

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FACEBOOK, INC.,
Petitioner,

v.

WINDY CITY INNOVATIONS LLC,
Patent Owner.

Case IPR2016-01155¹
Patent 8,694,657 B1

Before KARL D. EASTHOM, DAVID C. McKONE, and
MELISSA A. HAAPALA, *Administrative Patent Judges*.

McKONE, *Administrative Patent Judge*.

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

¹ Case IPR2017-00622 has been joined with this proceeding.

I. INTRODUCTION

A. Background

Microsoft Corporation filed a Petition (Paper 1, “Pet.”) to institute an *inter partes* review of claims 1, 2, 18, 27, 35, 43, 51, 65, 79, 93, 100, 108, 114, 126, 138, 150, 156, 168, 170, 172, 176, 178, 180, 182–90, 202, 208, 214, 220, 226, 238, 250, 262, 268, 274, 280, 292, 304, 316, 322, 328, 334, 336, 340, 342, 344, 346, 348, 350, 352–54, 362, 366, 370, 374, 378, 386, 394, 402, 406, 410, 414, 422, 430, 438, 442, 450, 452, 454, 456, 458, 460, 462, 464–66, 476, 481, 486, 491, 496, 505, 515, 525, 530, 535, 545, 555, 565, 570, 580, 582, 584, 586, 588, 590, 592, 594, 596–98, 606, 607, 615–17, 619, 621, 622, 624–26, 628, 630, 632–34, 636, 638, 640–42, 644, 646, and 648–71 of U.S. Patent No. 8,694,657 B1 (Ex. 1001, “the ’657 patent”).

Windy City Innovations LLC (“Patent Owner”) filed a Preliminary Response (Paper 9, “Prelim. Resp.”).

Pursuant to 35 U.S.C. § 314, in our Institution Decision (Paper 12, “Dec.”), we instituted this proceeding as to each of these challenged claims.

Patent Owner filed a Patent Owner’s Response (Paper 27, “PO Resp.”), and Petitioner filed a Reply to the Patent Owner’s Response (Paper 44, “Reply”).

Between the PO Response and the Reply, Facebook, Inc. (“Petitioner”) filed a Petition (IPR2017-00622, Paper 2, “Joinder Pet.”) for *inter partes* review of claims 189 and 465 of the ’657 patent in IPR2017-00622 along with a Motion for Joinder with this proceeding (IPR2017-0622, Paper 3). Before we ruled on the Motion for Joinder, Microsoft and Patent Owner settled and moved to terminate this proceeding. Paper 29. We granted the Motion to Terminate as to Microsoft, but not as to Patent Owner.

Paper 31. Subsequently, we instituted an *inter partes* review of claims 189 and 465 in IPR2017-0622, granted Petitioner's motion for joinder, and dismissed all challenged claims except for 189 and 465. Paper 32 ("Joinder Dec."). We then denied the Motion to Terminate as to Patent Owner.

Paper 33. We also denied a Request for Rehearing of our decision denying the Motion to Terminate. Paper 53.

Petitioner relies on the Declarations of Christopher M. Schmandt (Ex. 1003, "Schmandt Decl."; Ex. 1100, "Schmandt Reply Decl."). Patent Owner relies on the Declaration of Jaime G. Carbonell, Ph.D. (Ex. 2006, "Carbonell Decl.>").

An oral argument was held on October 19, 2017 (Paper 62, "Tr.>").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 189 and 465. Based on the record before us, Petitioner has proved, by a preponderance of the evidence, that claims 189 and 465 of the '657 patent are unpatentable.

B. Related Matters

The parties indicate that the '657 patent has been asserted in *Windy City Innovations, LLC v. Microsoft Corp.*, Civ. A. No. 15-cv-00103-GM (W.D.N.C.) (transferred to 16-cv-1729 (N.D. Cal.)), and *Windy City Innovations, LLC v. Facebook, Inc.*, Civ. A. No. 15-cv-00102-GM (W.D.N.C.) (transferred to 16-cv-1730 (N.D. Cal.)). Pet. 3; Paper 7, 1. The '657 patent also is the subject of an *inter partes* review petition in IPR2016-01159. Pet. 3; Paper 7, 1. Related U.S. Patent Nos. 8,458,245, 8,407,356, and 8,473,552 are subject to additional *inter partes* reviews. Pet. 3.

C. Asserted Prior Art References

Petitioner relies on the following prior art:

U.S. Patent No. 5,941,947, issued Aug. 24, 1999, filed Aug. 18, 1995
(Ex. 1012, “Brown”); and

Donath & Robertson, *The Sociable Web* (Ex. 1019, “Sociable Web”).²

D. The Instituted Ground

We instituted a trial on the ground of unpatentability of claims 189 and 465 as obvious, under 35 U.S.C. § 103(a), over Brown and Sociable Web. Dec. 36–37; Joinder Dec. 17–18.

E. The ’657 Patent

The ’657 patent describes an Internet “chat room.” According to the ’657 patent, it was known to link computers together to form chat rooms in which users communicated by text, graphics, and multimedia, giving the example of “America On Line.” Ex. 1001, 1:33–37. The ’657 patent acknowledges that chat rooms have been implemented on the Internet, albeit with “limited chat capability,” but contends that the complex chat room communications capable with Internet service providers had not been developed on the Internet because “[t]he Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications” and because “there is no particular control over

² Petitioner also submitted Exhibit 1030, which Petitioner contends is a version of Sociable Web archived by the Internet Archive at <https://web.archive.org/web/19980111061831/http://judith.www.media.mit.edu/SocialWeb/SociableWeb.html>. Pet. 18.

the platform that would be encountered on the Internet.” *Id.* at 1:38–44, 1:50–52.

Figure 1, reproduced below, illustrates an embodiment of the invention:

