim 5, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious

based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 5 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes that stored user information may include demographic and geographic information about the user such as the user's age group and zip code, as well as the user's interest. We also agree with Petitioner that Roker describes demographic and geographic information about the user, as well as user preferences, such as address, contact information, preferences, and financial, familial and professional information. We are persuaded by Petitioner's evidence and arguments that this information must have been determined because the methods of both Harada and Roker rely on collected user profile information to target content to the user based on demographic, geographic or preference information.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, wherein the determining user information includes: determining demographic information related to the user, determining geographic information related to the user, and determining user preferences."

e. Claim 6

Dependent claim 6 reads as follows:

> 6. The method of claim 5, wherein the user identifier is generated using the determined demographic information and determined geographic information.

Ex. 1001, 17:56–58.

With respect to claim 6, Petitioner argues,

> both *Harada* and *Roker* disclose generating a user identifier using user information determined from a stored user profile. Also [] that profile information includes not only the user's name, but also demographic and geographic information.
>
> In particular, *Harada* discloses a field inserted into the HTTP header of an outgoing data request message that includes a user identifier ("UserName=JohnDoe") as well as demographic information ("YoungTeen") and geographic information ("ZipCode=60609"). Ex. 1004, 6:20–26, Fig. 3B. *Harada* also discloses a shortcut token for use in subsequent requests that is representative of this information. *Id.*, 12:17–23. A POSA would have understood that while *Roker* teaches the desirability of removing personally identifiable information, geographic information and phone number information could still be provided in the form of zip codes or area codes. Ex. 1010 ¶ 113 (citing Ex. 1005, 5:11–12, 7:7–8, 8:3–7). *Roker* uses this information to create relevancy tags to identify the user to allow customized content to be delivered to the user. *Id.*, 5:15–17, 8:20–9:3. *Id.*
>
> A POSA would have had reason to generate the user identifier in the combination of *Harada* and *Roker* not only by using the user's name, but also by including geographic and demographic information about the user, because doing so would "help to distinguish between different users with common names or between family members of different generations living in the same household, which is more likely to ensure better precision and flexibility in targeting" advertisements. Ex. 1010 ¶ 114 (citing

> Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26).

Pet. 40–41.

With respect to claim 6, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 6 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "Petitioner is improperly using the '314 Patent disclosure and claims as a roadmap for adding teachings into *Harada* and *Roker* that are not disclosed." *Id.* at 44. Patent Owner further argues, "even if it would be desirable to distinguish between different users with common names, there is no teaching or suggestion in either *Harada* or *Roker* to do so by using either geographic or demographic information along with a user name to create the user identifier. Rather, there are many other ways of achieving this objective, such as simply using a randomly-generated number along with the user name to generate the user identifier." *Id.* at 45.

Mr. Gray testifies that both Harada and Roker teach generating a user identifier using user information determined from a stored user profile. Ex. 1010 ¶¶ 81–85, 113. Mr. Gray explains that profile information includes not only the user's name, but also demographic and geographic information. *Id.* ¶ 79. In particular, Mr. Gray testifies that Harada describes a field inserted into the HTTP header of an outgoing data request message in field 304 that includes a user identifier ("UserName=JohnDoe") as well as demographic information ("YoungTeen") and geographic information

("ZipCode=60609"). *Id.* ¶ 113 (citing Ex. 1004, 6:20–26, Fig. 3B). Mr. Gray also testifies that Harada describes a shortcut token for use in subsequent requests that is representative of this information. *Id.* (citing Ex. 1004, 12:17–23).

Mr. Gray further testifies that a person of ordinary skill in the art would have understood that, while Roker explains the desirability of removing personally identifiable information, geographic information and phone number information could still be provided in the form of zip codes or area codes. *Id.* (citing Ex. 1005, 5:11–12, 7:7–8, 8:3–7). Mr. Gray testifies that Roker uses this information to create relevancy tags to identify the user to allow customized content to be delivered to the user. *Id.* (citing Ex. 1005, 5:15–17, 8:20–9:3).

In addition, Mr. Gray testifies that a person skilled in the art would have had reason to generate the user identifier in the combination of Harada and Roker not only by using the user's name, but also by including geographic and demographic information about the user, because doing so would help to distinguish between different users with common names or between family members of different generations living in the same household, which is more likely to ensure better precision and flexibility in targeting content such as advertisements to users while avoiding redundancy and reducing errors, which is an object of both Harada and Roker. *Id.* ¶ 114 (citing Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26).

In light of this evidence, Patent Owner's generalized "hindsight" argument is unpersuasive. Moreover, Patent Owner's argument that neither Harada nor Roker provide any teaching or suggestion for Petitioner's

combination does not consider the extent of the Supreme Court's decision in *KSR*, that the motivation to combine references does not require an explicit teaching or motivation within the four corners of the references, but that "any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed." *KSR*, 550 U.S. at 420.

We are persuaded by Petitioner's arguments and evidence that both Harada and Roker describe generating a user identifier using information determined from a stored user profile where that profile information includes a user's name, demographic information, and geographic information concerning the user. We are also persuaded that a person of ordinary skill in the art would have had reason to include such information in the user identifier.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 5, wherein the user identifier is generated using the determined demographic information and determined geographic information."

f. Claim 7

Dependent claim 7 reads as follows:

> 7. The method of claim 5, wherein the tagging further includes encrypting the determined user information in the alphanumeric string, and wherein decoding the tagged network traffic further includes obtaining the encrypted user information, the method further comprising storing the obtained user information with the stored user information associated with the user identifier.

Ex. 1001, 17:59–65.

