

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Microsoft Corporation
Petitioner

v.

Windy City Innovations, LLC
Patent Owner

U.S. Patent No. 8,407,356

TITLE: REAL TIME COMMUNICATIONS SYSTEM

Inter Partes Review No. IPR2017-00605

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,407,356**

Table of Contents

	Page
I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)	1
A. Real Party-In-Interest under 37 C.F.R. § 42.8(b)(1)	1
B. Related Matters under 37 C.F.R. § 42.8(b)(2)	1
C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)	1
D. Service Information	2
E. Power of Attorney	3
II. PAYMENT OF FEES - 37 C.F.R. § 42.103	3
III. REQUIREMENTS FOR <i>INTER PARTES</i> REVIEW	3
A. Grounds for Standing under 37 C.F.R. § 42.104(a)	3
B. Identification of Challenge under 37 C.F.R. § 42.104(b) and Statement of Precise Relief Requested	4
C. Requirements for <i>Inter Partes</i> Review 37 C.F.R. § 42.108(c)	5
IV. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	5
A. “token”	5
B. “channel”	6
C. “providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type”	8
D. “pointer”	15
V. CLAIMS 1-9, 12, 14-28, 31 AND 33-37 ARE UNPATENTABLE	16
A. Brief Summary and Date Qualification of the Prior Art	16
1. Brief Overview of Roseman (Ex. 1003)	16
2. Brief Overview of Rissanen (Ex. 1004)	19
3. Brief Overview of Vetter (Ex. 1005)	21
4. Brief Overview of Pike (Ex. 1006)	21
5. Gosling (Ex. 1007)	23
B. Ground 1: Claims 1-5, 8, 9, 12, 14-16, 19-24, 27, 28, 31, 33-35, 37 Are Obvious Over Roseman, Rissanen, and Vetter	23

Table of Contents
(continued)

	Page
1. Claim 1	23
a. “A method of communicating content among users using [sic] of 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” (Claim 1, Preamble)	23
b. “authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database” (Claim 1[a])	33
c. “affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity” (Claim 1[b])	35
d. “affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity” (Claim 1[c]).....	40
e. “running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers” (claim 1[d])	40
f. “providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers” (claim 1[e])	44

Table of Contents
(continued)

	Page
g. “communicating real-time messages within the group of the interactively connected said participator computers” (claim 1[f]).....	50
2. Claims 2-5 (Different Media Types)	51
3. Claims 8, 9, and 12 (“API Messages”)	53
4. Claims 14, 15 (“Censorship” Claims).....	53
5. Independent Claim 19	55
6. Claims 20-24, 27, 28, 31, 33-35 (Dependent Claims)	57
7. Independent Claim 37	58
C. Ground 2: Claims 6, 7, 17, 26, and 36 are Obvious Over Roseman, Rissanen, and Vetter, in Further View of Pike.....	60
D. Ground 3: Claims 18 and 25 Are Obvious Over Roseman in view of Rissanen and Vetter, in further view of Gosling.....	64
VI. CONCLUSION.....	64

List of Exhibits

Ex. No	Description of Document
1001	U.S. Patent No. 8,407,356 to Daniel L. Marks
1002	Declaration of Tal Lavian, Ph.D.
1003	U.S. Patent No. 6,608,636 to Robert D. Roseman
1004	EP 0621532 A1 to Eugene Rissanen, published on April 13, 1994
1005	Ronald J. Vetter, <i>Videoconferencing on the Internet</i> , Computer, IEEE Computer Society, Vol. 28, No. 1, at pp.77-79 (Jan. 1995)
1006	Excerpts from Mary Ann Pike et al., <i>Using Mosaic</i> (1994)
1007	James Gosling, <i>Java Intermediate Bytecodes</i> , ACM SIGPLAN Workshop on Intermediate Representations (Jan. 1995)
1008	Excerpts from <i>IEEE Std 100-1996, The IEEE Standard Dictionary of Electrical and Electronics Terms</i> (6th ed. 1997)
1009	Excerpts from <i>Microsoft Press Computer Dictionary</i> (2d ed. 1994)
1010	Declaration of Lee A. Hollaar, Ph.D., dated March 26, 2012 (from the file history of the '356 patent)
1011	James Coates, <i>A Mailbox in Cyberspace Brings World to Your PC</i> , Chicago Tribune, Mar. 1995
1012	Tim Berners-Lee et al., Request for Comments (RFC) 1738, <i>Uniform Resource Locators (URL)</i> , Dec. 1994
1013	Date-stamped Excerpts from Mary Ann Pike et al., <i>Using Mosaic</i> (1994)

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

Microsoft Corporation submits this Petition for *Inter Partes* Review of claims 1-9, 12, 14-28, 31 and 33-37 of U.S. Patent No. 8,407,356 (Ex. 1001) (“’356 patent”). This petition is substantively identical to pending IPR2016-01157 filed by Facebook, Inc. (“the Facebook IPR”), and relies on the same evidence and expert testimony. Petitioner requests institution on the same grounds as any grounds instituted in the Facebook IPR, and concurrently moves to join the Facebook IPR. *See* Paper 2.

I. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8(A)(1)

A. Real Party-In-Interest under 37 C.F.R. § 42.8(b)(1)

The Petitioner, Microsoft Corporation (“Petitioner”), is the real party-in-interest.

B. Related Matters under 37 C.F.R. § 42.8(b)(2)

The ’356 patent is the subject of one pending litigation involving the Petitioner: Windy City Innovations, LLC v. Microsoft Corp., Case No. 4:16-cv-1729-YGR (N.D. Cal.), in which the patent owner contends that the Petitioner infringes the ’356 patent. The ’356 Patent has also been asserted against Facebook Inc. in the Northern District of California (No. 3:16-cv-01730-RS), and is the subject of the pending Facebook IPR (No. IPR2016-01157).

C. Lead and Back-Up Counsel under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation of counsel.

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

LEAD COUNSEL	BACK-UP COUNSEL
Joseph A. Micallef USPTO Reg. No. 39,772 SIDLEY AUSTIN LLP 1501 K Street, N.W. Washington, D.C. 20005 Telephone: 202-736-8492 Facsimile: 202-736-8711 iprnotices@sidley.com	John W. McBride <i>pro hac vice</i> to be filed jwmcbride@sidley.com SIDLEY AUSTIN LLP 1 South Dearborn St. Chicago, IL 60603 Telephone: 312-853-7014 Facsimile: 312-853-7036 Herman F. Webley <i>pro hac vice</i> to be filed hwebley@sidley.com SIDLEY AUSTIN LLP 1501 K Street, N.W. Washington, D.C. 20005 Telephone: 202-736-8609 Facsimile: 202-736-8711 Todd M. Siegel USPTO Reg. No. 73,232 KLARQUIST SPARKMAN, LLP 121 S.W. Salmon Street, Ste. 1600 Portland, Oregon 97204 Telephone: (503) 595-5300 Facsimile: (503) 595-5301 todd.siegel@klarquist.com

D. Service Information

This Petition is being served to the current correspondence address for the '356 patent, PETER K. TRZYNA, ESQ., P.O. Box 7141, Chicago, IL 60680. The Petitioner may be served at the addresses provided above for lead and back-up counsel, and consents to electronic service at those addresses.

E. Power of Attorney

Filed concurrently herewith in accordance with 37 C.F.R. § 42.10(b).

II. PAYMENT OF FEES - 37 C.F.R. §§ 42.15(A), 42.103

The Director is authorized to charge the fee specified by 37 CFR § 42.15(a) to Deposit Account No. 50-1597.

III. REQUIREMENTS FOR *INTER PARTES* REVIEW

A. Grounds for Standing under 37 C.F.R. § 42.104(a)

The Petitioner certifies that the '356 patent is available for *inter partes* review and that the Petitioner is not barred or otherwise estopped from requesting *inter partes* review on the ground identified in the present Petition. On June 2, 2015, the Patent Owner filed a complaint alleging infringement of the '356 patent by the Petitioner. *Windy City Innovations, LLC v. Microsoft Corporation*, 1:15-cv-103 (N.D. Cal.). On June 3, 2016, the Petitioner filed a petition for *inter partes* review of the '356 patent, and an IPR was instituted on December 8, 2016. *See* IPR2016-01067. While the Petitioner was served with a complaint alleging infringement of the '356 patent more than one year before the date this Petition is filed, the time limitation of 35 U.S.C. § 315(b) "shall not apply to a request for joinder under" 35 U.S.C. § 315(c). Because this Petition is accompanied by such a request (Paper 2), it complies with 35 U.S.C. § 315(b).

**B. Identification of Challenge under 37 C.F.R. § 42.104(b) and
Statement of Precise Relief Requested**

The Petitioner respectfully requests that the Board initiate *inter partes* review of claims 1-9, 12, 14-28, 31 and 33-37 of the '356 patent. The grounds on which this Petition is based are listed below:

Ground	Claims	Basis for Challenge
1	1-5, 8, 9, 12, 14-16, 19-24, 27, 28, 31, 33-35, 37	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , under 35 U.S.C. § 103(a)
2	6, 7, 17, 26, 36	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , in further view of <u>Pike</u> , under 35 U.S.C. § 103(a)
3	18, 25	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , in further view of <u>Gosling</u> , under 35 U.S.C. § 103(a)

As explained in Part V below (discussion under “Prior Art and Date Qualification”), each of the references listed above qualifies as prior art to the '356 patent. **Part V** below also provides a detailed explanation as to why the challenged claims are unpatentable based on the grounds identified above. The Petitioner has also submitted an accompanying Declaration of Tal Lavian, Ph.D. (“Lavian Decl.”) (Exhibit **1002**), a technical expert with more than two decades of relevant experience, including extensive experience in computer programming and software development. (Lavian Decl., Ex. 1002, ¶¶ 2-8, Ex. A.)

C. Requirements for *Inter Partes* Review 37 C.F.R. § 42.108(c)

The Board should institute *inter partes* review of claims 1-9, 12, 14-28, 31 and 33-37 because this Petition establishes a reasonable likelihood of prevailing. Each limitation of the challenged claims is disclosed and/or suggested by the prior art, as explained in detail in **Part V**.