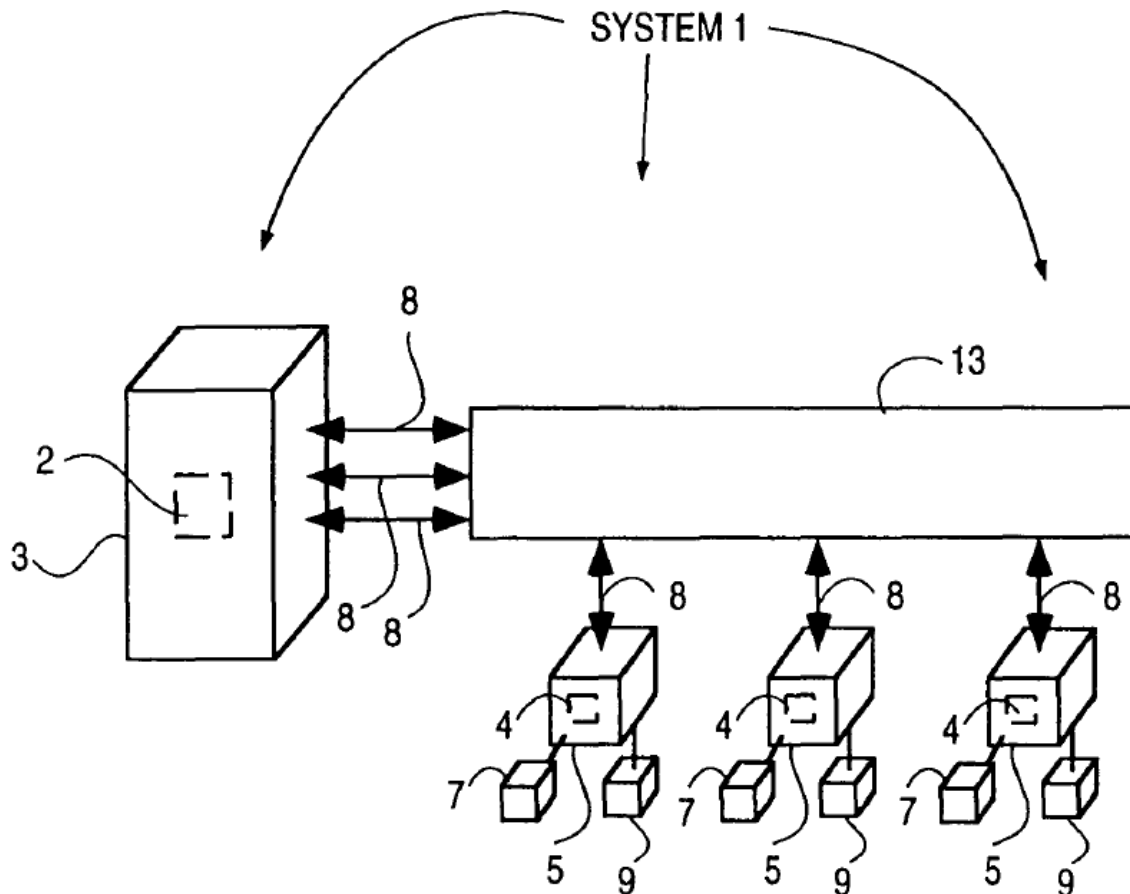


Figure 1 is a block diagram showing the components and data flow of a computerized human communication arbitrating and distributing system. *Id.* at 4:36–40. The system includes controller computer 3 in communication with several participator computers 5 (e.g., IBM-compatible personal computers) over connection 13 (e.g., an Internet connection or a World Wide Web connection). *Id.* at 4:41–60.

Controller computer 3 runs under the control of controller software 2, and the software arbitrates, in accordance with predefined rules (including user identities), which participator computers 5 can interact in a group through the controller computer, and directs real-time data to the members of the group. *Id.* at 4:61–67. The software uses “identity tokens,” or pieces of information associated with user identity, in the arbitration. *Id.* at 7:49–52. The tokens are stored in a memory in a control computer database along with personal information about the users. *Id.* at 7:52–57.

The arbitration can be used to control a user’s ability to join or leave a group of participator computers, to moderate communications involving the group, and to see other users in the group. *Id.* at 7:62–8:6. Arbitration using tokens also can be used to perform censorship:

Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user’s tokens. By checking the tokens, a user’s access can be controlled per group, as well as in giving group priority, moderation privileges, etc.

Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

Id. at 8:11–19.

According to the specification, “[t]he present invention comprehends communicating all electrically communicable multimedia information as Message 8, by such means as pointers, for example, URLs. URLs can point to pre-stored audio and video communications, which the Controller Computer 3 can fetch and communicate to the Participator Computers 5.” *Id.* at 5:11–16.

Claims 189 and 465, reproduced below, are the only claims challenged in this proceeding:

189. A method of communicating via an Internet network by using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method including:

- affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;

- affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity; and

- determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications; and

- determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and

- if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein, for the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and

presenting the content at an output device of the second participator computer, and

if the first user identity is censored from the sending of the data, not allowing sending the data that is censored from the first participator computer to the second participator computer.

465. An Internet network communications system, the system including:

a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the computer system in communication with a first of the participator computers responsive to a first authenticated user identity and with a second of the participator computers responsive to a second authenticated user identity, wherein the computer system

determines whether the first user identity and the second of the user identity are able to form a group to send and to receive real-time communications; and

determines whether the first user identity, is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and

if the user identities are determined to be able to form the group, forms the group and facilitates sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein the computer system facilitates, for the communications which

are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer; and

if the first user identity is censored from sending the data, does not facilitate sending the data that is censored from the first participator computer to the second participator computer.

II. ANALYSIS

A. *Claim Construction*

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–45 (2016). Nevertheless, the '657 patent is expired. “[T]he Board’s review of the claims of an expired patent is similar to that of a district court’s review.” *In re Rambus Inc.*, 694 F.3d 42, 46 (Fed. Cir. 2012) (internal citations omitted). District courts construe claims in accordance with their ordinary and customary meanings, as would be understood by a person of ordinary skill in the art, in the context of the specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

1. Constructions in the Institution Decision

In the Institution Decision, we preliminarily construed the following terms (Dec. 8–15; Joinder Dec. 10):

Claim Term	Preliminary Construction
“token”	“piece of information associated with user identity”
“censor”	“control what is said in a group”
“the first user identity is individually censored from sending data in the communications” ³	refers to control of data sent by the first user identity, individually, and is not limited to data suppressed based on the content of those data or by a moderator
“pointer”	“a link or reference to a file, data, or service”
“a pointer-triggered message on demand” ⁴	“a message, where the content of the message is specified by a pointer and found on demand of the operator of the participator software”

Patent Owner adopts our construction of “token” (which Petitioner initially proposed), PO Resp. 11, and challenges our construction of “censor,” *id.* at 15–16. Petitioner accepts our construction of “censor” and presents arguments in favor of that construction. Reply 5–6. We maintain

³ The Institution Decision (at 12–16) construed the term “the first user identity is individually censored from receiving data in the communications,” recited in claim 1, no longer challenged. The Joinder Decision (at 10) construed the similar term “the first user identity is individually censored from sending data in the communications,” recited in claim 189.

⁴ Neither of the currently challenged claims recites “a pointer-triggered message on demand.”

our construction of “token” on the complete record. We address the construction of “censor,” below, as well as the construction of the related term “the first user identity is individually censored from sending data in the communications.” Neither party challenges our construction of “pointer” and we maintain that construction on the complete record.⁵ Patent Owner also proposes construing “database.” PO Resp. 11–15. We agree with Petitioner (Reply 1–2), however, that Patent Owner does not argue that the construction of “database” affects any disputed issue in this proceeding. Thus, it is not necessary to expressly construe “database” to resolve the parties’ dispute. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.”).

2. “*censor*” / “*the first user identity is individually censored from sending data in the communications*”

Claim 189 recites “determining whether the first user identity is individually censored from sending data in the communications.” Claim 465 includes a similar recitation. As noted above, we preliminarily construed “censor” to mean “control what is said in a group” and explained that “the first user identity is individually censored from receiving data in the communications” refers to control of data received by the first user identity, individually, and is not limited to data suppressed based on the content of those data or by a moderator. Dec. 14–15. In the Joinder Decision (at 10),

⁵ Although this decision analyzes the claims under the *Phillips* standard, in related proceedings, we reach substantially the same constructions of these claim terms under the broadest reasonable interpretation.

we made clear that, for the same reasons as given in the Institution Decision for claim 1, “the first user identity is individually censored from sending data in the communications,” as recited in claim 189, refers to control of data sent by the first user identity, individually, and is not limited to data suppressed based on the content of those data or by a moderator.

We based our construction on the description of that term in the specification. *Id.* at 13–14. Specifically, the specification describes censorship as follows:

Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. *Censorship can control of access to system 1 by identity of the user*, which is associated with the user’s tokens. By checking the tokens, a user’s access can be controlled per group, as well as in giving group priority, moderation privileges, etc.

Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

Ex. 1001, 8:10–19 (emphasis added). Here, the specification describes “censorship” as “broadly encompass[ing] control of what is said in a group” and includes an example in which an action is taken on a user, rather than the data itself.

Patent Owner “proposes that censorship be construed as ‘examine in order to suppress or delete anything considered objectionable.’” PO Resp. 16. According to Patent Owner, “[i]n order to control what is said in a group, it is necessary to first know what is said (or proposed to be said).” *Id.* at 15. Patent Owner argues that this is consistent with the meaning given to “censor” and “censorship” in dictionaries, including “to examine in order to suppress or delete anything considered objectionable” (Webster’s

Collegiate Dictionary (Ex. 2002)) and “[t]he action of preventing material that a party considers objectionable from circulating within a system of communication over which that party has some power” (Microsoft Press Computer Dictionary (Ex. 2003)).