With respect to claim 7, Petitioner argues,

> *Harada* encrypts certain profile information in an alphanumeric string in field 305 of the HTTP request header of the outgoing network traffic. Ex. 1004, 6:20–27. The profile information there encrypted is included within "the determined user information," as claimed, because it is profile information associated with the user retrieved by the proxy server, *id.*, 6:14–21, which may comprise, e.g., the "user's age, and interest." *Id.*, 7:8–9. Encryption is implemented by using the "SecureData protocol." *Id.*, 6:26–27. Ex. 1010 ¶ 115. [A] POSA would have recognized that field 305 of *Harada* is an alphanumeric string because it consists of "letters A through Z, numbers 0 through 9, punctuation marks, and symbols that can be entered from the keyboard." Ex. 1010 ¶ 116 (citing Ex. 1020, p. 17). A POSA would have had reason to substitute letters and numbers for other symbols in field 305 because doing so would entail the simple substitution of one known element (letters and numbers) for another (other symbols) to yield the predictable result of creating user profile information in a form suitable for use in delivering targeted advertising. *Id.*
>
> [] *Harada* discloses that when the web server receives a request, "the request can be passed to proxy data exchange filter software that can extract the added fields," and then "decrypt the session key and the user profile information" to "make the user profile information available to web server applications." Ex. 1004, 12:9–12. A POSA would have understood from this disclosure that during this process, the exchange filter software "obtains" the encrypted user information, as claimed, because it would be necessary for the exchange filter to

> obtain this encrypted information in order to decrypt it. Ex. 1010 ¶ 117.
>
> *Harada's* web server 503 stores received profile data in a local database for future request processing purposes. For a subsequent request by a user, the "proxy server 502 may add a shortcut token to a subsequent request 518 in place of the 'full' user profile data sent in the request 514." Ex. 1004, 12:17–23. The shortcut token is "used to reference the stored user profile data." *Id.* A POSA would have understood that in this operation the "obtained user information" is stored with "the stored information associated with the user identifier," as claimed, because any newly retrieved user information for a particular user received in a subsequent request with the shortcut token (e.g., the URL of a new request 517, 518 or a more recent profile, Ex. 1004, 14:1–3) would be used to update any previously stored information about that user at the web server to more accurately target content. Ex. 1010 ¶ 119.
>
> [A] POSA would have had reason to maintain and update the stored user information in *Harada* or *Roker* because doing so would ensure better precision and flexibility in targeting content such as advertisements to users while avoiding redundancy and reducing errors, which is an object of both the *Harada* and *Roker* disclosures. Ex. 1010 ¶ 120 (citing Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26). *See also* Ex. 1005, 21:24–25, 22:23–24 (disclosure of specific examples of updating in *Roker*).

Pet. 41–43.

With respect to dependent claim 7, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious

based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 7 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes encrypting certain profile information in an alphanumeric string of the HTTP request header of the outgoing network traffic, and that this profile information is associated with the user retrieved by the proxy server. We are persuaded by Petitioner's evidence and arguments that a person of ordinary skill in the art would have recognized that field 305 of Harada is an alphanumeric string. We agree with Petitioner that Harada describes that a request can be passed to the proxy data exchange filter software that can extract the fields, and then decrypt the session key and the user profile information to make the user profile information available to web server applications. We also agree with Petitioner that Harada describes a web server that can store received profile data in a local database for future request processing purposes.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 5, wherein the tagging further includes encrypting the determined user information in the alphanumeric string, and wherein decoding the tagged network traffic further includes obtaining the encrypted user information, the method further comprising storing the obtained user information with the stored user information associated with the user identifier."

g. Claim 10

Dependent claim 10 reads as follows:

> 10. The method of claim 1, wherein generating the user identifier includes determining a unique device identifier for a client computing device.

Ex. 1001, 18:9–11.

With respect to claim 10, Petitioner argues,

> *Harada* teaches that the "user profile may be selected from the database 220 based on the identifying information associated with a particular computer or user of that computer." Ex. 1004, 6:5–7. That database may associate "user identity information with network connection information," such as a "unique combination of TCP/IP address and port number." Ex. 1004, 6:8–16. A POSA would have understood that an IP address identifies a device, as claimed, because addresses were understood as an identifier of computing devices, as reflected by the named inventors' statement that: "'the IP address of the network access device is used . . . to identifier [sic] the particular network access device.'" Ex. 1035 ¶ 10; Ex. 1010 ¶ 121.
>
> A POSA also would have understood that an IP address uniquely identifies the user's computer on the computer's local network because IP addresses need to be locally unique. Ex. 1010 ¶ 122 (citing Ex. 1036, p.7). Nothing more is required by the claimed "unique device identifier," because the '314 patent teaches that the "unique identifier (DID) for the client device" can be a "port identifier." Ex. 1001, 8:39–41. A POSA would understand that port identifiers are rarely, if ever, globally unique because there are relatively few of them available under prevailing protocols. Ex. 1010 ¶ 122. Additionally, while certain embodiments of the '314 patent include "global unique identifiers" based on "extracting non-personal/device information during MAC/network layer

> processing," Ex. 1001, 5:21–28, claim 10 recites no such limitations. Ex. 1010 ¶ 122.
>
> *Roker* similarly discloses identifying the user's device by a unique static IP address. User attribute information is obtained by "matching the IP address of user's computer 10 against a list of users stored in database 80." Ex. 1005, 11:28–29. The IP address "may be a static IP address used by the service provider to identify their customers." *Id.*, 16:12–13. Although the "nature of the identification method is arbitrary," the "purpose of the identification is to link the user's Internet address to a static unique identifier for the authenticated user on the network." *Id.*, 16:13–16. Ex. 1010 ¶ 123. Static IP addresses generally do not change and are sometimes referred to as "permanent IP addresses." Ex. 1010 ¶ 17. A static IP address can thus be used to uniquely identify a device on a service provider's network, as Roker teaches. Ex. 1010 ¶ 124.
>
> A POSA would have had reason to include the step of determining a unique device identifier, as claimed, (that is, determining a static IP address as taught by *Roker*) during the step of generating the user identifier because *Harada* teaches that the user is identified by, inter alia, her IP address and *Roker* teaches the desirability of linking the user's IP address to a static unique identifier, such as a static IP address, in order to create a persistent profile to assist in ad targeting. Ex. 1010 ¶ 125 (citing Ex. 1005, 16:14–24).

Pet. 42–45.

With respect to dependent claim 10, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for []

dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 10 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes that the user profile may be selected from a database based on the identifying information associated with a particular computer or user. We agree with Petitioner that Harda teaches the database may associate user identity information with network connection information, such as a unique combination of TCP/IP address and port number. We agree with Petitioner that a person of ordinary skill in the art would have understood that an IP address uniquely identifies the user's computer on a local network. We also agree with Petitioner that Roker describes identifying a user's device by a unique static IP address.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, wherein generating the user identifier includes determining a unique device identifier for a client computing device."

h. Claim 11

Dependent claim 11 reads as follows:

> 11. The method of claim 10, wherein generating the user identifier includes performing a one-way hashing operation on the unique device identifier to generate the local user identifier.