IV. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)

“A claim in an unexpired patent shall be given its broadest reasonable construction in light of the specification of the patent in which it appears.” 37 C.F.R. § 42.100(b). The “broadest reasonable construction” standard is different from the manner in which the scope of a claim is determined in litigation. *See In re Swanson*, 540 F.3d 1368, 1377-78 (Fed. Cir. 2008).¹

A. “token”

Each independent claim recites a database that provides a “repository of tokens” used to perform user authentication. Claim 1, for example, recites “authenticating a first user identity and a second user identity according to

¹ As explained by Dr. Lavian, a person of ordinary skill in the art as of April 1996 would have had at least a bachelor’s degree in electrical engineering or computer science (or equivalent degree or experience) with practical experience or coursework in the design or development of systems for network-based communication between computer systems. (Lavian Decl., Ex. 1002, ¶ 13.)

permissions retrieved from [a] repository of tokens of the database.” The patent describes a “token” as follows:

With regard to the arbitrating of the controller computer **3** is directed by the controller computer program **2** to use “identity tokens”, which are pieces of information associated with user identity. The pieces of information are stored in memory **11** in a control computer database, along with personal information about the user, such as the user’s age.

(’356, 8:9-14 (underlining added).) The specification goes on to describe several exemplary uses for tokens, including “to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process” (’356, 8:22-23), “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” (’356, 8:31-33), and “to permit a user’s control of identity, and in priority contests between 2 users, for example, a challenge as to whether a first user can see a second user.” (’356, 8:36-38.)

Based on the definitional language in the written description, the term “**token**” should be interpreted under its broadest reasonable construction as a “**piece of information associated with user identity**.” (Lavian Decl. ¶¶ 17, 18.)

B. “channel”

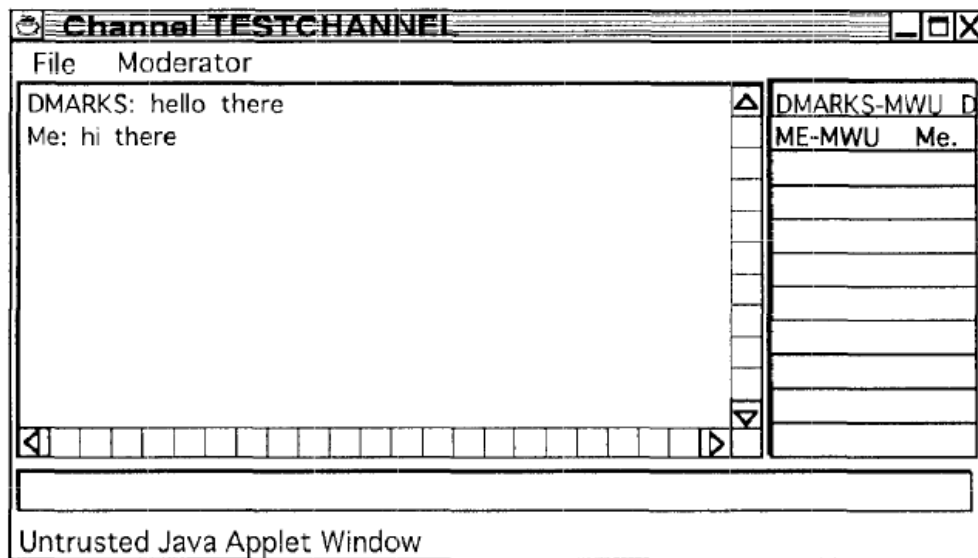
The word “**channel**” to persons of ordinary skill in the art ordinarily refers to a transmission medium or connection, but the patent uses the term in a different

context. (Lavian Decl. ¶ 19.) The patent explains that “a group is sometimes known as a channel in multiplexing terminology” (’356, 8:28-29), and this statement is generally consistent with the use of “channel” throughout the patent. For example, the following passage equates a “channel list” with a “group list”:

Then the channel list area is shown at FIG. 8. The Channel List area is a window which shows a list of all of the groups currently on the server in active communication. Because no one is yet connected in this example, there are no groups currently available on the screen.

(’356, 9:24-28 (underlining added).) Figure 14 shows an exemplary channel showing a screen similar to a “chat room” from America Online:

FIG. 14



(’356, Fig. 14; *see also* 3:21-22 (“FIG. 14 is an illustration of a private message window on the new channel screen of the present invention”) (underlining added).)

In the example shown in Figure 14, DMARKS has typed in a message “hello there,” which was sent to the channel members, DMARKS and “Me.” (’356, 9:47-51 (“The user DMARKS now types ‘hello there’ into the response area and presses RETURN (at FIG. 12). This message is passed to the controller computer 5, which sends the message to all channel members, i.e., those using participator computers 5, including DMARKS.”) (underlining added).)

Based on this description, “**channel**” under its broadest reasonable construction means a “**group of users that can communicate with each other.**” (Lavian Decl. ¶ 20.)

C. “providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type”

This entire phrase warrants an explicit construction because, simply put, it repeatedly uses confusing terminology and terms (such as “API”) that have a meaning different from their understood meaning to persons of ordinary skill in the art. This Petition will address this phrase piece-by-piece.

To begin with, the term “**multiplexing**” outside the patent ordinarily refers to techniques for combining multiple messages for transmission through a single communications pathway. (Lavian Decl. ¶ 22 (citing Ex. 1008 & Ex. 1009).) The term “**demultiplexing**” to a person of ordinary skill in the art generally refers to the reverse of multiplexing, *i.e.* separating out the individual messages that were incorporated into the combined (multiplexed) signal. (*Id.* ¶ 23 (citing Ex. 1008, at

p. 270).) For example, hardware may demultiplex signals from a transmission line based on time or carrier frequency to allow multiple, simultaneous transmissions across a single physical cable. (*Id.* ¶ 23.) The terms multiplexing and demultiplexing are commonly used to describe the physical transport and processing of digital and analog signals. (*Id.*)

But the '356 patent uses these terms in a slightly different context. In particular, the Background of the Invention uses the term “multiplexing” to describe messaging technologies such as email, conferencing, and chat messages that may be distributed through a shared network. ('356, 1:34-52.) Each example of “multiplexing” refers to transporting a message (typically originating from one person) using a shared communications pathway, such as a shared network or the Internet, that also carries other messages. Accordingly, “demultiplexing” would be understood as the reverse of multiplexing, *i.e.* separating an individual message from the combined signal carried by the communications pathway to deliver it to the intended recipient. (Lavian Decl. ¶ 24.)

The patent also uses the term “**API**” in an idiosyncratic way. The term “API” outside the patent generally refers to an “application programming interface” (API), a concept very familiar to persons of ordinary skill in the art. (Lavian Decl. ¶ 25.) During the prosecution of the '356 patent, however, the applicant emphatically stated that the term “**API**” did **not** refer an application

programming interface. In particular, following a claim rejection based on Brown (U.S. Patent No. 5,941,947), applicant submitted a declaration of Lee A. Hollaar, Ph.D., in an attempt to distinguish Brown stating:

With respect to the Marks specification and claims, the Examiner correctly concedes that “Brown does not specifically teach an application programming interface (API) within the reference” at page 7 of the Final Rejection.

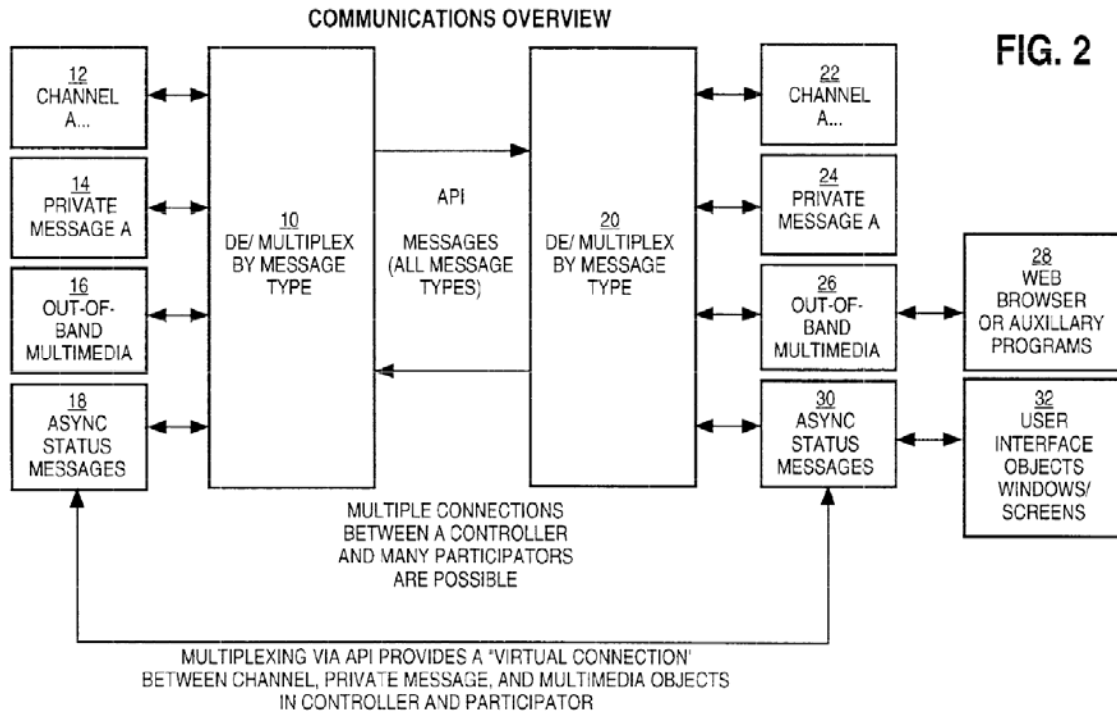
However, the Examiner has misunderstood the Marks specification and claims by assuming that an API means an applications program interface to the operating system (Final Rejection, Page 7 “Horn also teaches that applications access the operating systems functions through an application programming interface (API) ...”).

There is no basis for this misunderstanding because, while the Marks specification does not define API, the Marks specification also never uses the term “application program interface” and only uses “application” once (“JAVA application”).

The best illustration of what API means in the context of the Marks specification is in Fig. 2, where API messages are the collection of all message types, between one computer and another, that are multiplexed for transfer and then demultiplexed by message type to rout them to the appropriate place. There is no possible way that Fig. 2 is compatible with the Examiner’s interpretation that the API is used to “access the operating systems functions.”

(Ex. 1010, ¶¶ 6-9 (underlining added).)

Figure 2 of the patent, which the applicant claimed is the “best illustration of what API means in the context of the Marks specification” (*id.* ¶ 9), shows the label “API” sitting in the middle between blocks **10** and **20**:



(’356, Fig. 2.)

The black boxes in Figure 2 refer to software functionality. Block **10** (to the left of “API”) refers to software on the “controller computer” for performing multiplexing and demultiplexing operations on messages. (’356, 5:45-48 (“Beginning with the Controller Computer Software 2, reference is made to Block **10**, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types.”) (underlining added).) The written description uses almost identical language to describe block **20** (to the right of

block **10**), except that block **20** refers to software on a “participator computer.” (’356, 5:58-61 (“With particular regard to the participator software 4 illustrated in FIG. 2, Block **20** is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types.”) (underlining added).)