We are not persuaded by Patent Owner’s arguments, which essentially track those presented in the Preliminary Response (at 7–9). The claim language itself does not support a construction of “censor” limited to analysis of the content of data and suppression based on that content. Claim 189 recites “determining whether the first user identity is individually censored from sending data in the communications.” The claim language focuses on censoring a user identity and does not specify that such censoring is based on the content of the data. As explained above, the specification describes censorship as an action taken on a user, rather than the data itself. As explained in the Institution Decision (at 14), extrinsic evidence such as dictionary definitions “may be used only to help the court come to the proper understanding of the claims; it may not be used to vary or contradict the claim language.” *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1584 (Fed. Cir. 1996); *accord Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005) (en banc) (“[W]hile extrinsic evidence can shed useful light on the relevant art, we have explained that it is less significant than the intrinsic record in determining the legally operative meaning of claim language.” (internal citations and quotation marks omitted)).

On the complete record, in accordance with the specification’s definition, “censor” means “control what is said in a group.” In the context of claim 189, for example, “determining whether the first user identity is individually censored from sending data in the communications” refers to

control of data received by first user identity, individually, and is not limited to data suppressed based on the content of those data or by a moderator. We apply the same definition of “censor” in interpreting similar language in claim 465.

B. Asserted Grounds of Unpatentability

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” We resolve the question of obviousness on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.⁶ *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

In an obviousness analysis, some reason must be shown as to why a person of ordinary skill would have combined or modified the prior art to achieve the patented invention. *See Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008). A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the “interrelated teachings of multiple patents”; “any need or problem known in the field of endeavor at the time of invention and addressed by the

⁶ The record does not include arguments or evidence regarding objective indicia of nonobviousness.

patent”; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

1. Level of Ordinary Skill

Relying on Mr. Schmandt’s testimony, Petitioner contends that a person of ordinary skill in the art “would have been a person with a Bachelor of Science degree in Computer Science, or equivalent, with at least two years’ experience designing and programming distributed multimedia computer systems, including experience with teleconferencing and on-line chat systems, such as on-line bulletin boards.” Pet. 5 (citing Ex. 1003 ¶ 140); Joinder Pet. 6. Patent Owner does not contest this statement in its Response. On the complete record, we adopt Petitioner’s statement of the level of ordinary skill.

2. Scope and Content of the Prior Art

Petitioner contends that claims 189 and 465 would have been obvious over Brown, alone or in combination with Sociable Web. Specifically, Petitioner cites Sociable Web for teachings of “via an Internet network” (Pet. 19–20; Joinder Pet. 19–20), “a pointer” (Pet. 28–29; Joinder Pet. 30–31), and “an Internet URL” (Pet. 31; Joinder Pet. 33–34) to the extent we find that those claim limitations are not taught in Brown.

a. Overview of Brown

Brown describes a system and method for controlling user access to content objects, such as bulletin board systems (“BBS”) and chat conferences, in a computer network. Ex. 1012, 2:20–39. User access rights are stored in a database, which is implemented as a relational database on one or more security servers connected to application servers by a local area network (“LAN”). *Id.* at 2:59–66. Access rights data are stored in association with multiple “tokens,” which identify categories or groupings of content objects. *Id.* at 2:66–3:7. Service applications running on application servers query the access rights database to obtain access rights lists of specific users. *Id.* at 3:26–29. A user’s access rights can be categorized in the form of a privilege level (e.g., “viewer,” “user,” “host,” “sysop,” and “supersysop”), which translate into specific sets of access capabilities by the service applications. *Id.* at 3:46–62.

Figure 1, reproduced below, illustrates an example:

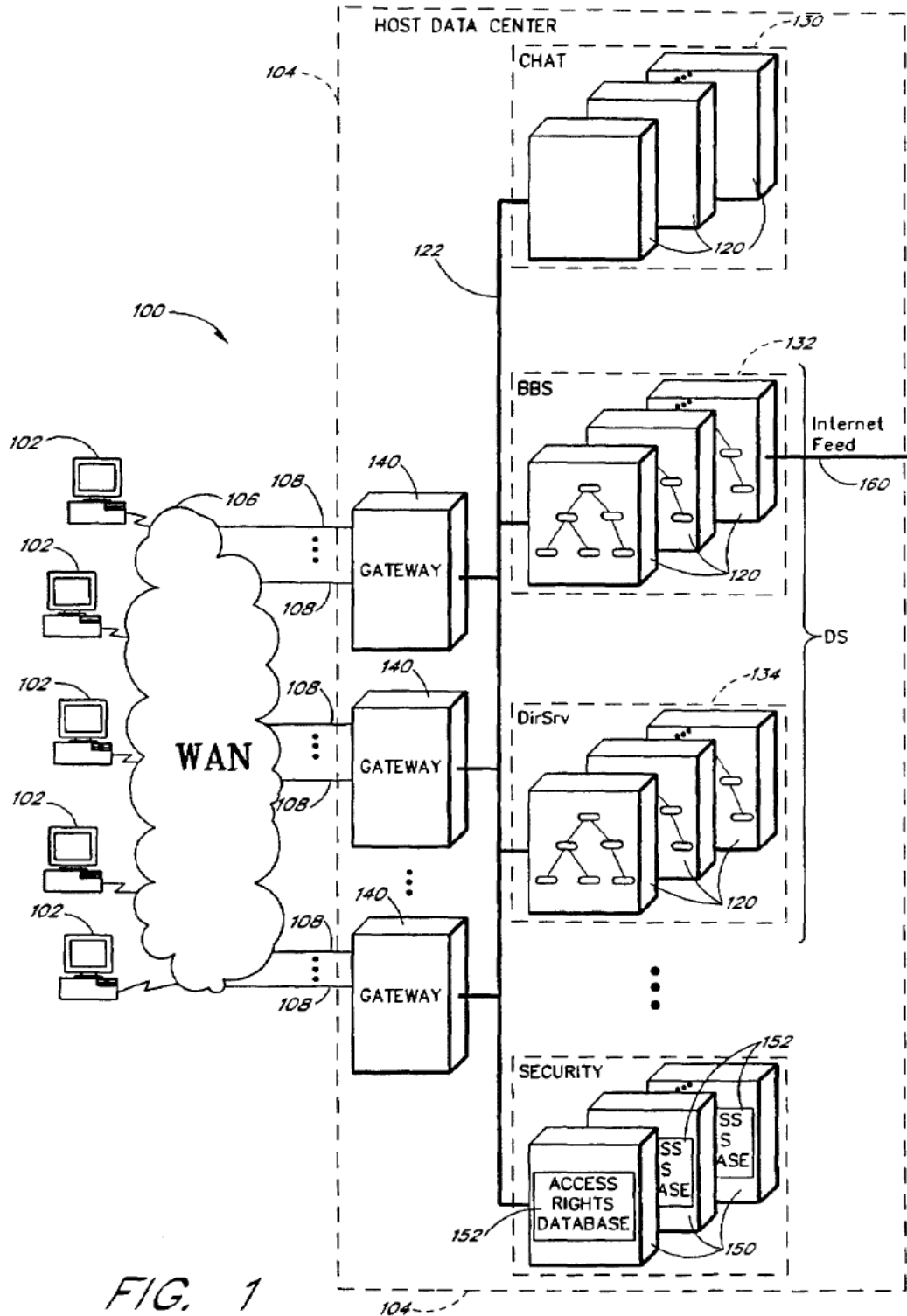


FIG. 1

Figure 1 is a block diagram of the general architecture of an on-line services network. *Id.* at 5:26–28, 6:62–63. On-line services network 100 includes

multiple client computers 102 connected to host data center 104 by wide area network (“WAN”) 106 provided by one or more telecommunications providers. *Id.* at 6:62–7:1. WAN lines 108 of WAN network 106 can include Transmission Control Protocol/Internet Protocol (“TCP/IP”) lines. *Id.* at 7:4–6. Host data center 104 includes application servers 120 arranged into service groups corresponding to on-line services (e.g., CHAT group 130 and BBS group 132) and connected over LAN 122. *Id.* at 7:9–11, 7:18–24. Multiple security servers 150, each maintaining relational database 152, are connected to LAN 122. *Id.* at 7:48–53.