Ex. 1001, 18:12–15.

With respect to claim 11, Petitioner argues,

> *Roker* teaches using the static "IP address of user's computer 10" to uniquely identify a computer and its user. Ex. 1005, 11:27–29, 16:10–16; Ex. 1010 ¶ 126. It is important to "obscure the identity of the user's profile … to ensure that acceptable levels of

> privacy are maintained" because the augmented "request can be further intercepted along its path by other" devices. Ex. 1005, 11:1–10, 12:6–8, 17:27–28. Because a POSA would nonetheless have wanted to send a user identifier across the Internet so that the content server could, for example, avoid showing duplicate ads to the same user, a POSA would have been motivated to send an anonymous identifier. Ex. 1010 ¶ 127 (citing Ex. 1024, 1:23–27).
>
> The motivation to send an anonymous identifier would have led a POSA to apply a one-way hash to the device identifier or static IP address. Ex. 1010 ¶ 128. *Harada* discloses "hash[ing]" information from the client HTTP request "to make forging or tampering more difficult." Ex. 1004, 11:22–23. A POSA would therefore have had reason to apply the disclosed hashing technique to device identifiers, such as a static IP address, to protect user privacy before the request left the service provider's network because hashing was one well-known way to obscure information for privacy and security. Ex. 1010 ¶ 128; *id.*, ¶¶ 33, 37, 39. Applying a one-way hash to the identifier would have enabled service providers to act as "trusted keepers of information about the user," which *Roker* taught was desirable. Ex. 1005, 11:1–10. Indeed, privacy is the precise reason for the one-way hash in the '314 Patent. Ex. 1001, 8:45–48 ("using a standard one-way hash algorithm to create a Local User ID (LUID) [or] any equivalent coding method that ensures adequate privacy"). Ex. 1010 ¶ 129.

Pet. 46–47.

With respect to claim 11, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to

prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 11 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "there would be no need to hash the IP address of a user's computer to obscure the identity of a user's profile because an IP address cannot be used to uniquely identify a user; rather, the same IP address is assigned to every device accessing the network though a particular gateway." Resp. 46. Patent Owner argues, "[o]nce again, Petitioner is improperly using hindsight analysis by using the '314 Patent disclosure and claims as a roadmap to modify the teachings of *Roker*." *Id.*

With respect to Harada, Patent Owner argues, "the cited *Harada* disclosure teaches performing a hash operation on a requested URL (i.e., a web address identifying where content requested by a user can be found on a network such as the Internet), not on a user identifier." *Id.* at 47. "To the extent that deriving a hash value from a requested URL could 'make forging or tampering more difficult …,' as taught by *Harada*, that goal is accomplished without hashing a user identifier, as is required by Claim 11 of the '314 Patent." *Id.*

Mr. Gray testifies that Roker describes using the static "IP address of user's computer 10" to uniquely identify a user. Ex. 1010 ¶ 126 (citing Ex. 1005, 11:27–29, 16:10–16). Mr. Gray also testifies that Roker explains it is important to "obscure the identity of the user's profile … to ensure that acceptable levels of privacy are maintained" because the augmented "request can be further intercepted along its path by other" devices. *Id.* ¶ 127 (citing Ex. 1005, 11:1–10, 12:6–8, 17:27–28). Mr. Gray testifies that a person of

ordinary skill in the art would have wanted to send a user identifier across the Internet so that the content server could avoid showing duplicate ads to the same user. *Id.* (citing, e.g., Ex. 1024, 1:23–27). Thus, Mr. Gray testifies, a skilled artisan would have been motivated to send an anonymous identifier. *Id.*

Mr. Gray also testifies that the motivation to send an anonymous identifier would have led a person of ordinary skill in the art to apply a one-way hash to the device identifier or static IP address. *Id.* ¶ 128. Mr. Gray testifies that Harada describes hashing information from the client HTTP request "to make forging or tampering more difficult." *Id.* (citing Ex. 1004, 11:22–23). Mr. Gray also testifies a person of ordinary skill in the art would have had reason to apply the disclosed hashing technique to device identifiers, such as a static IP address, to protect user privacy before the request left the service provider's network because hashing was one well-known way to obscure information for privacy and security. *Id.*; *see also id.* ¶¶ 37, 39. Mr. Gray testifies that hiding IP addresses is one of the known features of proxy servers. *Id.* ¶¶ 33, 128.

In light of this evidence, Patent Owner's "hindsight" argument is unpersuasive. Mr. Gray testifies that hashing was a well-known technique to obscure information to protect privacy and that Roker explains the desirability of protecting user privacy by anonymizing data about the user sent over the internet. Roker would have provided a reason to anonymize the user identifier and would have led a person of ordinary skill in the art to apply a one-way hash to the device identifier or static IP address. Patent Owner's argument that Harada discloses only hashing a URL improperly attacks Harada alone where the ground is based on the combination of

Harada and Roker.

We are persuaded by Petitioner's arguments and evidence that the combination of Harada and Roker describes using a hashing operation with a device identifier or unique IP address to create an anonymous user identifier. We are also persuaded that a person of ordinary skill in the art would have had reason to do so in order to protect the privacy of the user and reduce duplicative services to the user.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 10, wherein generating the user identifier includes performing a one-way hashing operation on the unique device identifier to generate the local user identifier."

i. Claim 14

Dependent claim 14 reads as follows:

> 14. The method of claim 1, wherein after the transmitting the stored user information to the requester, the requester, using a server, transmits targeted content to the user, the targeted content determined by the requester based in part on the user information.

Ex. 1001, 18:23–27.

With respect to claim 14, Petitioner argues,

> *Harada* discloses that once web server 203 receives the augmented HTTP request, it can extract the user profile information by decrypting the encrypted information in field 305 using a "decode request" from "the requester" (e.g., the "IIS or Netscape server software" on the content server). Ex. 1004, 7:5–6, 12:9–12. The content server can then "customize data sent in response" based on, for example, demographic information like a "browser user's age, and interest." *Id.*, 7:6–9. Ex. 1010 ¶ 130.