The patent does not appear to describe in detail how the processes of “demultiplexing and multiplexing operations,” using an “API,” take place. It instead largely repeats the language of the claims by stating: “De/multiplexing via API provides a ‘virtual connection’ between Channel, Private Message, and Multimedia objects in the controller computer **3** and each participator computer **5**.” (’356, 6:3-5.) Based on this description, the term “API” does not describe an application programming interface; it simply describes software functionality that may reside on a controller or participant computer. (Lavian Decl. ¶ 29.)

With respect to the term “**API messages**,” it appears only twice in the written description in stating that blocks **10** and **20** of Figure 2 illustrate “demultiplexing and multiplexing operations carried out by message type on API messages of all types.” (’356, 5:47-48 (block 10), 5:60-61 (block 20).) The written description later describes six possible message types, “ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG,” which are used to mediate communications between the controller and participant computers. (’356, 7:6-8 (capital letters in original); *see also id.*, 22:6-8 (Claim 9:

“The method of claim 1, wherein communications among the controller computer and the participator computers are mediated via API messages.”.)

The patent confirms that the “API messages” are simply messages that are processed by the “API” software functionality. For example, Figure 3 shown at the

right describes aspects of the “**multiplexing**”

operation. Block 10 in yellow highlighting shows “MULTIPLEXING OF MESSAGE

TYPE,” which evaluates the type of message

and then routes the message to the appropriate software functionality. For

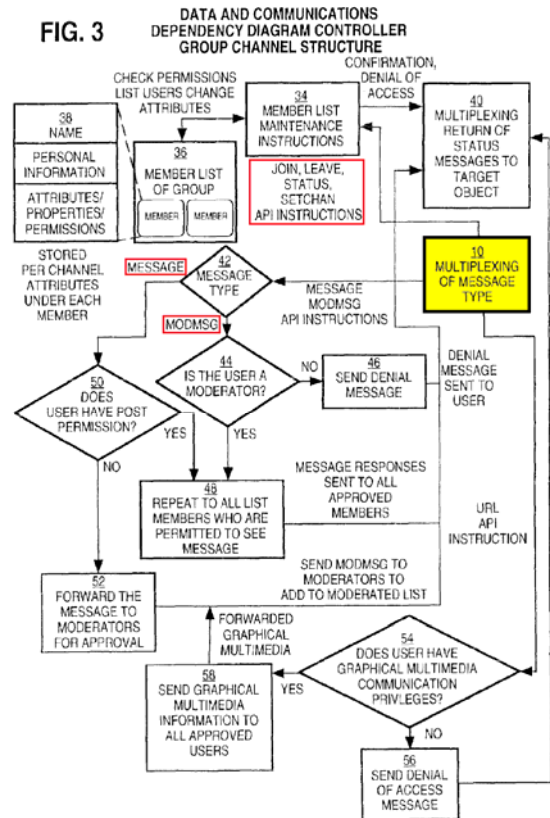
example, for MESSAGE or MODMSG types, the logic moves to block 42, and

branches further to block 50 for MESSAGE

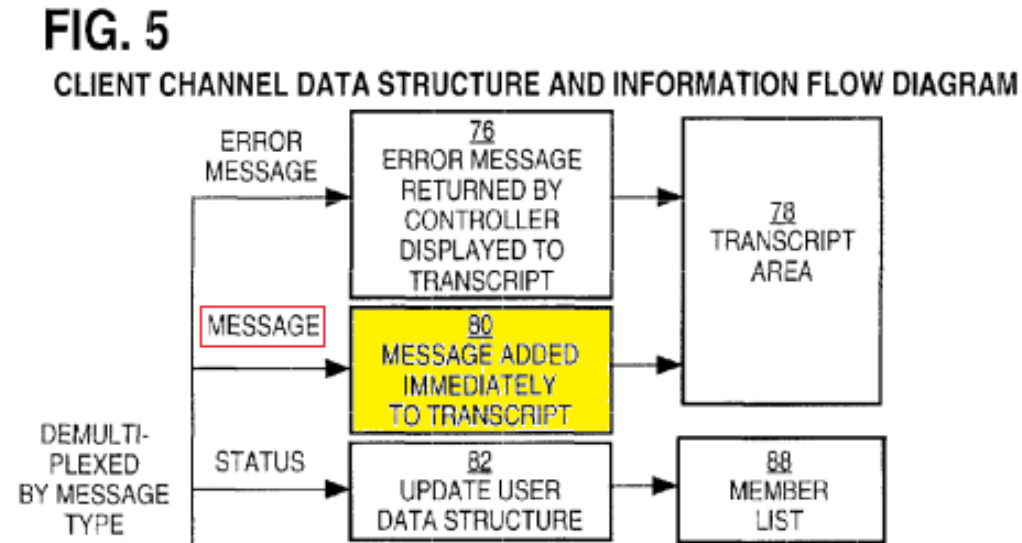
and block 44 for MODMSG. (’356, 6:25-

40.) For other types of messages, the logic branches to block 34. (’356, 6:12-15.)

In this case, “**multiplexing**” simply involves communicating an “API message” to the appropriate software based on the type of the message.



The patent provides a similar description of “**demultiplexing**” API messages by message type – when an API message is received, it is routed to the appropriate software “Block” based on its message type. To illustrate, a portion of Figure 5 is shown below to describe how API messages of “ERROR MESSAGE,” “MESSAGE,” and “STATUS” are handled:



Taking the example of an API message of type “**MESSAGE**,” Figure 5 shows that demultiplexing that message routes the message to logic Block **80**, which immediately adds the message content to the transcript area 78. (’356, 7:11-12, 7:30-32.) This example shows that, like “multiplexing” discussed above, “**demultiplexing**” simply refers to routing a received API message to the correct software functionality based on the type of message.

Based on all of this analysis, the broadest reasonable construction of the phrase, “providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type,” should be **“providing software functionality on the controller computer for sending and receiving messages of different types and communicating each message to software functionality based on the message type.”** (Lavian Decl. ¶ 33.)

D. “pointer”

The term “pointer” appears in dependent claims 2, 7, 20, and 26. “Pointers” are well-known in computer science and exist at all levels of computer system design. (Lavian Decl. ¶ 34.) To persons of ordinary skill in the art, a “pointer” is a piece of information that “points to,” or references, other information. (*Id.*)

The written description provides only the following mention of pointers, which identifies a Uniform Resource Locator (URL) as an example of a pointer:

The 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**.

(’356, Ex. 1001, 5:38-43.) Based on this description, the term “pointer” should be construed as a **“piece of information that points to or references other information.”** (Lavian Decl. ¶ 35.)

V. CLAIMS 1-9, 12, 14-28, 31 AND 33-37 ARE UNPATENTABLE

This Petition identifies the following grounds on which IPR should be instituted for claims 1-9, 12, 14-28, 31 and 33-37:

Ground	Claims	Description of Ground
1	1-5, 8, 9, 12, 14-16, 19-24, 27, 28, 31, 33-35, 37	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , under 35 U.S.C. § 103(a)
2	6, 7, 17, 26, 36	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , in further view of <u>Pike</u> , under 35 U.S.C. § 103(a)
3	18, 25	Unpatentable over <u>Roseman</u> in view of <u>Rissanen</u> and <u>Vetter</u> , in further view of <u>Gosling</u> , under 35 U.S.C. § 103(a)

A. Brief Summary and Date Qualification of the Prior Art

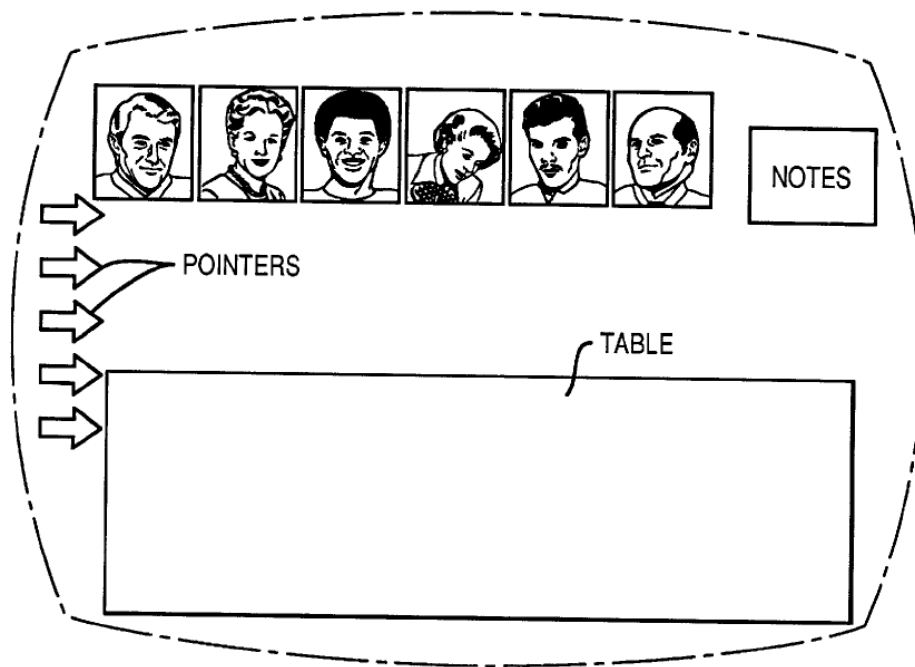
1. Brief Overview of Roseman (Ex. 1003)

Roseman, entitled “Server Based Virtual Conferencing,” discloses a system for creating a virtual conference room that allows participants to collaborate in real time over a computer network. Roseman qualifies as prior art under at least 35 U.S.C. § 102(e) (pre-AIA) because it is a patent issuing from an application filed on May 13, 1992, before the filing of the earliest application to which the ’356 could claim priority (April 1, 1996). This Petition cites Roseman for the majority of the limitations in the challenged claims, and relies on the other references (Vetter, Rissanen, Pike and Gosling) only for a few limitations to the extent not disclosed in Roseman.

The virtual conferencing system in Roseman “allows multiple persons, at different locations, to hold a conference, by providing many of the conveniences which the participants would have if present together in the same physical room.” (Roseman, 1:19-23.) Roseman describes “a virtual conferencing system which allows multiple persons to view, and also manipulate, a common video display, which is simultaneously displayed at their different locations.” (Roseman, 1:28-31.) Each conference participant has his or her own “local computer.” (Roseman, 1:34-35; *see also id.*, 2:64-65.) The local computers “have associated video cameras, speaker-type telephones, and pointing devices (such as ‘mouses’). When a conference is established, the local computers become connected to a host computer, via commercially available Local Area Networks (LANs) and Wide Area Networks (WANs).” (Roseman, 1:36-41; *see also id.*, 3:14-19.)