Relational database 152 is organized as a set of two or more interrelated tables that contain the access rights data for all users of on-line services network 100. *Id.* at 7:53–56. Tokens also can correspond to content categories, or groups. *Id.* at 20:1–3. In one example, “[t]he content category ‘Family and Friends for Brown Family’ may similarly be formed to allow private correspondence between a small group of subscribers (e.g., Brown family members plus designated friends), and may contain, for example, Chat and BBS objects which have been designated for this purpose.” *Id.* at 20:19–24, 7:53–56. Brown describes the following example of assigning such access rights:

To provide a specific example, suppose that a system administrator wants to create a Chat room to allow members of a certain organization to carry on an interactive conversation. To create such a Chat room, the system administrator initially creates a Chat room node, specifying a unique security token for the Chat room. The system administrator then updates the group-member table 602 so as to create a new group that consists of the accounts of the members of the organization. (If the group is small, the system administrator may forego creating a new user group, and may alternatively generate one user-specific row in

the account-token table 606 for each member of the organization.) Finally, the system administrator adds a row to the group-token table 604, specifying (1) the group ID of the newly-created user group, (2) the security token of the Chat room, and (3) an appropriate access rights value.

Id. at 31:5–21.

Brown describes its chat service as “an interactive communications service which allows users to have real time conversations with other users on specific topics. Chat conversations or ‘conferences’ are organized as ‘Chat rooms’ which may be entered or exited by end users to join or leave the corresponding conferences.” *Id.* at 9:45–50. According to Brown, “[p]articipants in a Chat conference can type in textual messages which will be displayed on the monitors of other participants. Voice and/or video capabilities may additionally be provided.” *Id.* at 9:52–55.

When a user navigates to a chat room, the Chat service calls an application program interface to determine the rights of the user with respect to the Chat room. *Id.* at 15:66–16:4. Chat servers 120 can generate such calls as a user moves from Chat object to Chat object within the Chat service. *Id.* at 27:28–30. The general privilege levels of the access rights are transformed into specific access capabilities for the on-line service. *Id.* at 17:25–28. “For example, the Chat service may give moderator-type access capabilities to users that have the privilege level of ‘host.’” *Id.* at 17:28–30; *see also id.* at 17:57–60.

b. Sociable Web

(1) Prior art status of Sociable Web

Sociable Web is a paper, archived by the Internet Archive, that Petitioner argues was presented to conference goers along with a live presentation at The Second International WWW Conference '94 in Chicago in late October 1994. Pet. 18. Petitioner contends that Exhibit 1030 is the Internet Archive version of Sociable Web. *Id.* In support of the assertion that Sociable Web was presented at the 1994 conference in Chicago, Petitioner cites to conference proceedings referring to the title of the paper and presenters (Ex. 1021, ix)⁷, and a declaration of one of the authors, Judith Donath (Ex. 1031). Dr. Donath testifies that she presented the paper (Ex. 1019) at the 1994 conference and made the paper available on the conference's website by the time of the conference. Ex. 1031 ¶ 7. Dr. Donath also testifies that the paper was available on her MIT web page at that time. *Id.* ¶ 9.

Patent Owner argues that Petitioner has not shown that Sociable Web is prior art. Specifically, Patent Owner argues that Sociable Web “is a web resource which, on its face, lists a date from the Web Archive in 1998—well after the priority date of the '657 Patent.” PO Resp. 8. Patent Owner further argues that Dr. Donath does not have copies or backups of Sociable Web bearing a date prior to 1998. *Id.* According to Patent Owner, Dr. Donath testified in deposition that there was a time when the images on her web page were not working. *Id.* (citing Ex. 2009, 14:22–15:2). Patent Owner

⁷ Petitioner cites to Exhibit 1015, which is not in the record. This appears to be a typographical error, and we assume that Petitioner intended to cite to Exhibit 1021, which is the document to which Petitioner refers.

also asserts that Dr. Donath was paid by Microsoft and, accordingly, we should give little to no weight to her testimony. *Id.* at 9 (citing Ex. 2009, 10:19–21, 11:3–8).

According to the Federal Circuit, “[b]ecause there are many ways in which a reference may be disseminated to the interested public, ‘public accessibility’ has been called the touchstone in determining whether a reference constitutes a ‘printed publication’” under Section 102. *Kyocera Wireless Corp. v. Int’l Trade Comm’n*, 545 F.3d 1340, 1350 (Fed. Cir. 2008) (quoting *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986)). A reference is publicly accessible “upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008). We assess public accessibility on a case-by-case basis. *See Kyocera*, 545 F.3d at 1350.

In instances of references cataloged in libraries, for example, “competent evidence of the general library practice may be relied upon to establish an approximate time when a thesis became accessible.” *In re Hall*, 781 F.2d at 899. On the other hand, “a printed publication need not be easily searchable after publication if it was sufficiently disseminated at the time of its publication.” *Suffolk Techs., LLC v. AOL Inc.*, 752 F.3d 1358, 1365 (Fed. Cir. 2014). In *Suffolk*, the Federal Circuit concluded that a posting to an internet newsgroup was sufficiently disseminated to those of ordinary skill in the art to be considered publicly accessible, after noting that the posting “elicited at least six responses over the week following its publication” and that “[m]any more people may have viewed the post

without posting anything themselves.” *Id.* The Court further noted: “the record indicates that those of ordinary skill in the art actually were using [the] newsgroups.” *Id.* at 1364. In another example, the Federal Circuit found that a paper presented orally at a technical conference and handed out afterward upon request was publicly accessible where “between 50 and 500 persons interested and of ordinary skill in the subject matter were actually told of the existence of the paper and informed of its contents by the oral presentation, and the document itself was actually disseminated without restriction to at least six persons.” *Mass. Inst. of Tech. v. AB Fortia*, 774 F.2d 1104, 1108–09 (Fed. Cir. 1985) (“MIT”); *cf. In re Klopfenstein*, 380 F.3d 1345, 1347 (Fed. Cir. 2004) (a printed slide presentation displayed continuously for two and a half days at a meeting of a technical association and displayed for less than a day at a university held to be publicly accessible). Discussing the *MIT* case, the *Klopfenstein* court noted that “[t]he key to the court’s finding [in *MIT*] was that actual copies of the presentation were distributed. The court did not consider the issue of indexing.” 380 F.3d at 1349 (citing *MIT*, 774 F.2d at 1108–10).

As stated above, according to Dr. Donath, Sociable Web was presented at the 1994 conference, a premiere conference well-known to those of skill in the art, and was made available to attendees prior to the conference on the conference’s website. Ex. 1031 ¶¶ 7–8. This is similar to the *MIT* and *Klopfenstein* cases, discussed above, in which papers presented at industry and academic conferences were found to be publicly accessible. Dr. Donath also testifies that she posted Sociable Web on her MIT Media Lab webpage prior to the conference and that her webpage was a popular Internet resource. *Id.* ¶ 9. Petitioner introduces uncontested evidence that a

paper by the same name, with the same authorship, was presented at this conference. Ex. 1021, ix. If the version of Sociable Web presented in this proceeding (Ex. 1019) is the same as the document presented at the conference and posted on her website in 1994, that document would have been publicly accessible as of the date of the conference.