> Similarly, *Roker's* method "allows … the tailoring of content to an audience of a single user." Ex. 1005, 5:3–4. A network device intercepts a request from a network user to a content provider, accesses personal information related to the user and determines whether to alter the request by "the addition of encoded relevancy tags." *Id.*, 5:7–16. The content provider may decode the relevancy tags and send a response back. *Id.*, 5:16–17. The content provider "control[s] the destination server" used to provide content to the user. *Id.*, 21:2–4. A POSA thus would understand that *Roker's* method "us[es] a server [to] transmit[] targeted content to the user," as claimed. Ex. 1010 ¶ 131.

Pet. 47–48.

With respect to dependent claim 14, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 14 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes a web server extracting user profile information by decryption using a decode request from the IIS or Netscape server software, where the content server can then customize data sent in response based on demographic information like a user's age and interest. We also agree with Petitioner that Roker describes tailoring content to a single user where a network device intercepts a request from a network user to a content provider, accesses personal information related to the user and determines whether to alter the request by the addition of encoded relevancy tags.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 1, wherein after the transmitting the stored user information to the requester, the requester, using a server, transmits targeted content to the user, the targeted content determined by the requester based in part on the user information."

j. Claim 15

Dependent claim 15 reads as follows:

> 15. The method of claim 14, wherein the targeted content was chosen by the requestor based on demographic information within the transmitted user information.

Ex. 1001, 18:38–39.

With respect to claim 15, Petitioner argues,

> In *Harada*, "a tourist information web server may customize a page based user profile data specifying a browser user's age, and interest." Ex. 1004, 7:8–9. *Roker* similarly discloses that its method "can be used to deliver localized content (e.g., advertisements) based on demographic and geo-targeted information." Ex. 1005, 28:23–25. A POSA would have understood that both references teach or suggest that the targeted content was "chosen by the requestor," as claimed, because in *Harada*, "tourist information web server" determines the content, Ex. 1004, 7:8–9, and in *Roker*, the "destination server" of the content provider determines the content sent to the user. *Id.*, 21:2–4. Ex. 1010 ¶ 132.

Pet. 48.

With respect to dependent claim 15, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has

failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 15 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes that a web server may customize a page based user profile data specifying a browser user's age, and interest, and that Roker describes a method that can be used to deliver localized content (e.g., advertisements) based on demographic and geo-targeted information.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 14, wherein the targeted content was chosen by the requestor based on demographic information within the transmitted user information."

k. Claim 16

Dependent claim 16 reads as follows:

> 16. The method of claim 14, wherein the targeted content was chosen by the requestor based on geographic information within the transmitted user information.

Ex. 1001, 18:32–34.

With respect to claim 16, Petitioner argues,

> *Harada* discloses that the user profile included in the augmented HTTP request includes geographic information (i.e., "ZipCode"). Ex. 1004, 6:24–26. [] *Harada's* profile information is used by the content server "to generate or customize data sent in response 213 to the proxy server for forwarding as a response 214 to a user or client computer (step 425)." *Id.*, 7:3–8. Ex. 1010 ¶ 133.

> Similarly, *Roker's* method "can be used to deliver localized content (e.g., advertisements) based on demographic and geo-targeted information about the subscriber." Ex. 1005, 28:23–25. "For example, service providers could include advertisements from local advertisers looking to access their customer base; from global advertisers looking to access their market region; or from content providers looking to access the service provider's local market." *Id.*, 28:25–29:1. Ex. 1010 ¶ 133.
>
> A POSA would have had reason to have the "requester," i.e., the web server/content provider or the third party ad server in the combination of *Harada* and *Roker*, determine the targeted content based on geographic information because (a) both teach that the destination site can use profile information to deliver targeted content, Ex. 1004, 7:6–9; Ex. 1005, 21:2–4, and (b) [] it was common to have either the web server itself or a third party ad service determine targeted content based on profile information. Ex. 1010 ¶ 134.

Pet. 49.

With respect to dependent claim 16, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for [] dependent claims [2-7, 10-11, and 14-16]." Resp. 43.

Patent Owner's argument with respect to claim 16 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

We agree with Petitioner that Harada describes that a user profile included in the augmented HTTP request can include geographic information such as a zip code, and that Harada's profile information is used

by the content server to generate or customize data sent in response to the proxy server for forwarding as a response to a user or client computer. We also agree with Petitioner that Roker describes a method that can be used to deliver localized content (e.g., advertisements) based on demographic and geo-targeted information about the subscriber.

We find, therefore, that the combination of Harada and Roker teaches or suggests "[t]he method of claim 14, wherein the targeted content was chosen by the requestor based on geographic information within the transmitted user information."

4. Obviousness over Harada and Roker in combination with Short, Parekh, Mathai, or Microsoft – Dependent Claims 8–9, 11–13, 17–19

a. Claim 8

Dependent claim 8 reads as follows:

> 8. The method of claim 5, wherein the determined user preferences include: profile data, browsing patterns, site preferences, product preferences, consumption preferences, or service preferences.

Ex. 1001, 17:66–18:3.

For claim 8, Petitioner relies on the combination of Harada, Roker, and Parekh. Petitioner argues,

> *Harada* and *Roker* disclose that user "interest[s]" and "user preferences," respectively, are included within the profile information stored for the user. Ex. 1005, 5:15, 7:7–8, 8:5–7. *Roker* further discloses that the information included in the outgoing user data request message also may include "browsing characteristics of the user," *id.*, 10:18–21. *Roker's* method further includes "the act of examining the browsing data, and recording user specific chronology about the behavior of the user.