A user in Roseman creates a virtual conference room by clicking an appropriate icon through a user interface, identifying the participants of the conference and providing other information such as the rules that govern the meeting. (Roseman, 3:22-56.) Once the parameters of the conference are established, the host computer “creates the conference room. The host does this by creating a common image, such as that shown in FIG. 9. The common image includes a picture of each invitee, a ‘table,’ and the room decor.” (Roseman, 7:30-34.) An example of the virtual conference room is shown in Figure 9 below:

FIG. 9



(Roseman, Fig. 9.)

Roseman explains that when a meeting participant enters a virtual conference room with other participants, “the data connection is made. Audio and video connections are made if supported by the user, the room and the other users. A small picture of each user is displayed in the meeting room to indicate presence.” (Roseman, 11:11-14.) Once inside the conference room, “[o]bjects (documents) can be shared in the conference room by placing them on the table. This might be done by dragging an icon . . . onto the table.” (Roseman, 11:18-22.) Additionally, the user can click on the picture of another participant to engage in a private voice conversation, or drag a textual note onto the picture of another

participant to send a private text message. (Roseman, 9:16-31.) Other communication features are described in the discussion of the claims below.

Roseman also discloses a security mechanism in which users must be invited and have an appropriate “**key**” to enter the conference room. (Roseman, *e.g.*, 9:34-55, 10:61-64 (“To open a door with a key, the user drops the key onto the door lock. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.”).) Roseman also discloses a database that stores the keys for the conference room. (Roseman, 9:49-50.) These conference room “keys,” as explained below, correspond to the “**tokens**” recited in the independent claims. More details about Roseman are set forth below

2. Brief Overview of Rissanen (Ex. 1004)

Each independent claim recites “**a database which serves as a repository of tokens for other programs to access.**” As noted above, the “keys” in Roseman disclose the claimed “tokens,” and those keys are stored on the central host computer. But Roseman does not use the word “database” to describe the storage of keys by the host. In the event it is argued that Roseman fails to disclose a “database” that stores the keys, as recited by the claims, this requirement would have been trivially obvious over Rissanen.

Rissanen, entitled “Password Verification System,” discloses a technique for user authentication using passwords stored in a database. Rissanen qualifies as

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

prior art under at least 35 U.S.C. § 102(b) (pre-AIA) because it was published more than one year before the filing of the earliest patent application to which the '356 patent could claim priority.

This Petition cites Rissanen as an alternative basis to teach “**a database which serves as a repository of tokens for other programs to access,**” in the event it is argued that Roseman alone does not disclose this limitation. Rissanen discloses storing user passwords in a database, and subsequently using those stored passwords to verify user identity when users subsequently attempt to log-on. (Rissanen, Ex. 1004, 1:21-28.) Rissanen also discloses that user login and password information may be stored in a database. (Rissanen, 2:22-29.) Although Rissanen also describes using spoken voice passwords, this Petition cites it for its more pedestrian teachings relating to database storage of passwords of any form.

As explained in detail below, the user and password information in the database in Rissanen is analogous to the conference room “keys” in Roseman. It would have been obvious to combine Roseman and Rissanen to produce the virtual conferencing system of Roseman in which the conference room keys are stored in a database serving as a repository of tokens (keys) for other programs to access, as taught in Rissanen. (Lavian Decl. ¶¶ 48, 67, 68.)

3. Brief Overview of Vetter (Ex. 1005)

Certain independent claims of the '356 patent require that information be transmitted “**via the Internet.**” Roseman discloses using “commercially available” Wide Area Networks (WANs) to communicate with participator computers, but does not specifically the Internet. (Roseman, 1:37-41; *see also id.*, 3:14-19.) Vetter, entitled “Videoconferencing on the Internet,” discloses software tools for enabling videoconferencing over the Internet. Vetter qualifies as prior art under at least 35 U.S.C. § 102(b).

This Petition cites Vetter for the straightforward and unremarkable proposition that simply adding “the Internet” to an existing computer-based conferencing products does not render it non-obvious over the prior art. Vetter confirms that the Internet was already being used with conferencing systems such as Roseman to enable real-time communication. (Vetter, Ex. 1005, at p. 77.) As will be explained below, the recitation of the “Internet” provides no meaningful distinction over Roseman.

4. Brief Overview of Pike (Ex. 1006)

Pike, entitled *Using Mosaic*, is a book describing NCSA Mosaic, one of the early browsers for accessing the World Wide Web. (Pike, Ex. 1006, at p. 1-2.) This Petition cites Pike in connection with dependent claims 6, 7, 17, 26, and 36, which recite that the information communicated between computers can include a

“pointer” that allows the content to be produced on demand, or recite that communicated content may be invoked with a Uniform Resource Locator (URL).

Pike qualifies as prior art under at least 35 U.S.C. § 102(b) (pre-AIA).

As explained below, Roseman discloses a pointer in the form of a clickable icon that, when clicked by a meeting participant, presents a document, message or other content to the user. (Roseman, Ex. 1003, *e.g.*, 14:53-57, 14:59-62 (icon representing document placed on table), 9:28-31.) Nevertheless, in the event it is argued that the claimed “pointer” requires something akin to an Internet URL, the pointer limitations would have been obvious in view Pike [**Ex. 1006**].

Pike provides an introductory section describing basic Internet concepts such as URLs. (Pike, at pp. 38-39.) Pike explains that “[a] *URL* is a complete description of an item, including the location of the item that you want to retrieve.” (*Id.* at 38 (italics in original).) “The location of the item can range from a file on your local disk to a file on an Internet site halfway around the world.” (*Id.*) Pike further explains that a URL can identify any resource on the Internet, and “is not limited to describing the location of WWW [World Wide Web] files.” (*Id.*) As demonstrated below, it would have been obvious to a person of ordinary skill in the art to adapt known URL techniques to Roseman.

5. Gosling (Ex. 1007)

56. Gosling, entitled *Java Intermediate Bytecodes*, is a paper describing aspects of the Java programming language. This Petition cites Gosling solely in connection with dependent claims 18 and 25, which recite that the controller software comprises “a JAVA™ application.” Gosling qualifies as prior art under at least 35 U.S.C. § 102(b) (pre-AIA). Gosling confirms that Java was a known computer programming language that predated the ’356 patent, and that a skilled artisan would be motivated to use it. (Gosling, Ex. 1007, at p. 111 & 115.)

**B. Ground 1: Claims 1-5, 8, 9, 12, 14-16, 19-24, 27, 28, 31, 33-35, 37
Are Obvious Over Roseman, Rissanen, and Vetter**

1. Claim 1

- a. **“A method of communicating content among users using [sic] of 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” (Claim 1, Preamble)**

Roseman discloses each aspect of the preamble.² First, Roseman discloses “[a] method of communicating content among users using [sic] of a computer system,” as recited in the first part of the preamble. Roseman discloses a virtual

² It is unnecessary for the Board to determine whether the preamble is limiting because, as demonstrated in the text, the prior art nevertheless discloses it.

conferencing system in which users (*e.g.*, conference participants) share content over a network. For example:

The parties send the information which they want displayed, such as drawings, to the host computer. The host computer generates a common video screen, which it distributes to the parties: they see the drawings at their own local computers. Each party can move a pointer on the display, and point to features on the drawings. The telephones and video cameras allow the parties to see and speak with each other.

(Roseman, 1:42-49.) In addition, “[t]he participants can privately whisper or pass notes to each other, without the knowledge of the others.” (Roseman, 2:49-50.) Further details on how Roseman discloses communicating content among users are set forth in the discussion of later claim limitations.

The preamble of claim 1 continues by reciting that the computer system **“includ[es] a controller computer and a database which serves as a repository of tokens for other programs to access . . .”** The “controller computer” in Roseman takes the form of a server called the “host computer” or “host”:

These individual [participant] systems are located at different geographic locations, and, when a virtual conference is to be held, become connected to a central, host, computer (or multiplicity of host computers) via the proper combination of Local Area Networks (LANs) and Wide Area Networks (WANs).

(Roseman, 3:14-19 (underlining added), 1:50-52 (“The host controls many of the events occurring during the conference, as well as those occurring both during initiation of the conference and after termination of the proceedings.”).)

Roseman also discloses “**a database which serves as a repository of tokens for other programs to access.**” The tokens in Roseman take the form of “**keys,**” which are stored and distributed by the host computer to potential conference participants. More specifically, Roseman explains that in creating a new virtual conference room, the creator can cause the host to send invitations to participants. Each invitation contains a “key” that relates to the identity of the invitee and provides the permissions allowing access to the conference room:

Before an invitation list is compiled, the level of invitations must be specified by the invitor. Three levels of invitations are considered.

1. an invitation is for the Invitee only.
2. an invitation is for the Invitee, but can be passed to a delegate, who will attend in place of the Invitee.
3. an invitation is an open invitation to anyone wishing to attend.

Invitations contain “keys” which conform to the above invitation level. Level 1 keys may not be passed to any other person and may not be copied. Level 2 keys may be passed to exactly one other person and may not be copied. If the key is returned to the original invitee than it may be passed again. Level 3 keys may be freely distributed and copied. The meeting is considered to be public.

The meeting room “knows” about each key and its invitation level.
Persons with improper keys are not admitted to the room. A person without a key may be admitted to the room only by someone already in the room or by the person responsible for the room. Invitations and keys are distributed electronically. The key is an electronic object attached to the invitation.

(Roseman, 9:34-55 (underlining added).)

The passages above show that the “**keys**” in Roseman qualify as “**tokens**” because they are pieces of information associated with user identity, that control whether a user has permission to enter a conference room. Roseman states that a “key is, essentially, a block of data, or a code.” (Roseman, 6:60-61; *see also id.*, 9:54-55 (“The key is an electronic object attached to the invitation.”).)

A “key” is also associated with user identity. For example, the “Level 1” key described in the passage above is associated with a single invitee, and cannot be passed to or used by any other person. (Roseman, 9:37, 9:43-44.) The key is also used to determine whether a user will be allowed access to the conference room. (Roseman, 10:61-64 (“To open a door with a key, the user drops the key onto the door lock. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.”) (underlining added).) The “keys” therefore qualify as “**tokens**” within the meaning of the ’356 patent.