Patent Owner is correct that Sociable Web does not bear a date early enough to establish it as prior art and that Dr. Donath has not introduced copies bearing such a date. PO Resp. 8. Nevertheless, Dr. Donath testifies that she reviewed the archived version of Sociable Web on her webpage and concluded that it is identical to the webpage that she posted in 1994. Ex. 1031 ¶ 10. She further testifies that she did not recall making any changes to the webpage between 1994 and the end of 1998. *Id.* We have examined the deposition testimony cited by Patent Owner (PO Resp. 8–9, citing Ex. 2009, 10:19–21, 11:3–8, 14:2–11, 14:22–15:2), including Dr. Donath’s testimony that she was paid by Microsoft, but find nothing to suggest that Dr. Donath’s direct testimony is dishonest or misleading. Rather, her testimony is consistent and credible. As to Patent Owner’s argument that images on Dr. Donath’s webpage were, at some point, not working, Dr. Donath further testified that the text of Sociable Web remained the same and that the substance of the images did not change. Ex. 2009, 14:22–15:25. After considering the evidence of record on this issue, we find that Petitioner establishes, by a preponderance of the evidence, that the copy of Sociable Web asserted in this proceeding (Ex. 1019) is identical to that posted on Dr. Donath’s webpage in 1994 and presented at The Second International WWW Conference ’94 in Chicago in late October 1994.

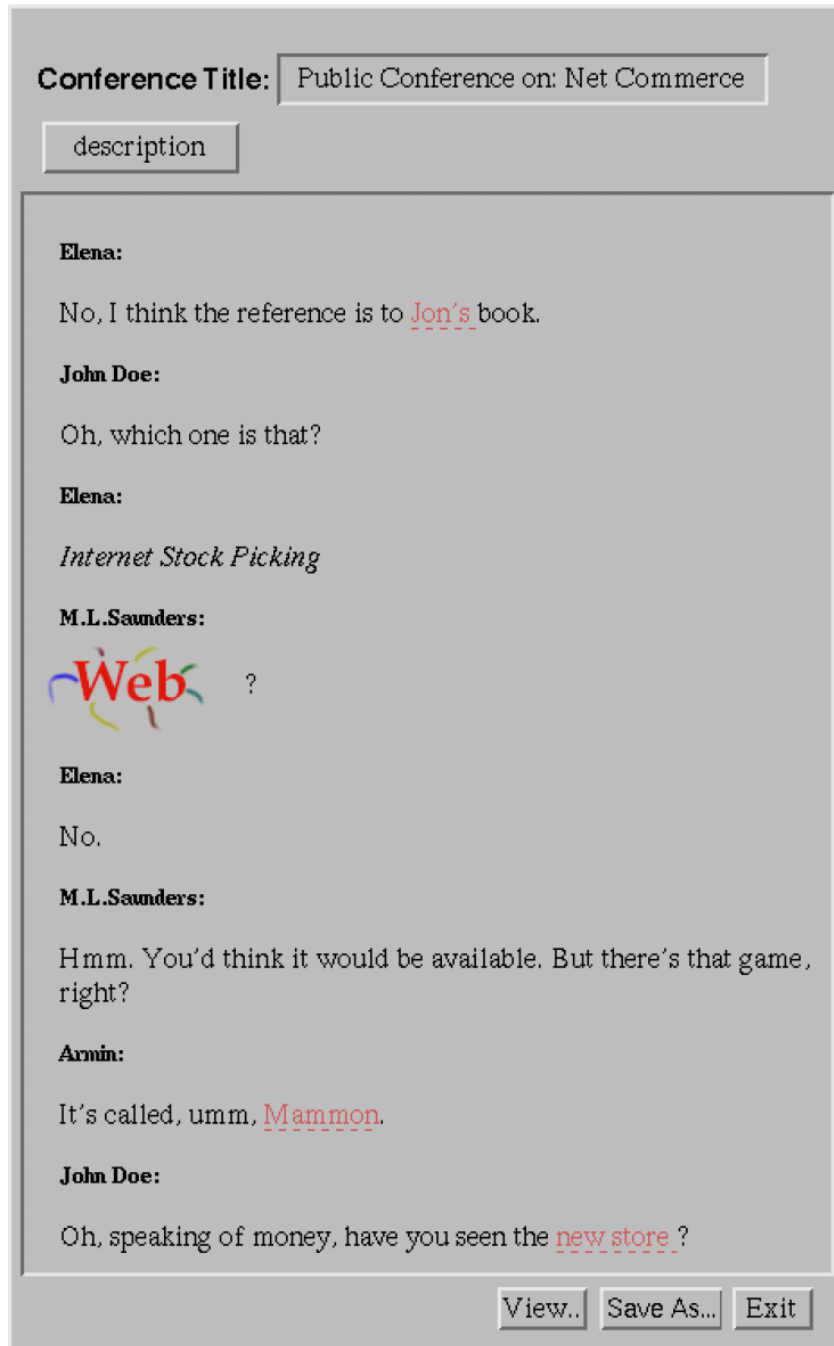
Accordingly, we find that Sociable Web was publicly accessible as of October 1994 and, thus, is prior art to the '657 patent.

(2) Overview of Sociable Web

Sociable Web describes a modified Web browser and server.

Ex. 1019, 2. When the browser visits a Web page not served by a Sociable Web server, the browser behaves as a conventional browser. *Id.* On Web pages served by a Sociable Web server, however, the browser provides social and collaborative features, such as the ability to see who else is visiting the page and to have discussions with them. *Id.* at 2–3.

Using a WebTalk feature, users can have discussions that are live in that, when a user types a message, it appears instantly on the screens of the intended recipients. *Id.* at 3. The figure on page 4, reproduced below, illustrates such a discussion:



Discussion window (try the buttons and links).

The figure reproduced above is a picture of a discussion window. According to Sociable Web,

[i]mages, sounds, and links to other pages can all be integrated with the flow of words. The WebTalk client includes several

tools for fluency in hypertext conversation. For instance, the user can highlight a phrase and then, simply by clicking on a picture (or link) on any Web page, attach the chosen object to the phrase. When the phrase is sent, the recipient sees it as highlighted text; if the recipient clicks on it, he or she will receive the picture (or follow the link).

Id. at 4.

3. *Claim 189, Differences Between the Claimed Subject Matter and the Prior Art, and Reasons to Modify or Combine*

Microsoft's Petition presented the majority of its arguments for claim 1 (no longer challenged) and referenced those arguments for the remaining claims, including claim 189. Pet. 18–37. As explained in the Joinder Decision, at 9–10, claim 189 differs from claim 1 in that, where claim 1 recites “determining whether the first user identity is individually censored from receiving data” and “if the first user identity is censored from the receiving of the data,” claim 189 recites “determining whether the first user identity is individually censored from sending data” and “if the first user identity is censored from the sending of the data.” The Joinder Petition essentially copies the arguments from Microsoft's Petition but maps those arguments to claim 189 specifically. Joinder Pet. 18–35; Joinder Dec. 9. We refer to both petitions below.

a. *“A method of communicating via an Internet network”*

Petitioner contends that the network described in Brown is a WAN that complies with Internet Protocol (“IP”), which is used in Internet networks. Pet. 19; Joinder Petition 19. According to Brown, WAN lines

108 are “provided by one or more telecommunications providers, and which allow end users (i.e., users of the microcomputers 102) over a wide geographic area to access the host data center 104.” Ex. 1012, 6:67–7:4. Brown continues, “[t]he WAN lines 108 may include, for example, X.25 lines, TCP/IP lines, and ISDN (Integrated Service Digital Network) lines. The host data center 104 provides a variety of information-related and communications-related on-line services to end users.” *Id.* at 7:4–8. Mr. Schmandt testifies that “Brown’s disclosure of TCP/IP lines refers to networks implementing the Transmission Control Protocol/Internet Protocol, which [w]as used in Internet networks.” Ex. 1003 ¶ 162. Petitioner, citing Mr. Schmandt’s testimony, argues that Brown’s telecommunications providers would have been connected to, and would have been part of, the Internet. Pet. 19 (citing Ex. 1003 ¶ 163); Joinder Petition 19. Mr. Schmandt gives the example of Sprint providing Internet access via Sprint Link. Ex. 1003 ¶ 163 (citing Ex. 1018, 9).