> This may include, but is not limited to, the following: performing user modeling; recording performance of advertising; or analyzing segment browsing behavior." *Id.*, 13:9–11.
>
> *Parekh* discloses creating a user profile "based upon the Internet users' interactions with the various web sites 60 … includ[ing, but not limited to] the types of web sites 60 visited, pages hit such as sports sites, auction sites, news sites, e- commerce sites, geographic information, bandwidth information, and time spent at the web site 60." Ex. 1007, 31:10–18. A POSA would have understood that the information enumerated in *Parekh* includes at least "browsing patterns" and "site preferences," as claimed, and would have had reason to include such information in the user profile in the combination of *Harada* and *Roker* because examining such information would lead to better precision and flexibility in targeting content such as advertisements to users while avoiding redundancy and reducing errors, which is an object of both *Harada* and *Roker*. Ex. 1010 ¶ 162 (citing Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26); *KSR*, 550 U.S. at 417 (holding that it is likely obvious to apply a known technique to "improve similar devices in the same way").

Pet. 60–61.

With respect to claim 8, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 8 is not persuasive for

the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims. *Id.* at 48.

This argument is also not persuasive. Reliance on multiple references, in and of itself, does not militate against a finding of obviousness. *See In re Gorman*, 933 F.2d 982 (Fed. Cir. 1991). Moreover, it must be recognized that "[a]ny judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning, but so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made and does not include knowledge gleaned only from applicant's disclosure, such a reconstruction is proper." *In re McLaughlin*, 443 F.2d 1392, 1395 (CCPA 1971).

Patent Owner further argues, "*Parekh* does not address the shortcomings of *Harada* and *Roker* addressed herein, and given that both *Harada* and *Roker* seek to deliver targeted content, *Parekh* does not meaningfully add to their disclosures with respect to the challenged claims." Resp. 49 (citing Ex. 2002 ¶ 105).

The general nature of Patent Owner's criticism with regard to Petitioner's proposed combination of Harada, Roker, and Parekh, and the lack of particularities as to what, precisely, is wrong or improper with Petitioner's combination, makes Patent Owner's argument impossible to analyze substantively and weigh, rendering it unpersuasive.

We agree with Petitioner that the combination of Harada, Roker, and Parekh describes creating profiles with user preferences, including web sites

visited, pages hit such as sports sites, auction sites, news sites, e-commerce sites, geographic information, bandwidth information, and time spent on each.

We find, therefore, that the combination of Harada, Roker, and Parekh teaches or suggests "[t]he method of claim 5, wherein the determined user preferences include: profile data, browsing patterns, site preferences, product preferences, consumption preferences, or service preferences."

b. Claim 9

Dependent claim 9 reads as follows:

> 9. The method of claim 5, wherein the determined user preferences include: user network usage information, the user network usage information including one or more of: usage frequency, usage patterns, length of sessions, or time of use.

Ex. 1001, 18:4–8.

For claim 9, Petitioner relies on the combination of Harada, Roker, and Parekh. Petitioner argues,

> *Harada* discloses that the encrypted data included in field 305 of the HTTP header may include a timestamp, which is used to determine the time of the user's data request. Ex. 1004, 11:17–21. A POSA would have understood that the timestamp in *Harada* indicates the "time of use" of the network, as claimed in one of the Markush options in claim 9, because the time information works to prevent replay attacks by comparing the time of the user's request against the current time and will trigger denial of the request or other security procedures if that time difference is larger than an acceptable threshold. *Id.*; Ex. 1010 ¶ 163.
>
> *Parekh* discloses creating a profile of user preferences that includes "the types of web sites

> 60," the "pages hit" and "time spent at the web site 60." Ex. 1007, 31:10– 18; *see also id.*, 33:10–15 (referring to previous hits on e-commerce sites and sports sites). A POSA would have understood that this information comprises "user network usage information" including at least "usage patterns" and "length of sessions," as claimed, and would have had reason to include such information among the user preferences stored in the combination of *Harada* and *Roker* because examining such information would lead to better precision and flexibility in targeting content such as advertisements to users while avoiding redundancy and reducing errors, which is an object of both *Harada* and *Roker*. Ex. 1010 ¶ 164 (citing Ex. 1004, 2:20–26, 4:20–22; Ex. 1005, 1:3–4, 1:11–15, 4:7–9, 18:10–26).

Pet. 61–62.

With respect to claim 9, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 9 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims. *Id.* at 48.

Patent Owner further argues, "*Parekh* does not address the shortcomings of *Harada* and *Roker* addressed herein, and given that both

Harada and *Roker* seek to deliver targeted content, *Parekh* does not meaningfully add to their disclosures with respect to the challenged claims. *Id.* at 49 (citing Ex. 2002 ¶ 105).

These arguments are also not persuasive for the reasons stated *supra* with respect to claim 8.

We agree with Petitioner that the combination of Harada, Roker, and Parekh describes creating profiles with user preferences such as the types of web sites visited, the web pages hit, and time spent at each web site.

We are persuaded, therefore, that the combination of Harada, Roker, and Parekh teaches or suggests "[t]he method of claim 5, wherein the determined user preferences include: user network usage information, the user network usage information including one or more of: usage frequency, usage patterns, length of sessions, or time of use."

c. Claim 11

Dependent claim 11 reads as follows:

> 11. The method of claim 10, wherein generating the user identifier includes performing a one-way hashing operation on the unique device identifier to generate the local user identifier.

Ex. 1001, 18:12–15.

For claim 11, Petitioner relies on the combination of Harada, Roker, and Microsoft. Petitioner argues,

> *Roker* teaches that, although a static IP address is one example, the method used to uniquely identify the network device is "arbitrary as it is often a unique method used by each service provider's network." Ex. 1005, 16:10–16. A POSA therefore would have had reason to use other known device identifiers to uniquely identify a user's device. Ex. 1010 ¶ 173.

> *Microsoft* discloses that several other known device identifiers, related to the PC's hardware components existed, such as a "Network Adapter MAC Address." Ex. 1009, p.7. In order to protect the user's privacy, however, these device identifiers should be run through a one-way hash. *Id.*, p.6; Ex. 1010 ¶ 174.
>
> *Roker* teaches that it is important to "obscure the identity of the user's profile … to ensure that acceptable levels of privacy are maintained" because the augmented "request can be further intercepted along its path by other" devices. Ex. 1005, 12:6–8, 17:27–28. *Harada* discloses "hash[ing]" information from the client HTTP request "to make forging or tampering more difficult." Ex. 1004, 11:22–23. A POSA "would have had reason to apply the disclosed hashing technique to any device identifiers, such as a MAC address, to protect user privacy before the request left the service provider's network because hashing was one well-known way to obscure information for privacy and security." 7 Ex. 1010 ¶ 175; *KSR*, 550 U.S. at 417. Indeed, this is the precise reason for the one-way hash in the '314 patent.