Roseman also discloses that the host computer has a “**database which serves as a repository**” of keys (tokens), because the host computer stores the keys for a particular conference room. In particular, Roseman discloses that a “meeting room” is stored on the host computer. (Roseman, 9:61-63 (“Meeting Facilitator (or Requestor) creates [sic] meeting room on a host computer which is accessible to all Invitees.”), 7:30-31 (“[T]he host creates the conference room.”), 12:16-18 (“The conference room itself is actually a combination of stored data and computer programs.”).) As noted above, Roseman explains that “[t]he meeting room ‘knows’ about each key and its invitation level. Persons with improper keys are not admitted to the room.” (Roseman, 9:49-51 (underlining added).)

A copy of each key is therefore stored on the host computer – otherwise the meeting room could not “know[] about each key and its invitation level” (*id.*), or verify whether the invitee’s user’s key was valid in response to a request for access. (Roseman, 10:61-64.) Thus, Roseman discloses a host computer with a “database which serves as a repository of tokens.”

As noted previously, although Roseman discloses the claimed database and repository of tokens, it does not expressly use the word “**database**” or describe the storage methodology in detail. But this provides no meaningful distinction over Roseman. A person of ordinary skill in the art would have understood the claimed “database” under its broadest reasonable construction to simply refer to a stored

collection of tokens. (Lavian Decl. ¶ 65.) The '356 patent does not require that the database be any particular type, such as relational. (*Id.*)

In any event, even if Roseman did not sufficiently disclose the claimed “database which serves as a repository of tokens,” the addition of a database to Roseman would have been obvious. Database technologies predated the '356 patent by decades, and it was known to use databases to store user identity and authentication information (“tokens”). (*Id.* ¶ 66.)

For example, Rissanen, entitled “Password Verification System,” discloses a technique for user authentication in which user identity information and passwords, which are analogous to and serve the same purpose as the “keys” in Roseman, are stored in a database:

Some business computer systems are arranged to initially record and store passwords assigned to users. In response to a prompt by the system for the user’s password, the user enters the password onto a keyboard and the system compares the keyboard entered password with the stored passwords and enables the user to access the system when the entered password matches the previously stored password.

(Rissanen, Ex. 1004, 1:21-28 (underlining added).) Rissanen discloses that this password information, as well as the user’s account code (login information), are stored in a database. (Rissanen, Ex. 1004, at 2:26-29 (“Users are initially entered into a password database stored in the computer system by assigning each user an

account code and a password, such as consisting of a number of numerical digits.”), Fig. 2 (showing password file **101** with passwords for each user).)

Rationale and Motivation to Combine: It would have been obvious to a person of ordinary skill in the art to combine Roseman with Rissanen, with no change in their respective functions, predictably resulting in the virtual conference system of Roseman in which the conference room “keys” are stored in a database which serves as a repository of keys for other programs to access. (Lavian Decl. ¶ 67.) A skilled artisan would have understood that the user identity and password information in Rissanen is analogous to the “keys” in Roseman, and would be motivated to make this combination. (*Id.*)

In fact, a person of ordinary skill in the art reading Roseman would have found it plainly apparent that the host computer should store and maintain a copy of the keys issued to invitees in order to verify the stored key against a key later provided by a user seeking access. (*Id.*) In fact, the key verification step in Roseman might not even function properly if the host computer could not store and retrieve previously-issued key information. (Roseman, 9:49-50 (“The meeting room ‘knows’ about each key and its invitation level.”), 10:61-64 (“To open a door with a key, the user drops the key onto the door lock. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.”).) Storing the keys in a database is one of a finite number of predictable,

well-known solutions to the problem of verifying whether a previously-issued key matches or otherwise corresponds to a key later presented by a user seeking access to a conference room. (Lavian Decl. ¶¶ 67, 68.) There is nothing non-obvious about storing “keys” in a database.

Now continuing back with the preamble of claim 1, Roseman discloses that the database serves as a repository of tokens **“for other programs to access.”** Roseman discloses that the keys on the host computer may be accessed by “other programs,” *e.g.*, the various meeting or conference rooms maintained on the host computer. As noted above, Roseman discloses that each conference room “is actually a combination of stored data and computer programs.” (Roseman, 12:16-18 (underlining added).) Moreover, in order to access a conference room, the host computer presents a virtual “hallway” containing “doors,” each door representing a different conference/meeting room. (Roseman, 9:63-65 (“The meeting room door is accessible from a hallway which has doors to other meeting rooms.”), 10:28-29 (“Meeting rooms are child rooms of the hallway.”).) Each meeting room therefore contains a number of computer programs, and each meeting room itself can be thought of as a program. These programs access the repository of keys when a user presents a key to obtain access to a conference room.

As explained in Roseman: “When a person wants to go to a room, he first enters the hallway. The user’s display shows an image of a hallway with various

doors to rooms.” (Roseman, 10:30-32.) If a user locates the door for the appropriate conference, it can drop the key to attempt to gain access: “To open a door with a key, the user drops the key onto the door lock. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.” (Roseman, 10:61-64.) The repository of tokens is therefore accessed by the conference rooms and the programs within them, *e.g.*, to verify if the user-provided token is valid. Moreover, the repository is also indirectly accessed by programs on participant computers as they must present their key to the host computer, which in turn validates the key against previously-issued keys in the repository to determine whether or not to allow access. Roseman in view of Rissanen therefore discloses multiple embodiments of a repository of tokens “**for other programs to access,**” as recited in the preamble.

The preamble of claim 1 concludes by reciting, “**thereby affording information to each of a plurality of participator computers.**” Roseman explains that, if the key (token) is valid and the user is authorized to use it, “the door opens and the user is admitted to the room. The other users in the room are alerted to a new presence and receive any relevant information.” (Roseman, 10:63-65.) The conference room participants are then afforded information:

When a user enters a room with other occupants, the data connection is made. Audio and video connections are made if supported by the

user, the room and the other users. A small picture of each user is displayed in the meeting room to indicate presence. If video links are enabled than [sic] the picture may be replaced with a video signal from the user, typically showing the user. The majority of the display shows the room's table, walls, etc.

(Roseman, 11:11-17.) Roseman discloses multiple ways of communicating (“affording”) information to meeting participants. For example, participants can place documents on a virtual table of the conference room to share with other users (8:1-4, 11:18-22), write shared notes (8:18-21), engage in private voice conversations with other participants (9:16-25), and send private text messages to other participants (9:26-31). Additional details on “affording information” are provided in the discussion of element 1[c], below.

The preamble of claim 1 concludes by reciting, thereby affording information to each of “**a plurality of participator computers.**” The participator computers in Roseman are called “local computers.” (Roseman, 1:34-35, 2:64-65.) Each of these local computers can run conventional operating systems and environments such as Microsoft Windows. (Roseman, 12:1-9.)

Finally, the claim requires that each local computer be “**otherwise independent of each other.**” Roseman meets this limitation because the local computers are located at different geographic locations and only become part of a virtual conference when connected to the host computer. (Roseman, 3:14-19)

(“These individual systems are located at different geographic locations, and, when a virtual conference is to be held, become connected to a central, host, computer (or multiplicity of host computers) . . .”).) Roseman confirms, in fact, that the local computers can be separated by considerable distances, *e.g.* in different states or in several cities within a state. (Roseman, 4:47-53, Fig. 4, Fig. 5 (showing company facilities in several cities in Ohio).) In the event it is argued that Roseman’s local computers are not “otherwise independent of each other” because they are connected through a network belonging to an enterprise or company, it would have been trivially obvious, as discussed above, to adapt Roseman to the Internet such that the Internet is the only network shared by the individual local computers. The participator computers in Roseman are therefore “otherwise independent of each other,” as recited in the preamble.

b. “authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database” (Claim 1[a])

Roseman discloses authenticating at least “a first user identity” and “a second user identity” according to permissions retrieved from the repository of tokens of the database, as recited in the claim. As explained in the discussion of the preamble, Roseman discloses that each user must be authenticated by using a “key” to attempt to enter the conference.

To open a door with a key, the user drops the key onto the door lock.

If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room. The other users in the room are alerted to a new presence and receive any relevant information.

(Roseman, 10:61-65 (underlining added).)

This process involves authenticating a “**user identity**.” As noted above, the host computer can assign a “Level 1” key to a user, which is “for the Invitee only” and “may not be passed to any other person and may not be copied.” (Roseman, 9:37, 9:43-44). Such a key is therefore associated with a single particular user identity. “The meeting room ‘knows’ about each key and its invitation level. Persons with improper keys are not admitted to the room.” (Roseman, 9:49-51.)

Finally, the user identity authentication process described above may occur for at least “**a first user identity**” and “**a second user identity**,” and more, because a conference may have multiple invitees. (See Roseman, Fig. 9 (showing conference having six participants).) Although Roseman describes the validation and authorization process above (e.g. invitee drops a key onto a lock to enter a conference room) by reference to one invitee, it would have been obvious to a person of ordinary skill that the same process would be repeated for each invitee who joined the conference. (Lavian Decl. ¶¶ 77, 78.) As Roseman explains, “[w]hen time for the conference has arrived, the host computer takes roll of the

participants as each arrives.” (Roseman, 7:44-45.) “When all participants have arrived, the meeting begins.” (Roseman, 7:54.)

c. **“affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity” (Claim 1[b])**

Roseman next discloses that, responsive to the first user identity being authenticated and allowed to enter the conference room, the host computer transmits (“affords”) some of the information from the conference room to that participant’s computer. As Roseman explains:

When a user enters a room with other occupants, the data connection is made. Audio and video connections are made if supported by the user, the room and the other users. A small picture of each user is displayed in the meeting room to indicate presence. If video links are enabled than the picture may be replaced with a video signal from the user, typically showing the user. The majority of the display shows the room’s table, walls, etc.

(Roseman, 11:10-17.) For example, the “display” that “shows the room’s table, walls, etc” and the “small picture[s]” or “video signal[s]” of other users in the conference room are communicated (“afforded”) to the participant **“responsive to”** the participant being authenticated and allowed to enter the room. In addition:

Objects (documents) can be shared in the conference room by placing them on the table. This might be done by dragging an icon of the object from the outside (users non-“meeting room” windows) onto the

table. Ownership of the object is still maintained. If the object owner wishes, the object may be copied, borrowed by other users, or given to other users. The object may be altered (changed, annotated) by anyone with permission to do so.

(Roseman, 11:18-26 (under “Inside the Meeting Room”).)

Roseman discloses several other ways of communicating (“affording”) some of the information to the first participant computer. For example:

- A participant can use a “notepad” tool to write on the virtual walls of the conference room. (Roseman, 8:18-37.)
- A participant can enter “Whisper Mode” to engage in a private voice conversation. (Roseman, 9:16-25.) “At this time, the host makes an audio connection between the two whispering parties, and between nobody else.” (Roseman, 9:22-23.)
- A participant can pass a private textual note. (Roseman, 9:26-31.) “When the other party sees the note on his picture, as in Figure 12, he can drag it to a private viewing area, double-click it, and read it. No other people are aware of the passed note.” (Roseman, 9:28-31.)