Patent Owner does not respond meaningfully to this contention. Rather, Patent Owner argues that “Brown does not expressly disclose the Internet for communication as between users and the servers. Instead, the Board instituted based on the teaching in Brown of a ‘WAN’ and IP communications.” PO Resp. 22–23. This argument implies that we did not institute on the basis that Brown alone teaches communication via an Internet network. Nevertheless, we did institute on that basis. Specifically, we explained that, “[a]lthough not expressly stated, Brown’s description of communicating over a WAN, along with disclosure that Internet Protocol is the preferred protocol for such communications, is sufficient evidence at this stage that Brown’s system communicates via an Internet network.” Dec. 25.

In addressing an “overall motivation to combine,” Patent Owner argues that Brown expresses “skepticism” of communication via an Internet network that “can be seen by the fact that Brown explicitly lists the Internet as feeding into its BBS system but does not refer to the Internet for connections to its users.” PO Resp. 23. Patent Owner cites to the testimony of Dr. Carbonell, who repeats this argument without adding to it meaningfully. *Id.* (citing Ex. 2006 ¶ 37).⁸ As we explained in the Institution Decision, we do not draw from Brown’s explicit reference to the Internet in connection with a BBS feature, an implication that Brown’s WAN is not an Internet network. Dec. 25–26.

On the complete record, we find that Brown’s description of communicating via a WAN using TCP/IP teaches “communicating via an Internet network,” as recited in claim 189.

Petitioner further argues that, to the extent that we disagree that Brown teaches communicating via an Internet network, Sociable Web describes a chat system that communicates via the Internet. Pet. 19; Joinder Pet. 19. As Petitioner observes (Pet. 19; Joinder Pet. 19), Sociable Web is directed to adding communicating abilities, including its “WebTalk” chat functionality, to web browsers for communication via the World Wide Web. Ex. 1019, 1–3. According to Sociable Web:

⁸ Patent Owner also cites to paragraphs 35 and 36 of the Carbonell Declaration. These paragraphs do not address any alleged skepticism in Brown and, instead, present additional argument not discussed in the PO Response. Accordingly, we do not consider this additional testimony. See 37 C.F.R. § 42.6(a)(3) (“Arguments must not be incorporated by reference from one document into another document.”).

The main feature of the Sociable Web is WebTalk: the discussions that occur in the context of the Web and that use its rich hypermedia capabilities. WebTalk discussions are live: one types a message and it appears instantly (or at least reasonably fast) on the screens of the intended recipients. The discussions can be public conferences, open to all, or they can be private conversations between two people.

Id. at 3. Patent Owner does not dispute that communications over the World Wide Web would have occurred via the Internet.

Petitioner contends that it would have been obvious to combine Sociable Web's teaching of communication via the Internet with Brown "to expand and efficientize online communications." Pet. 19–20; Joinder Pet. 19–20. We find that Petitioner's reason to combine has rational underpinnings.

Patent Owner argues that a lack of motivation to combine Brown with Sociable Web is evidenced by a half-page article in a technical magazine by Robert Metcalfe, founder of 3Com, "[p]redicting the Internet's catastrophic collapse" at the end of 1995 due to reasons such as low user measurements, telecom company monopolies, and security and capacity concerns. PO Resp. 23–24 (quoting Ex. 2011). Patent Owner offers no persuasive evidence, however, that Dr. Metcalfe's views were shared widely, or at all, by skilled artisans in 1995. Indeed, the article itself suggests the contrary. Ex. 2011 ("Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth.").

Citing Dr. Metcalfe's article, Dr. Carbonell testifies that other technologies such as Integrated Services Digital Network (ISDN) and Asynchronous Transfer Mode (ATM) would have been better suited than the Internet to handle video conferencing in the mid-1990's. Ex. 2006 ¶ 40. As

explained above, Patent Owner has not explained persuasively why Dr. Metcalfe's magazine article is representative of the views of a skilled artisan. The article itself does not state that there were, or identify evidence of, technologies better suited than the Internet to handle videoconferencing. Ex. 2011. Thus, we are not persuaded that the Internet would have been an inferior technology for videoconferencing in 1995. Moreover, claim 189 on its face is not limited to videoconferencing. In any case, the Federal Circuit has explained that "just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes." *In re Mouttet*, 686 F.3d 1322, 1334 (Fed. Cir. 2012).⁹

On the complete record, we find that a skilled artisan would have had reason to modify Brown's system to communicate via an Internet network in light of Sociable Web's description of conducting similar communications over the Internet.

- b. *"by using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method including: "*

Petitioner points to Brown's application servers 120 and client microcomputers 102 as a controller computer and participator computers, respectively. Pet. 20, 22; Joinder Pet. 20, 22. Petitioner argues that Brown's

⁹ Patent Owner also argues that "engineering issues highlighted in Vetter" further weigh against a motivation to combine. Vetter is asserted as a prior art reference in related proceedings, but is not part of the record of this proceeding. Accordingly, Patent Owner's argument is not persuasive.

distribution of chat messages to participants teaches “affording information” to the participator computers. *Id.* at 22–23; Joinder Pet. 22–23. As explained in Brown:

During a typical logon session, a client microcomputer 102 will maintain a communications link with a single Gateway 140, but may access multiple on-line services (and thus communicate with multiple application servers 120). . . .

Throughout the service session, the Gateway 140 routes messages between the client microcomputer 102 and the application server 120 as the client and server portions of the service application communicate.

Ex. 1012, 9:12–15, 9:23–26. We find that this teaches “a controller computer . . . affording information to each of a plurality of participator computers which are otherwise independent of each other,” as recited in claim 189.

As to “a database which serves as a repository of tokens for other programs to access,” Petitioner cites Brown’s access rights database, or relational database 152, which Brown describes as storing “multiple content category identifiers, or ‘tokens,’ which identify categories or groupings of content objects.” Pet. 20–21; Joinder Pet. 20–21; Ex. 1012, 2:66–3:2.

Petitioner contends that Brown’s “tokens” correspond to the “tokens” recited in claim 189. Pet. 21; Joinder Pet. 21. Patent Owner does not dispute that Brown’s access rights database is a “database which serves as a repository of tokens,” as recited in claim 189. On this evidence, we find that it is.

Petitioner argues that Brown’s database holds tokens for later use by services and programs within the network. Pet. 21; Joinder Pet. 21. According to Petitioner, “various application servers and gateways generate user-specific access rights queries in response to user requests.” Pet. 21

(citing Ex.1012, 3:27–30, 3:48–62, 20:8–27, 24:1–11, 25:23–27, 25:64–26:2); Joinder Pet. 21. For example, Brown describes multiple servers and gateways accessing the database:

In the preferred embodiment, each security server 150 is programmed to receive account-specific access rights queries from the application servers 120 and Gateways 140 within the network, and to respond to each such query by returning all of the access rights data of the user specified in the query.

Ex. 1012, 24:2–7. We find that Brown teaches a database that serves as a repository of tokens “for other programs to access,” as recited in claim 189.

Patent Owner argues that “Petitioner loses sight of the requirement that the **database** allows other programs to access the tokens.” PO Resp. 20. Patent Owner contends that Mr. Schmandt testifies that Brown’s database contains a UserID and a password and that Mr. Schmandt, in deposition, testified that Brown’s participant computers use telnet as their client software. PO Resp. 20–21.¹⁰ Patent Owner argues that “Telnet is not an ‘other program’ within the context of the claims” and that Mr. Schmandt does not explain how Telnet could access tokens in Brown’s database. *Id.* at 22. Brown, however, does not refer to Telnet. As Petitioner points out (Reply 9), Mr. Schmandt’s deposition testimony was directed to different prior art asserted in related proceedings. Patent Owner may have inadvertently copied argument from briefing in a related proceeding into its response in this proceeding. In any case, Patent Owner’s arguments are not

¹⁰ Patent Owner cites to Exhibit 1023 ¶ 128 for Mr. Schmandt’s direct testimony. Exhibit 1023, however, does not include Mr. Schmandt’s testimony. Moreover, paragraph 128 of Exhibit 1003, the Schmandt Declaration, does not include testimony relevant to this issue.

relevant to any issue in this proceeding. Patent Owner does not raise additional arguments as to these claim limitations.