Pet. 65–67.

With respect to claim 11, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 11 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

This argument is also not persuasive for the reasons stated *supra* with respect to claim 8.

Patent Owner further argues, "*Microsoft* (Ground V; Claim 11) is directed to addressing software piracy, and utilizes an 'installation ID' made up of 'the product ID and a hardware hash' to do so. Resp. 49–50 (citing Ex. 1009, 6). A person of ordinary skill in the art, Patent Owner argues, "would not have looked to *Microsoft's* methods for combating piracy for additional guidance regarding identifiers in Petitioner's combination of *Harada* and *Roker*." *Id.* at 50 (citing Ex. 2002 ¶ 107).

In its Reply, Petitioner argues,

> *Microsoft* teaches that the disclosed features are "designed to guarantee anonymity." Ex. 1009, p. 6. Nothing in *Microsoft* limits the disclosure to piracy. *Roker* recognizes the benefit of obscuring the user's profile "to ensure that acceptable levels of privacy are maintained," and *Harada* discloses hashing information "to make forging or tampering more difficult." Pet. 66 (quoting Ex. 1005, 12:6–8; Ex. 1004, 11:22–23). Thus all three references suggest the desirability of ensuring user privacy and thus a POSA seeking to implement the privacy teachings of *Roker* would look to *Microsoft*. Pet. 66 (citing Ex. 1010 ¶ 175).

Reply 23.

We agree with Petitioner that the combination of Harada, Roker, and Microsoft describes creating a user identifier by using unique device

identifiers, such as a MAC address, run through a hashing operation to protect the user's privacy. We also agree with Petitioner Harada, Roker, and Microsoft all discuss the desirability of privacy and that a person of ordinary skill in the art seeking to implement the privacy teachings of Roker would look to Microsoft.

We are persuaded, therefore, that the combination of Harada, Roker, and Microsoft teaches or suggests "[t]he method of claim 10, wherein generating the user identifier includes performing a one-way hashing operation on the unique device identifier to generate the local user identifier."

d. Claim 12

Dependent claim 12 reads as follows:

> 12. The method of claim 10, further comprising verifying a right of the client computing device based in part on the unique device identifier.

Ex. 1001, 18:17–19.

For claim 12, Petitioner relies on the combination of Harada, Roker, and Short. Petitioner argues,

> *Roker* discloses that one type of profile information that may be inserted into the user's request message may be "rules about how or why certain content should be placed." Ex. 1005, 10:18–23. In particular, *Roker's* network device "may alter the response by blocking said response," *id.*, 5:19, or "add, remove or block selected information in the HTTP stream." *Id.*, 11:21–23. This is useful, for example, to perform "[c]ontent filtering… to block or alter web pages before they are sent to a subscriber's computer." *Id.*, 29:5–11.

> *Short* discloses a system to manage rights to view content "that enables a content provider to regulate the distribution of digital content and to regulate the use of digital content subsequent to distribution." Ex. 1006, ¶ 7. In particular, *Short* governs access to digital content by retrieving a unique identifier associated with the client device, and using that identifier to generate an encryption key to encrypt information associated with the digital content. *Id.*, ¶¶ 60–63. The encrypted information can be unlocked only by the authorized client device. *Id.*, ¶ 69.
>
> A POSA would have had reason to implement rules-based blocking of content (i.e., "verifying a right") in the combination of *Harada* and *Roker*, by using a system that verifies a right of the client device based on a unique device identifier, as claimed, as disclosed by *Short*, to control the type of content shown to the user based on user profile information. Ex. 1010 ¶ 159; *KSR*, 550 U.S. at 416 ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). This is consistent with *Roker's* purpose to "customize the browsing experience for the benefit of the user or content provider 40," Ex. 1005, 10:21–22, and to improve the user's "browsing experience." *Id.*, 18:15; Ex. 1010 ¶¶ 156–159.

Pet. 58–59.

With respect to claim 12, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 12 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

This argument is also not persuasive for the reasons stated *supra* with respect to claim 8.

Patent Owner further argues,

> *Short* (Ground II; Claims 12–13) is directed to "a digital rights management (DRM) approach that enables a content provider to regulate the distribution of digital content and to regulate the use of the digital content subsequent to distribution." *See, e.g.*, Ex. 1006, ¶ 7. The cited disclosures of Short are not generally related to delivery of targeted content, but instead generally focuses on delivery of custom ringtones and sounds to phones and DRM protection of that content, and a POSITA would not have looked to *Short* for addition of the cited portions to the combination of *Harada* and *Roker*. *See e.g.*, Ex. 1006, ¶¶ 4, 63, 69; Ex. 2002 ¶ 104.

Resp. 48–49.

However, Mr. Gray testifies that

> [a] person skilled in the art would have had reason to implement rules-based blocking of content (that is, "verifying a right") in the combination of *Harada* and *Roker*, by using a system that verifies a right of the client device based on a unique device identifier as disclosed by *Short*. This would provide the predictable result of allowing control over the type of content shown to the user based on user profile information. This is consistent with *Roker's*

> purpose to "customize the browsing experience for the benefit of the user or content provider 40," Ex. 1005, 10:21–22, and to improve the user's "browsing experience." Ex. 1005, 18:15.

Ex. 1010 ¶ 158–159.

Two tests define the scope of analogous prior art: (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. *In re Klein*, 647 F.3d 1343, 1348 (Fed. Cir. 2011).

The abstract of the '314 patent explains that the "[e]mbodiments within describe a system and method of tagging network traffic with relevant user information for facilitating the delivery of directed media." Ex. 1001, Abstract. The '314 patent goes on to explain that "[t]he ability to provide directed or targeted message delivery to users based on network access is of critical importance to content providers, such as online advertisers. *Id.* at 1:28–29.

Short explains, "[t]here is a growing trend to deliver content in digital form. Today, more and more digital content is being delivered online over private and public networks, such as intranets, the Internet, cable television networks, telephone networks, and digital radio networks." Ex. 1006, ¶ 2. Short goes on to explain, "[t]here is also a need for systems and methods for enabling the content owner or provider to deliver digital content tailored to the preferences of the user (i.e. the intended audience) to the client device." *Id.* ¶ 6.