These categories of information are communicated (“afforded”) to the participant “responsive to” the participant being authenticated because the participant would otherwise not be able to receive such information.

As noted above, this limitation recites “affording **some** of the information to a first of the participator computers.” To the extent the word “some” requires that not all of the information in a conference room be made available to the first participant computer, this is readily disclosed by the teachings above. Because meeting participants can engage in private conversations and one-on-one note-passing, Roseman makes clear that less than all of the information for a conference may be made available to a given participant. (Lavian Decl. ¶ 82.)

Finally, this claim limitation recites “affording some of the information to a first of the participator computers **via the Internet network**.” Roseman discloses that the host and participant computers may be connected via a Wide Area Network (WAN). (Roseman, 3:14-19, 1:37-41.) A person of ordinary skill in the art would have understood that the Internet is a Wide Area Network (WAN), but Roseman does not expressly mention the Internet. (Lavian Decl. ¶ 83.)

But adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill. (*Id.* ¶¶ 84-89.) For example, Vetter discloses that, well before April 1996, the Internet was being used to facilitate precisely the same types of computer-based conferencing functions described in Roseman, such as video and audio conferencing and document sharing (via shared whiteboards):

Videoconferences are becoming increasingly frequent on the Internet

and generating much research interest. Readily available software tools enable real-time audio and video channels as well as shared whiteboards that allow groups to collaborate on distributed group work more quickly and easily than ever (see sidebar on available tools).

The Internet infrastructure is beginning to support videoconferencing applications in several ways. First, the emerging multicast backbone (or MBone) can efficiently send traffic from a single source over the network to multiple recipients. At the same time, many workstations attached to the Internet are being equipped with video capture and sound cards to send and receive video and audio data streams. The price/performance of these hardware devices has finally reached a level that makes wide-scale deployment possible, which is perhaps the most important factor in the recent growth of videoconferencing applications.

(Vetter, Ex. 1005, at p. 77 (underlining added).)

Vetter describes a number of conferencing tools for performing real-time collaboration over the Internet. (*Id.* at p. 78 (under “Available Conferencing Tools”).) One example is “CU-SeeMe,” which Vetter describes as “a software platform that supports audio and video conferencing over the Internet.” (*Id.*) Vetter explains that CU-SeeMe “is becoming very popular” (*id.* at p. 77), and discloses a server program known as the CU-SeeMe “reflector” that facilitates

multiparty conferencing. (*Id.* at p. 78.) Vetter therefore discloses communicating information to participator computers via the Internet network.

Rationale and Motivation to Combine: It would have been obvious to a person of ordinary skill in the art to combine Roseman with Vetter, with no change in their respective functions, predictably resulting in the conferencing system of Roseman in which the host and participant computers communicate via the Internet. (Lavian Decl. ¶ 86.) Vetter provides an express motivation for this combination by confirming that “[v]ideoconferences are becoming increasingly frequent on the Internet” (Ex. 1005, p. 77), and that the “CU-SeeMe videoconferencing tool is also becoming very popular.” (*Id.* (underlining added to both).) Moreover, a person of ordinary skill in the art would have recognized the Internet as a leading network for connecting remote computers, making it the obvious choice of Wide Area Network (WAN). (Lavian Decl. ¶ 86.)

Nothing in Vetter would discourage or “teach away” from this combination. Vetter has an extended discussion of some of the challenges he encountered in using Internet videoconferencing in a classroom context. As explained in great detail by Dr. Lavian, none of those issues would have discouraged a skilled artisan from adapting Roseman to the Internet. (*Id.* ¶¶ 88-89.)

- d. “affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity” (Claim 1[c])**

This limitation is substantially identical to the previous limitation except that it pertains to the “second of the participator computers” and the “second user identity.” The analysis for the previous limitation applies with full force here. As explained above, Roseman discloses that a conference can contain multiple participants who receive and share information. Because the features described in Roseman are available to multiple conference participants, the same analysis for the “first participator computer” in claim 1[b] would apply to a second participator computer. (Lavian Decl. ¶ 90.)

- e. “running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers” (claim 1[d])**

Roseman discloses that the software running on the controller computer (the “host computer”) controls the conference/meeting room. In fact, Roseman includes an Appendix with “pseudo-code” instructions describing the various programming operations that the host computer can perform to carry out conference functions. (Roseman, 12:66-13:2, 13:7-16:43.)

Roseman discloses that the controller software on the host computer uses “predefined rules” to “direct arbitration of which ones of the participator

computers interactively connect within a group of the participator computers.” For example, a conference requester specifies a number of things upon creating a conference, such as “[w]hat rules govern the conduct of the meeting,” “[d]oes the Requester have absolute control of the voice and message interaction among the participants,” or “[i]s the meeting a brainstorming free-for-all, where numerous people can speak at once?” (Roseman, 3:52-56.) These predefined rules are further described as follows:

The room may be used to impose discipline on the meeting procedure. For instance, Robert’s Rules of Order may be used to prevent a free for all of communication. The room would require that certain procedural issues be followed before allowing a vote, identified or anonymous, to occur (another built in meeting procedure), or before someone was allowed to speak. Within the room a talking queue might be built so that only one person would speak at a time, followed by the next person and so on.

(Roseman, 11:38-46 (underlining added).)

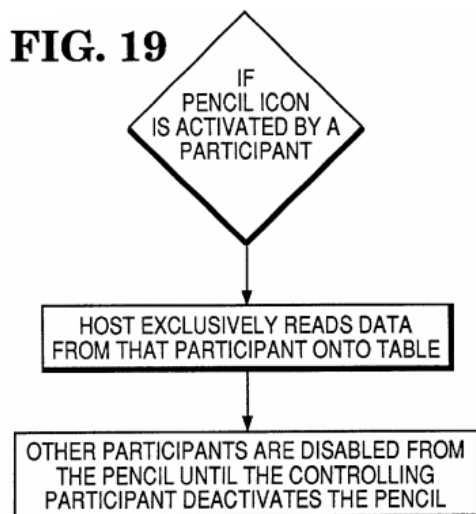
Roseman therefore discloses predefined rules that may be used to “direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers.” A person of ordinary skill in the art would have understood that the rules described above are enforced through software functionality on the host computer (“controller software on the controller computer”). (See Lavian Decl. ¶ 93; Roseman, 1:50-52 (“The host controls many

of the events occurring during the conference, as well as those occurring both during initiation of the conference and after termination of the proceedings.”).)

Roseman also discloses that these rules qualify as “**predefined rules**” because the user can specify them as part of the conference room creation process, before any participant has joined. (Roseman, 3:22-28, 3:52-56 (in creating a conference room, the requester may specify “[w]hat rules govern conduct of the meeting”).)

Roseman discloses many other examples of “predefined rules” enforced by the host computer that separately and independently satisfy this limitation. For example, Roseman teaches a “pencil” tool that allows a participant to “write” in the conference room. As shown in Figure 19 (to the right), when a participant activates the pencil feature, other participants may not use the pencil until the controlling participant is finished. This provides another example of “**predefined rules**” that arbitrate which participant may use the pencil.

FIG. 19



Roseman also describes at least two private messaging techniques that satisfy this claim limitation. First, as described previously, a participant can enter “Whisper Mode” to engage in a private voice conversation with another participant. (Roseman, 9:16-25.) “At this time, the host makes an audio

connection between the two whispering parties, and between nobody else. The parties can communicate, until they terminate whisper mode.” (Roseman, 9:22-25 (underlining added).) Second, a participant can pass a private textual note to another participant. (Roseman, 9:26-31.) “When the other party sees the note on his picture, as in Figure 12, he can drag it to a private viewing area, double-click it, and read it. No other people are aware of the passed note.” (Roseman, 9:28-31 (underlining added).) The privacy of the note is enforced by software functionality on the host. (Roseman, 15:12-15 & Fig. 17C (“HOST TRANSMITS NOTE TO IDENTIFIED PARTICIPANT ONLY.”) (capital letters in original).)

In both of these examples, Roseman discloses a means of privately sharing information between two participants of the conference that is not shared with other participants. These features provide a further example of rules that determine what information will be provided to which participant computer – in other words, “direct[ing] arbitration of which ones of the participator computers interactively connect within a group of the participator computers,” as recited in the claim.

All of these functionalities involve software running on the host computer, *i.e.* “**controller software on the controller computer**,” as claimed. Roseman confirms as much by including an Appendix with “[p]seudo-code usable for programming the host and the local computers,” which is “considered self-explanatory” and also “presented in flow-chart format in FIG. 15, et seq.”

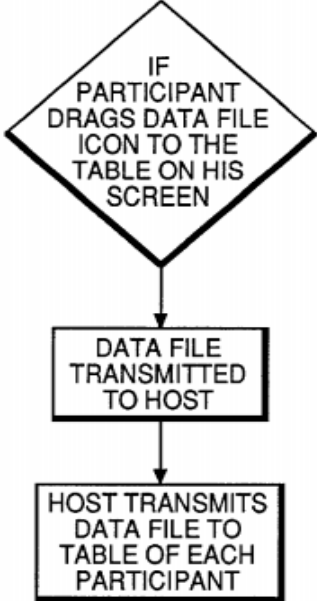
(Roseman, 12:66-13:2.) That pseudo-code describes how the host computer carries out the Whisper Mode, note-passing and pencil features discussed above. (Roseman, 15:6-9 & Fig. 17B (Whisper Mode), 15:10-13 & Fig. 17C (private note-passing), 15:21-27 & Fig. 19 (pencil).) All of these functionalities further describe “predefined rules” because the access controls are performed by the preexisting and built-in programming for these conference features, and as such, before any participant joined the meeting. (Lavian Decl. ¶ 97.)

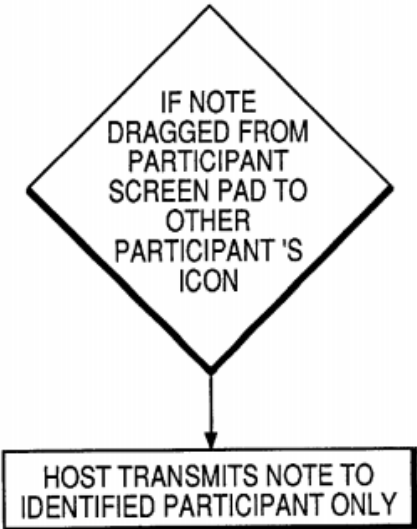
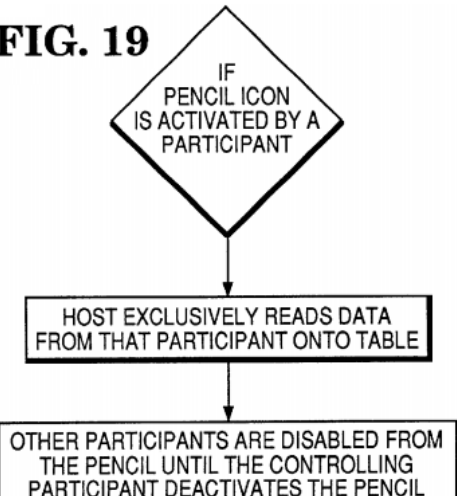
- f. **“providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers” (claim 1[e])**

Because of the length of this claim limitation, this Petition will address portions of the language to ensure all of its limitations are covered.