On the complete record, we find that Brown teaches “using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other,” as recited in claim 189.

- c. *“affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity”*
“affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity”

As explained above, we find that Brown teaches affording information to several client microcomputers, which correspond to participator computers. We also find that Brown teaches affording information via the Internet network.

Petitioner contends that Brown teaches affording information “responsive to an authenticated [first/second] user identity” through its description of authenticating the users’ identities and requiring the users to have sufficient access rights before providing requested services. Pet. 23–24 (citing Ex. 1012, 14:18–25, 24:2–11); Joinder Pet. 23–24. On the complete record, we find that Brown teaches “affording some of the information to a [first/second] of the participator computers via the Internet network, responsive to an authenticated [first/second] user identity.”

- d. “determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications”

Petitioner contends that Brown discloses a system operator defining and assigning tokens for a chat room and the use of such tokens to define “user groups,” or groups of users who will be given access to the chat room. Pet. 25–26 (citing, *inter alia*, Ex. 1012, 15:27–37, 31:5–21); Joinder Pet. 25–26. For example, Brown describes that a system administrator creates a chat room node for an organization specifying a unique security token for the chat room, updates a group-member table to create a new group consisting of accounts of the members of the organization, and adds a row to a group-token table specifying a group ID, the security token of the chat room, and an access rights value. Ex. 1012, 31:5–21. The particular group could be for private communications among family members. *Id.* at 15:27–37, 31:1–5. Petitioner contends that Brown discloses users forming groups when joining a particular chat room. Pet. 26 (citing Ex. 1012, 9:45–52); Joinder Pet. 26. Here, Brown explains that “Chat conversations or ‘conferences’ are organized as ‘Chat rooms’ which may be entered or exited by end users to join or leave the corresponding conferences. For example, an end user may enter a ‘sports’ Chat room to join an interactive conversation on sports-related topics.” Ex. 1012, 9:47–52.

Petitioner argues that chat messages are sent and received in real time. Pet. 27 (citing Ex. 1012, 9:46–47); Joinder Pet. 27. Brown discloses that its “Chat service is an interactive communications service which allows users to have real time conversations with other users on specific topics.” Ex. 1012, 9:45–47. Patent Owner appears to concede that Brown’s chat communications are sent and received in real time. PO Resp. 27 (“At best,

joining a chat room may satisfy the determination as to whether two users can ‘receive real-time communications,’ . . .”).

Patent Owner argues that “[t]he users referred to in the limitation are the same users who were previously authenticated in the earlier claim limitations.” PO Resp. 26. According to Patent Owner:

a single user by himself cannot determine whether another user can form a group with him. While the creation of a chat room with permissions may be the prerequisite to forming a group, the step of creating a chat room does not involve any determination as to whether a group should be formed based on the claimed first and second user and thus cannot meet this limitation.

Id. We disagree with Patent Owner. In Petitioner’s example, when a system administrator updates a group-member table to specify at least two user accounts that are permitted to participate in an organization’s chat, the administrator determines whether those two user identities are able to form a group. Thus, contrary to Patent Owner’s argument, the step of creating a chat room with permissions does involve the determination of whether a group that includes the two users can be formed.

Patent Owner also argues that in *Brown*, the act of joining a chat room and, thus, a determination of rights in the chat room, “is done on an individual user basis and the claims require determining whether **two users** are able to form a group[,] *i.e.* the claims require a determination where information about both users is considered in the determination step.” PO Resp. 27. According to Patent Owner, “[a]ssessing chat-room permissions when joining a chat room does not meet this limitation.” *Id.* Patent Owner also appears to contend that this claim limitation requires a two-step process in which the system determines whether two users can form a group and then determines that the users may receive real-time communications.

Id. (“At best, joining a chat room may satisfy the determination as to whether two users can ‘receive real-time communications,’ but joining the chat room could not satisfy both of these limitations.”).

Patent Owner’s arguments are not commensurate with the scope of the claim language. Claim 189 does not recite a simultaneous determination, at the time two users are authenticated, that those two users have permission to communicate with each other. Nor does claim 189 recite determining that the users have permission to send real-time communications. Rather, claim 189 recites determining whether a first user identity and a second user identity are able to form a group to send and to receive real-time communications. Real-time communications are a characteristic of the group. Indeed, the ’657 patent describes a system similar to Brown’s in which tokens are assessed to determine whether users have permission to join a group (also called a channel) in which real-time communications are exchanged: “Accordingly, tokens are used by the controller computer 5 to control a user’s group priority and moderation privileges, as well as controlling who joins the group, who leaves the group, and the visibility of members in the group.” Ex. 1001, 8:1–4. As Petitioner points out (Reply 13), Dr. Carbonell conceded in deposition that this limitation is satisfied by a disclosure that two users have the appropriate rights to join the same chat room:

Q. . . . So if both users have the appropriate rights to join the same chat room, in your view the step of determining whether the first user identity and the second user identity are able to form a group is disclosed?

A. That seems to me what the claim requires, what the claim element requires.

Ex. 1101, 127:5–13. Petitioner’s evidence shows this to be the case in Brown.

In sum, we find that Brown’s disclosure of a system administrator determining who can join a particular Chat room, along with disclosures that multiple users join such a Chat room and that the communications in the Chat room are in real time, teaches “determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications,” as recited in claim 189.

- e. *“determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities”*
“if the first user identity is censored from the sending of the data, not allowing sending the data that is censored from the first participator computer to the second participator computer”

Regarding “determining whether the first user identity is individually censored from sending data in the communications . . . by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities,” as recited in claim 189, Petitioner argues that Brown discloses that a user can be given a set of permissions, such as “observer,” that does not include the right to send data. Pet. 34 (citing Ex. 1012, 17:35–18:5); Joinder Pet. 28–29. For example, according to Brown, a user with “observer” privileges “can see the existences of the node and can open the service, but cannot actively

participate in the service”; a user with “user” privileges “can do whatever is ‘normal’ for the particular service” such as “the ability to actively participate in public Chat conferences”; a user with “sysop” privileges “is given the access rights consistent with normal (entry-level) sysop-type activities for the service, such as the ability to delete BBS messages, or the ability to edit a certain subset of the properties of a node”; a user with “Sysop Manager” privileges “is given various ownership-type privileges with respect to the node” such as “the ability to change any of the properties (e.g., name, icon ID, etc.) for that node”; and a user with “SyperSysop” privileges “has the highest level of access authority provided by the service.” Ex. 1012, 17:35–18:5. Petitioner argues that this teaches that a user, such as one with “observer” privileges, is individually censored from sending data because the user is prevented, based on privilege levels, from taking actions such as sending or posting messages. Pet. 34; Joinder Pet. 28–29.

Petitioner argues that, because one of the respective users in the group can have “SuperSysop” privileges and may modify the access rights of a lower-rank user in the group, the system determines whether a parameter corresponding to a first user identity (the lower-rank user) has been determined by another of the user identities (the SuperSysop user). Pet. 29; Joinder Pet. 31. According to Petitioner, this teaches censoring “by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities.” Pet. 29; Joinder Pet. 31.

We agree with Petitioner and find that Brown teaches determining whether a first user identity, e.g., one with “observer” privileges only, is individually censored from sending data in the communications (because the

observer privileges do not allow sending data), by determining whether a respective at least one parameter corresponding to the first user identity has been determined by another of the user identities (e.g., one with “SuperSysop” privileges assigning the first user identity the “observer” privileges). This is consistent with our construction of “censor,” detailed in Section II.A.2 above.

Petitioner marshals essentially the same evidence to show that Brown teaches “if the first user identity is censored from the sending of the data, not allowing the data that is censored to be presented from the second participator computer to the output device,” as recited in claim 189. Pet. 36–37; Joinder Pet. 34–35. We agree, and find that, because a user with observer privileges does not have permission to send data, those data will not be presented to an output device.