Based on the similarity of these two references, we find that Short and the '314 patent are from the same general field of endeavor, i.e. providing

directed or targeted digital content to users over a network. Moreover, Mr. Gray's testimony provides a sufficient reason why a person of ordinary skill in the art would have combined the teachings of Harada, Roker, and Short in the manner described by Petitioner.

We are persuaded, therefore, that the combination of Harada, Roker, and Short teaches or suggests "[t]he method of claim 10, further comprising verifying a right of the client computing device based in part on the unique device identifier."

e. Claim 13

Dependent claim 13 reads as follows:

> 13. The method of claim 12, wherein the right of the client computing device determines a time that content may be accessed.

Ex. 1001, 18:20–23.

For claim 13, Petitioner relies on the combination of Harada, Roker, and Short. Petitioner argues,

> *Roker* discloses blocking content based on information in a user's profile. *Roker's* method further allows specialized messages to be dispatched to the user based on, inter alia, "a scheduled time and day" in addition to "a matching condition from the user's profile." Ex. 1005, 21:23–24. A POSA would have understood from this disclosure that access to content can be regulated according to a determined "time that content may be accessed," as claimed, because doing so is consistent with *Roker's* purpose to "customize the browsing experience for the benefit of the user or content provider 40," *id.*, 10:21–22, and to improve the user's "browsing experience." *Id.*, 18:15; Ex. 1010 ¶ 160.

Pet. 59–60.

With respect to claim 13, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 13 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

This argument is also not persuasive for the reasons stated *supra* with respect to claim 8.

Patent Owner further argues,

> *Short* (Ground II; Claims 12–13) is directed to "a digital rights management (DRM) approach that enables a content provider to regulate the distribution of digital content and to regulate the use of the digital content subsequent to distribution." *See, e.g.*, Ex. 1006, ¶ 7. The cited disclosures of *Short* are not generally related to delivery of targeted content, but instead generally focuses on delivery of custom ringtones and sounds to phones and DRM protection of that content, and a POSITA would not have looked to *Short* for addition of the cited portions to the combination of *Harada* and *Roker*. *See e.g.*, Ex. 1006, ¶¶ 4, 63, 69; Ex. 2002 ¶ 104.

Resp. 48–49.

This argument is not persuasive for the reasons stated *supra* with

respect to claim 12.

We agree with Petitioner that the combination of Harada, Roker, and Short describes or suggests how access to content can be regulated based on a scheduled time or day in addition to other condition from a user's profile.

We are persuaded, therefore, that the combination of Harada, Roker, and Short teaches or suggests "[t]he method of claim 12, wherein the right of the client computing device determines a time that content may be accessed."

f. Claim 17

Dependent claim 17 reads as follows:

> 17. The method of claim 16, wherein the targeted content includes information about one or more commercial interests.

Ex. 1001, 18:35–37.

For claim 17, Petitioner relies on the combination of Harada, Roker, and Parekh. Petitioner argues,

> *Harada* discloses that "[f]or example, a tourist information web server may customize a page based user profile data specifying a browser user's age, and interest." Ex. 1004, 7:8–9. *Parekh* discloses targeted content to "be dynamically shown to the user 5 based on the detailed profile of that user 5," Ex. 1007, 32:6–7, including, for example "an offer to buy an umbrella" or "sports items for sale … such as surf boards." *Id.*, 33:5– 3. This allows for "more customized experiences for users at e-commerce and information sites." *Id.*, 33:13–15.
>
> A POSA would have understood that "tourist information" and information about items offered for sale and "advertisement choices" are "commercial interests," as claimed, because both tourism and offers for sale are typically profit-

> making forms of commerce. A POSA would have had reason to include information about items for sale among the targeted advertising content provided in the combination of *Harada* and *Roker* because increasing sales is the purpose of targeted advertising. Ex. 1010 ¶¶ 165–167.

Pet. 62–63.

With respect to claim 17, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 17 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

Patent Owner further argues, "*Parekh* does not address the shortcomings of *Harada* and *Roker* addressed herein, and given that both *Harada* and *Roker* seek to deliver targeted content, *Parekh* does not meaningfully add to their disclosures with respect to the challenged claims." *Id.* at 49 (citing Ex. 2002 ¶ 105).

These arguments are also not persuasive for the reasons stated *supra* with respect to claim 8.

We agree with Petitioner that the combination of Harada, Roker, and Parekh describes providing targeted content to a user based upon the user's

profile, including, for example, information or offers to purchase products that may be of interest to the user.

We are persuaded, therefore, that the combination of Harada, Roker, and Parekh teaches or suggests "[t]he method of claim 16, wherein the targeted content includes information about one or more commercial interests."

g. Claim 18

Dependent claim 18 reads as follows:

> 18. The method of claim 16, wherein the targeted content includes information about a location itself.

Ex. 1001, 18:38–39.

For claim 18, Petitioner relies on the combination of Harada, Roker, and Parekh. Petitioner argues,

> *Harada* discloses that "[f]or example, a tourist information web server may customize a page based user profile data specifying a browser user's age, and interest." Ex. 1004, 7:8–9. *Roker* discloses that targeted content may be "advertisements from local advertisers looking to access their customer base" or "content providers looking to access the service provider's local market." Ex. 1005, 28:25–29:1. *Parekh* discloses a specific example in which "the web site sends Alice a web page that is tailored for her geographic location, for instance it contains the Atlanta weather forecast and the new headlines for Atlanta." Ex. 1007, 32:14–18.
>
> A POSA would have had reason to include information about a geographic location itself, as claimed, such as the local weather and news, among the targeted content provided in the combination of *Harada* and *Roker*, along with, for example, the "tourist information" as disclosed in *Harada* or

> advertisements from local advertisers looking to access their customer base or service providers looking to access a local market as in *Roker*, because including such information is more useful to the user and thus more likely to accomplish the purpose of effectively targeting content based on user profile information. Ex. 1010 ¶¶ 168–169.

Pet. 63–64.