As explained above, the phrase, **“providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type,”** should be construed under its broadest reasonable construction as “providing software functionality on the controller computer for sending and receiving messages of different types and communicating each message to software functionality based on the message type.” As noted, Roseman discloses pseudo-code programming for the host computer, which is also shown in Figures 15-22.

(Roseman, 12:66-13:2.) This software functionality performs functions such as responding to a file being dragged onto the virtual conference/meeting table (Fig. 16A), one participant sending a private note to another (Fig. 17C), one participant using an electronic “pencil” and having his or her actions shown to other participants (Fig. 19), among others. In each of these examples, the host computer receives a type of message and routes the message to the appropriate software functionality to handle that message type, as shown below:

Pseudocode Functionality from Roseman	Multiplexing/Demultiplexing Messages by Type
<p>FIG. 16A</p>  <pre> graph TD A{IF PARTICIPANT DRAGS DATA FILE ICON TO THE TABLE ON HIS SCREEN} --> B[DATA FILE TRANSMITTED TO HOST] B --> C[HOST TRANSMITS DATA FILE TO TABLE OF EACH PARTICIPANT] </pre>	<p>The host computer receives a message of a particular type (e.g. a participant has dragged a file icon onto his or her conference table), to which the host responds by invoking software to receive the file and then send it to each participant.</p> <p>(<i>See also</i> Roseman, 8:1-5 (“Each Invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it. To place a document on the table, an Invitee performs a ‘drag-and-drop.’).)</p>

Pseudocode Functionality from Roseman	Multiplexing/Demultiplexing Messages by Type
<p>FIG. 17C</p>  <pre> graph TD A{IF NOTE DRAGGED FROM PARTICIPANT SCREEN PAD TO OTHER PARTICIPANT'S ICON} --> B[HOST TRANSMITS NOTE TO IDENTIFIED PARTICIPANT ONLY] </pre>	<p>The host computer receives a message of a particular type (request by one participant to send a private note to another), to which the host responds by activating software functionality to receive the note and transmit it only to the other identified participant (and no one else).</p> <p>(See also Roseman, 9:26-31 (“One person can write a note . . . and drag it to the picture of another party. When the other party sees the note on his picture, as in FIG. 12, he can drag it to a private viewing area, double-click it, and read it. No other people are aware of the passed note.”).)</p>
<p>FIG. 19</p>  <pre> graph TD A{IF PENCIL ICON IS ACTIVATED BY A PARTICIPANT} --> B[HOST EXCLUSIVELY READS DATA FROM THAT PARTICIPANT ONTO TABLE] B --> C[OTHER PARTICIPANTS ARE DISABLED FROM THE PENCIL UNTIL THE CONTROLLING PARTICIPANT DEACTIVATES THE PENCIL] </pre>	<p>The host computer receives a message of a particular type (pencil icon), to which the host responds by activating software functionality to receive the input from the participant and modify the table accordingly, while disabling other participants from using the pencil.</p>

(Lavian Decl. ¶ 100.)

As shown above, Roseman discloses software functionality that transmits and processes particular types of messages, such as placing a document on the table (causing the document to be sent to each participant), using the pencil

(causing the participant's actions to be sent to each participant), sending a private message (causing the message to be sent only to the intended recipient), and other messaging functions. Messages corresponding to these commands are multiplexed because the host computer processes each message using the software functionality described above – using the message type to determine the appropriate software.

Moreover, the fact that Roseman discloses the claimed “multiplexing” and “demultiplexing” is further confirmed by the Background section of the '356 patent, which identifies conferencing systems like Roseman as examples of systems that perform “multiplexing” as that term is used in the patent:

On a more complex level, corporations may link remote offices to have a conference by computer. A central computer can control the multiplexing of what appears as an electronic equivalent to a discussion involving many individuals.

('356, Ex. 1001, 1:42-45 (underlining added).) This description mirrors what the “host computer” in Roseman does.

Turning to the next part of this limitation, Roseman discloses “**creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers.**” The virtual conference room in Roseman provides the “virtual connection” recited in this claim limitation.

First, the software functionality described above (the “API”) provides a virtual conference room that connects a group of participants (a “**channel**”) via the host computer. (Roseman, 7:44-45, 7:54-56 (“When time for the conference has arrived, the host computer takes roll of the participants as each arrives. . . . When all participants have arrived, the meeting begins. The table is a common display area which is shown to, and available for work by, each Invitee.”).) Each conference room can also have “child rooms” that conference room participants can join. (Roseman, 10:18-25.) Each “child room” can thus serve as a secondary “**channel**” within the parent conference room. (Roseman, 10:22-23 (“A person may not enter the child-room if he cannot enter the parent room.”).)

With respect to “**private messages**,” once the meeting begins, the virtual conference room allows participants to send and receive private messages via note-passing or private conversions, as previously mentioned. (Roseman, *e.g.*, 2:49-50 (“The participants can privately whisper or pass notes to each other, without the knowledge of the others.”).)

Finally, the virtual conference room allows the participants to share and collaborate on “**multimedia objects**” through the host computer. The ’356 patent does not define the word “multimedia,” but it generally refers to content that combines two or more media types (such as graphics, text, video, audio, etc.). (Lavian Decl. ¶ 107.) Consistent with this understanding, the patent identifies a

web page containing graphics and text (Fig. 26) as an example of a “graphical multimedia message.” (’356, 3:53-55; *see also id.*, 11:1-3.)

Roseman explains that “[w]ith ‘multi-media’ conferencing, multiple parties are linked by both video and audio media: the parties can see, as well as hear, each other.” (Roseman, Abstract (underlining added).) For example, a user can place a multimedia document, such as a document including text and graphics, on the virtual table and then draw or point to different positions on the document. (Roseman, 2:38-45 (“In the invention, the participants share a common virtual conference table. Each participant can (1) place a document onto the table electronically, (2) write on the document, draw on it, and otherwise manipulate it, and (3) move a pointer to different positions on the document, to point to specific parts of it.”), 8:1-4 (“Each Invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it.”).) At the same time, users can communicate with each other via audio and video. (*See, e.g.*, Roseman, 7:65-67 (“With this cursor positioning, each participant can point to items which he or she verbally discusses, using the audio link.”), 11:11-13 (“When a user enters a room with other occupants, the data connection is made. Audio and video connections are made if supported by the user, the room and the other users.”).) Roseman therefore discloses a virtual connection for multimedia objects.

Roseman accordingly discloses a virtual conference room that allows groups of conference participants to communicate via the host computer, including through private messages or collaboration on multimedia objects.

g. “communicating real-time messages within the group of the interactively connected said participator computers” (claim 1[f])

This final limitation was already covered in previous claim limitations. Roseman discloses that real-time messages are communicated within the group of the interactively connected participator computers, placing documents on the table and moving from the electronic pencil, among others. Roseman confirms that these messages are communicated in real-time:

In the invention, the participants share a common virtual conference table. Each participant can

- (1) place a document onto the table electronically,
- (2) write on the document, draw on it, and otherwise manipulate it, and
- (3) move a pointer to different positions on the document, to point to specific parts of it.

All other participants see the [sic] the preceding three events as they occur.

(Roseman, 2:38-47 (underlining added); *see also id.*, 7:54-8:5.)

All of these interactions involve “real-time messages” because the messages are communicated to participants as the underlying events occur. In fact, Roseman

discloses a feature for recording and archiving the “real-time” events and discussions at a conference. (Roseman, 8:41-46 (“The Requester is given several options of recording the conference. One option is a recording, in real-time, of all events and discussions occurring during the conference.”), 12:26-28 (“This persistence allows a person who did not attend the virtual conference in real time to witness it, or parts of it, afterward.”) (underlining added to both).)

2. Claims 2-5 (Different Media Types)

Dependent claims 2-5 recite closely-related subject matter:

2. The method of claim 1, wherein the communicating content includes communicating at least one of sound, video, graphic, pointer, and multimedia content.
3. The method of claim 2, wherein said at least one comprises at least two.
4. The method of claim 2, wherein said at least one comprises at least three.
5. The method of claim 2, wherein said at least one comprises at least four.

(’356, 21:57-65.) Roseman makes clear that at least four types of content (sound, video, graphic, multimedia) may be communicated to conference participants. The fifth type of content (“pointer”) is addressed in Ground 2.

Sound and Video: As explained in Roseman: “When a user enters a room with other occupants, the data connection is made. Audio and video connections

are made if supported by the user, the room and the other users. A small picture of each user is displayed in the meeting room to indicate presence. If video links are enabled than [sic] the picture may be replaced with a video signal from the user, typically showing the user.” (Roseman, 11:11-16 (underlining added).) As explained at length previously, Roseman discloses that users can talk to each other. (Roseman, 9:16-25, 11:11-13, 11:44-46, 12:34-45.)

Graphic: Roseman discloses many ways in which graphic content may be communicated. For example: “Each Invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it.” (Roseman, 8:1-4 (underlining added); *see also id.*, 1:42-46 (“The parties can send the information which they want displayed, such as drawings, to the host computer. The host computer generates a common video screen, which it distributes to the parties: they see the drawings at their own local computers.”) (underlining added).)

Multimedia: As noted for claim 1, Roseman explains that “[w]ith ‘multi-media’ conferencing, multiple parties are linked by both video and audio media: the parties can see, as well as hear, each other.” (Roseman, Abstract (underlining added).) As explained in detail above and in the preceding paragraphs of this section, Roseman confirms that conference room content can include sound, video, graphics, and text, thus disclosing many examples of “multimedia content.”

3. Claims 8, 9, and 12 (“API Messages”)

Claim 8 recites, “[t]he method of claim 1, wherein the API includes API messages,” and claim 9 recites, “[t]he method of claim 1, wherein communications among the controller computer and the participator computers are mediated via API messages.” Claim 12 recites, “[t]he method of claim 1, wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages.” These claims do not appear to impose any limitations that were not already covered in the discussion of claim 1 above.