As to “the data presenting at least one of a pointer, video, audio, a graphic, and multimedia,” as recited in claim 189, Petitioner points to examples in which chat conferences involve text, voice, and/or video capabilities. Pet. 28 (citing Ex. 1012, 9:52–55); Joinder Pet. 30. We agree that these are examples of data presenting video, audio, a graphic, and multimedia (the “and/or” suggesting that multiple forms of media can be presented together). Because claim 189 recites the data presenting “at least one of” a pointer, video, audio, a graphic, and multimedia, showing any one of these is sufficient. Thus, we find that Brown teaches “the data presenting at least one of a pointer, video, audio, a graphic, and multimedia.” We need not reach Petitioner’s additional arguments (Pet. 28–29; Joinder Pet. 30–31) that Sociable Web teaches “a pointer.”

We note that Patent Owner does not dispute that Brown teaches these limitations.

- f. *“if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network”*

As explained above, we find that Brown teaches user identities forming a group and communicating with each other in real time using a Chat service (provided they have permissions of “user” or above and, thus, are not censored from sending data), and that the communications can be via an Internet network. Thus, we find that Brown teaches this limitation.

- g. *“wherein, for the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer”*

As explained above, we find that Brown teaches user identities forming a group and communicating with each other in real time using a Chat service, and that the communications can be via an Internet network.

Regarding communications “which present an Internet URL,” Petitioner contends that Sociable Web teaches a chat functionality, WebTalk, that “allows users to ‘insert hypertext links, sounds and images amidst their normal conversational text’ in a chat window, as well as ‘link[s] to other pages.’” Pet. 31 (quoting Ex. 1019, 1, 4); Joinder Pet. 33.

Petitioner argues that a skilled artisan would have combined the teachings of Brown and Sociable Web to “maximize two important offerings available in the network” and to use Brown’s improved access rights mechanism to enhance the security of Sociable Web’s chat system. Pet. 31; Joinder Pet. 33–34.

Patent Owner argues that chats in Sociable Web “would have been hypertext, the actual images, graphics, sounds, or other media would not have been transferred between users” and that Sociable Web’s teaching “directly contradicts Brown, which accomplishes all of its communications using servers as a conduit.” PO Resp. 28. According to Patent Owner “one of ordinary skill in the art would not have wanted to break the server-based paradigm of Brown, which would have been a necessity according to the Sociable Web.” *Id.* Petitioner takes issue with Patent Owner’s characterization of Sociable Web, arguing that “Sociable Web contains extensive disclosures of server-based systems for multimedia communication over the Internet, and discusses non-server-based approaches only for the specific category of private messages.” Reply 23–24 (citing Schmandt Reply Decl. (Ex. 1100) ¶¶ 48–49). According to Sociable Web,

The WebTalk port is a tcp socket that is kept open for data transfer: it is through this socket that the Web Talk discussions take place. Private conversations and public conferences are handled differently, to minimize the load on the server. For private conversations, the server simply provides the two parties with each other’s address; the connection is made directly between the two.

Ex. 1019, 5.

Patent Owner acknowledges this distinction between private conversations and public conferences. PO Resp. 27. Nevertheless, Dr. Carbonell argues (without citation), that “[t]he only communication of data such as images, graphics, or sound, would have been in the context of private messages, which bypass the server.” Ex. 2006 ¶ 44. Sociable Web expressly states, however, that WebTalk can include both private conversations and public conferences, implying that communication of images, graphics, and sound would have been in the context of public conferences as well. Ex. 1019, 5. Thus, Dr. Carbonell’s testimony is not credible on this point.

Moreover, Patent Owner’s arguments amount to an argument that a skilled artisan would not have bodily incorporated Sociable Web into Brown. “It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements. . . . Rather, the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art.” *Mouttet*, 686 F.3d at 1332–33. Assuming that Sociable Web teaches communicating images, graphics, sounds, and video between users without such data passing through the same central server as its text-based communications, applying Sociable Web’s teachings would not “contradict” or “break” Brown’s teachings. Rather, Sociable Web’s teachings would have added desirable functionality to Brown’s system with Brown’s existing functionality continuing to operate as described. Thus, a skilled artisan would have had reason to combine these teachings of Sociable Web with Brown.

Patent Owner further contends that a skilled artisan would have understood that “concerns such as bandwidth and server load were real world problems experienced on the Internet,” and that, accordingly, “one of ordinary skill in the art would not have necessarily looked to add the Internet web-server of the Sociable Web due to its limitations.” PO Resp. 28.

Dr. Carbonell repeats Patent Owner’s arguments, nearly verbatim, in his testimony. Ex. 2006 ¶ 44. We reject those arguments for the reasons given in Section II.B.3.a above.

In sum, we find that Brown and Sociable Web teach “for the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer,” as recited in claim 189.

4. Claim 465

Petitioner contends that claim 465 “requires a system including in all material respects the elements and configured to perform the steps recited in claim 189, and is unpatentable for the same reasons.” Pet. 38; Joinder Pet. 35. We have compared claim 465 to claim 189 and agree that these claims are materially indistinct, other than that claim 465 is a system claim and claim 189 is a method claim. We find that Brown and Sociable Web teach each limitation of claim 465 for the same reasons as given for claim 189, discussed above. We note that Patent Owner does not present separate arguments for claim 465.

5. Conclusion of Obviousness

As explained above, Brown and Sociable Web teach each limitation of claims 189 and 465. Petitioner has introduced persuasive evidence that a skilled artisan would have had reasons to combine the teachings of Brown and Sociable Web. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. In sum, upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 189 and 465 would have been obvious over Brown and Sociable Web.

III.PATENT OWNER’S MOTION TO EXCLUDE

Patent Owner filed a paper styled “Motion to Exclude Evidence,” seeking to exclude certain portions of the Schmandt Reply Declaration that it argues exceeds the proper scope of a reply. Paper 51, 1. Specifically, Patent Owner seeks to exclude portions of paragraphs 21–23, 26–30, 42, and 45–51 of the Schmandt Reply Declaration. *Id.* at 1–7.

Petitioner opposes this motion on the ground that it is not directed to the admissibility of evidence and, therefore, is procedurally improper. Paper 55, 1–2. Patent Owner contends that arguments that exceed the scope of a reply are irrelevant, prejudicial, confusing, or misleading under Federal Rules of Evidence 401, 402, and 403. Paper 57, 1–2. As Petitioner points out, however, the Board repeatedly has denied, as improper, motions to exclude that merely argue that evidence is outside the proper scope of a reply. Paper 39, 1–3. Despite its invocation of Rules 401, 402, and 403, we agree that Patent Owner’s Motion to Exclude is nothing more than an

argument that Petitioner's Reply exceeds its proper scope. Accordingly, we deny Patent Owner's Motion.

Nevertheless, we have considered Patent Owner's argument with respect to those portions of Petitioner's Reply that are relied upon in this decision, and determine they do not belatedly raise new issues or present evidence that should have been presented in the Petition. We do not rely on paragraphs 21–23, 26–30, and 42 of the Schmandt Reply Declaration. The testimony of paragraphs 45–51 properly responds to the arguments raised in the PO Response and, accordingly, does not exceed the scope of evidence appropriate for a reply.

IV. CONCLUSION

Petitioner has proved by a preponderance of the evidence that claims 189 and 465 are unpatentable.

V. ORDER

For the reasons given, it is

ORDERED, based on a preponderance of the evidence, that claims 189 and 465 are unpatentable; and

FURTHER ORDERED, because this is a final written decision, the parties to this proceeding seeking judicial review of our Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

IPR2016-01155
Patent 8,694,657 B1

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

Daniel Knauss
dknauss@cooley.com

Mark Weinstein
mweinstein@cooley.com

PATENT OWNER:

Peter Lambrianakos
plambrianakos@brownrudnick.com

Vincent Rubino
vrubino@brownrudnick.com