With respect to claim 18, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 18 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

Patent Owner further argues, "*Parekh* does not address the shortcomings of *Harada* and *Roker* addressed herein, and given that both *Harada* and *Roker* seek to deliver targeted content, *Parekh* does not meaningfully add to their disclosures with respect to the challenged claims." *Id.* at 49 (citing Ex. 2002 ¶ 105).

These arguments are also not persuasive for the reasons stated *supra* with respect to claim 8.

We agree with Petitioner that the combination of Harada, Roker, and Parekh describes providing targeted content to a user based upon the user's

profile, including, for example, web pages that are tailored to a user's geographic location.

We are persuaded, therefore, that the combination of Harada, Roker, and Parekh teaches or suggests "[t]he method of claim 16, wherein the targeted content includes information about a location itself."

h. Claim 19

Dependent claim 19 reads as follows:

> 19. The method of claim 17, wherein the targeted content includes information about local events.

Ex. 1001, 18:40–41.

For claim 19, Petitioner relies on the combination of Harada, Roker, and Mathai. Petitioner argues,

> *Harada* discloses that "[f]or example, a tourist information web server may customize a page based user profile data specifying a browser user's age, and interest." Ex. 1004, 7:8–9. *Roker* discloses that targeted content may be "advertisements from local advertisers looking to access their customer base" or "content providers looking to access the service provider's local market." Ex. 1005, 28:25–29:1.
>
> *Mathai* discloses a system that enables targeted delivery of content to users based on a user's profile information and usage history. Ex. 1008, Abstract. The targeted content may include information about the user's local area, including "local events and happenings" such as "local concerts and other music-related events" and "online ticket sales for local events." *Id.*, 7:6–12, 23:25–24:1, 24:24.
>
> A POSA would have had reason to include information about local events in the combination of *Harada* and *Roker* because *Mathai* teaches that such content "allows advertisers to directly engage

> potential customers," *id.*, 6:6, and providing such content is one effective way to accomplish the purposes stated in *Harada* and *Roker*, for example, "to tailor and deliver[] localized and personalized content to individual users." Ex. 1005, 10:2; Ex. 1010 ¶¶ 170–172; *KSR*, 550 U.S. at 417 (holding that it is likely obvious to apply a known technique to "improve similar devices in the same way").

Pet. 64–65.

With respect to claim 19, Patent Owner argues, "Petitioner has failed to demonstrate that independent Claim 1 would have been obvious based on the combination of *Harada* and *Roker*. Therefore, Petitioner has failed to prove obviousness by a preponderance of the evidence for the dependent claims [8–9, 11–13, 17–19] addressed in Petitioner's Grounds II-V (which also depend from Claim 1)." Resp. 47.

Patent Owner's argument with respect to claim 19 is not persuasive for the reasons discussed *supra* with respect to independent claim 1.

Patent Owner also argues, "the necessity of Petitioner's reliance on four additional references (*Short, Parekh, Mathai,* and *Microsoft*)—all for challenged claims that depend from Claim 1—demonstrates Petitioner's hindsight reliance on the roadmap of the challenged claims." *Id.* at 48.

This argument is also not persuasive for the reasons stated *supra* with respect to claim 8.

Patent Owner further argues,

> *Mathai* (Ground IV; Claim 19), is directed to "a network of publicly accessible terminals located in public spaces" that users access with a "system access card having a unique serial number" and where the system utilizes codes relate to the terminal that pinpoint the user's location when at that terminal. *See, e.g.*, Ex. 1008, 8:4–9, 11:13–15.

> Petitioner relies on *Mathai* for targeted content including "information about local events," but in *Mathai*, the users change location; the terminals do not. A POSITA would not have looked to the public terminal system of *Mathai* to address "information about local events" in the combination of *Harada* and *Roker*. *See also* Ex. 2002 ¶ 106.

Resp. 49.

Mathai, like Harada and Roker, is directed to delivering targeted content to a user. Ex. 1008, 7:11–12 (stating that the system can provide "personalized content related to user-identified interests."). Patent Owner does not explain why it matters whether the terminal or the user changes location with respect to one of ordinary skill in the art consideration of using Mathai. Mr. Smoot explains that a person of ordinary skill in the art "would not have considered *Mathai's* disclosure as particularly applicable . . . because of the very different architecture of *Mathai*." Ex. 2002 ¶ 106. Mr. Smoot, however, does not identify this "different architecture" or explain why any such difference would have discouraged a person of ordinary skill in the art from considering or applying Mathai in the manner proposed by Petitioner.

Petitioner argues that in either case, "information about local events" might be relevant content to deliver to the user. Reply. 22. Petitioner points out that this comports with one of the goals of Roker—"to tailor and deliver[] localized and personalized content to individual users." *Id.* (citing Ex. 1005, 10:2; Ex. 1010, ¶¶ 170–72).

We agree with Petitioner that the combination of Harada, Roker, and Mathai describes targeted content that includes information about local events. We are persuaded, therefore, that the combination of Harada, Roker, and Mathai teaches or suggests "[t]he method of claim 17, wherein the

targeted content includes information about local events."

III. CONCLUSION

Based on the complete record, we determine that Petitioner has established by a preponderance of the evidence that claims 1–7, 10, 11, 14–16, 20, and 21 are unpatentable under 35 U.S.C. § 103 as obvious over the combined teachings of Harada and Roker. We also determine that Petitioner has established by a preponderance of the evidence that claims 12 and 13 are unpatentable over the combined teachings of Harada, Roker, and Short; claims 8, 9, 17, and 18 are unpatentable over the combined teachings of Harada, Roker, and Parekh; claim 19 is unpatentable over the combined teachings of Harada, Roker, and Mathai; and claim 11 is unpatentable over the combined teachings of Harada, Roker, and Microsoft.

IV. ORDER

For the reasons given, it is

ORDERED that claims 1–21 of the '314 patent are unpatentable; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of the Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Jay I Alexander
Peter P. Chen
COVINGTON & BURLING LLP
jalexander@cov.com
pchen@cov.com

PATENT OWNER:

Lauren N. Robinson
Denise M. De Mory
Christina M. Finn
BUNSOW DE MORY LLP
lrobinson@bdiplaw.com
ddemory@bdiplaw.com
cfinn@bdiplaw.com