As explained previously, the software functionality on the host computer in Roseman (the “API”) sends and receives messages (“API messages”) to communicate information to other participants and to control the features of the conference, such as activating the pencil icon, placing a document on the table, engaging in private audio or voice communications, or sending private textual notes. (*See supra* **Part IV.E.1(f)**, the analysis of the “providing an API on the controller computer” limitation of claim 1.) These claims are therefore unpatentable for the same reasons as claim 1.

4. Claims 14, 15 (“Censorship” Claims)

Claim 14 recites “[t]he method of claim 1, further including determining censorship of the content,” and claim 15 recites “[t]he method of claim 1,

wherein the controller computer determines censorship.” Roseman describes several means of censorship. For example:

The room would require that certain procedural issues be followed before allowing a vote, identified or anonymous, to occur (another built in meeting procedure), or before someone was allowed to speak.

Within the room a talking queue might be built so that only one person would speak at a time, followed by the next person and so on.

(Roseman, 11:40-46.) In addition, the host computer (the “controller computer”) can perform censorship by acting as a conference “moderator” and regulating when and/or how long participants can speak during the conference, or preventing a disruptive participant from continuing to speak. (Roseman, 12:29-45.)

These disclosures satisfy the “censorship” limitation of claims 14 and 15. In fact, Roseman’s examples of limiting who can communicate mirror the examples of “censorship” in the written description of the ’356 patent. (’356, 8:41-46 (“Censorship can control of [sic] 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 can also use the tokens for real time control of data (ascii, text, video, audio) from and to users”).)

5. Independent Claim 19

Claim 19 recites an apparatus with substantially similar limitations as claim

1. As shown by the side-by-side chart below, in fact, claim 19 is actually somewhat broader than claim 1 as it is missing two limitations. Nevertheless, as shown by the underlining below showing overlap of claim language, there is no material difference between the two claims for purposes of Ground 1:

Method Claim 1	Apparatus Claim 19
1. A method of <u>communicating content among users</u> using [sic] <u>of a computer system</u> including a <u>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</u> , the method comprising:	19. An apparatus to <u>communicate content among users of a computer system</u> . . . comprising: <u>a controller 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</u> in communication with each of the participator computers by
[a] <u>authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database;</u>	<u>authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database,</u>
[b] affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	<i>Limitation not present</i>
[c] affording some of the information to a second of the participator computers via the Internet network, responsive to	<i>Limitation not present</i>

Method Claim 1	Apparatus Claim 19
an authenticated second user identity;	
[d] <u>running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers;</u>	wherein the <u>controller computer is running controller software, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers, to</u>
[e] <u>providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers; and</u>	<u>provide an API on the controller computer, whereby the API multiplexes and demultiplexes API messages by type, to create a virtual connection and provide the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers, and to</u>
[f] <u>communicating real-time messages within the group of the interactively connected said participator computers.</u>	<u>allow communication of real-time messages within the group of the interactively connected said participator computers.</u>

As shown above, other than the fact that claim 19 lacks the two “affording” limitations from claim 1, the differences between claim 1 and 19 consist largely of insubstantial verb tense differences. As explained in connection with claim 1 above, this claim is obvious over Roseman and Rissanen. Roseman discloses an apparatus in the form of a computer system that includes the controller computer (“host computer”), and the participator computers (participants’ “local

computers”). The host computer carries out all of the functions of claim 19 for the same reasons as claim 1. (Lavian Decl. ¶¶ 133, 134.)

6. Claims 20-24, 27, 28, 31, 33-35 (Dependent Claims)

These claims depend from claim 19 and are substantially the same as claims depending off independent claim 1 (underlining showing overlap):

Apparatus Dependent Claims	Method Dependent Claims
20. The apparatus of claim 19, <u>wherein the content includes at least one of sound, video, graphic, pointer, and multimedia content.</u>	2. The method of claim 1, <u>wherein the communicating content includes communicating at least one of sound, video, graphic, pointer, and multimedia content.</u>
21. The apparatus of claim 20, <u>wherein said at least one comprises at least two.</u>	3. The method of claim 2, <u>wherein said at least one comprises at least two.</u>
22. The apparatus of claim 20, <u>wherein said at least one comprises at least three.</u> 23. The apparatus of claim 20, <u>wherein said at least one comprises at least three.</u> (Duplicates)	4. The method of claim 2, <u>wherein said at least one comprises at least three.</u>
24. The apparatus of claim 20, <u>wherein said at least one comprises at least four.</u>	5. The method of claim 2, <u>wherein said at least one comprises at least four.</u>
27. The apparatus of claim 19, <u>wherein the API includes API messages.</u>	8. The method of claim 1, <u>wherein the API includes API messages.</u>
28. The apparatus of claim 19, <u>wherein communications among the controller computer and the participator computers are mediated via API messages.</u>	9. The method of claim 1, <u>wherein communications among the controller computer and the participator computers are mediated via API messages.</u>

Apparatus Dependent Claims	Method Dependent Claims
31. The apparatus of claim 19, <u>wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages.</u>	12. The method of claim 1, <u>wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages.</u>
33. The apparatus of claim 19, wherein the computer system <u>determines censorship of the content.</u>	14. The method of claim 1, further including <u>determining censorship of the content.</u>
34. The apparatus of claim 19, <u>wherein the controller computer determines censorship.</u>	15. The method of claim 1, <u>wherein the controller computer determines censorship.</u>
35. The apparatus of claim 19, <u>wherein the content is communicated over a network, including the Internet.</u>	16. The method of claim 1, <u>wherein the communicating is conducted over the network, including the Internet.</u>

For the same reasons provided above for claims 2-5, 8, 9, 12, and 14-16, respectively, these claims are unpatentable.

7. Independent Claim 37

Claim 37 presents another example of a redundant, duplicative claim that presents no material differences for purposes of Ground 1. In fact, it is essentially a spitting image of claim 19, with the primary difference being that claim 37 expressly requires the “Internet” whereas claim 19 does not.

Apparatus Claim 37	Apparatus Claim 19
37. An apparatus comprising: <u>a computer system, the computer system including</u>	19. An apparatus to communicate content among users of <u>a computer system, the computer system</u>

Apparatus Claim 37	Apparatus Claim 19
<u>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 independent participator computers which are otherwise independent of each other, via the Internet network communicating with the participator computers by</u>	comprising: <u>a controller 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 in communication with each of the participator computers by</u>
<u>authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database,</u>	<u>authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database,</u>
<u>the controller computer running controller software, in accordance with predefined rules, directing arbitration of which ones of the participator computers interact within a group of the participator computers,</u>	<u>wherein the controller computer is running controller software, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers, to</u>
<u>providing an API on the controller computer, whereby the API is multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers, and</u>	<u>provide an API on the controller computer, whereby the API multiplexes and demultiplexes API messages by type, to create a virtual connection and provide the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers, and to</u>
<u>providing communication of real-time messages within the group of the interactively connected said participator computers.</u>	<u>allow communication of real-time messages within the group of the interactively connected said participator computers.</u>

Claim 37 is obvious for the same reasons as independent claims 1 and 19, as explained in detail above.

C. Ground 2: Claims 6, 7, 17, 26, and 36 are Obvious Over Roseman, Rissanen, and Vetter, in Further View of Pike

Dependent claims 6, 7, 17 and 26 all address a particular type of content known as a “pointer,” such as a Uniform Resource Locator (URL). In particular, claim 6 requires that sound, video, graphic, multimedia and pointer content be communicated. As explained in the discussion of claims 2-5 for Ground 1 above, Roseman clearly discloses at least sound, video, graphic, and multimedia content, so only “**pointer content**” remains to be addressed for claim 6. Claims 7 and 26 similarly recite that the content includes a “**pointer**” that “**allows the content to be produced on demand.**” These limitations are disclosed by Roseman alone or in combination with Pike. Claims 17 and 36 recite that the content can be communicated by invoking “**a URL,**” which is disclosed by Pike. Because of the related subject matter of these claims, this Petition will address them together.

Roseman discloses several examples of a “**pointer.**” For example, if a user places a document onto the table of the virtual conference room, the host sends an icon to the table of each conference participant. (Roseman, 14:53-57.) This icon serves as a “pointer” because it points to, or references, the underlying document. Clicking on the icon by a participant causes the host computer to present the file to all participants. (Roseman, 14:59-62 (“IF ANY PARTICIPANT ACTIVATES

ICON ON TABLE,” “DATA FILE PRESENTED ON TABLE BY HOST,” “HOST SENDS OPEN FILE TO ALL PARTICIPANTS TABLES”) (capital letters in original).) The icon therefore points to the file on the host computer, and when clicked by the user, causes the content to each conference participant.

Roseman’s note-passing feature provides another example of a “pointer.” A user can type a note and drag it onto the picture of another meeting participant. (Roseman, 9:26-28.) A small square icon representing the note appears on the other participant’s screen. (Roseman, Fig. 12.) “When the other party sees the note on his picture, as in FIG. 12, he can drag it to a private viewing area, double-click it, and read it. No other people are aware of the passed note.” (Roseman, 9:28-31 (underlining added).) The icon similarly serves as a pointer because it points to, or references, the underlying note content, and causes the host computer to produce the content on demand.

The disclosures of Roseman alone disclose the claimed pointer functionality. But in the event it is later argued or determined that “pointer” requires an Internet URL or something functionally similar, then Roseman would render these claims obvious in view of the teachings of Pike [Ex. 1006].

Pike provides an introductory section describing basic Internet concepts including URLs. (Pike, Ex. 1006, at 36-39.) Pike explains that “[a] *URL* is a complete description of an item, including the location of the item that you want to

retrieve.” (*Id.* at 38 (*italics in original*).) “The location of the item can range from a file on your local disk to a file on an Internet site halfway around the world.” (*Id.*) Pike explains that a URL can identify any resource on the Internet, and “is not limited to describing the location of WWW [World Wide Web] files.” (*Id.*) Pike further explains that a URL can be used to locate and retrieve a document from another computer, and includes “a UNIX-style path for the file that you want to retrieve.” (*Id.* at 39.) Pike therefore discloses a “pointer” in the form of a URL.

As explained by Dr. Lavian, it would have been obvious to a person of ordinary skill in the art to combine Roseman and Vetter with Pike, with no change in their respective functions. This would have predictably resulted in the virtual conferencing system of Roseman in which the clickable icons used to access content (such as documents and notes) included a URL that identified the location of content on the host computer, that could be used to produce the content on demand. (Lavian Decl. ¶ 121.) There are several reasons a skilled artisan would have made this combination.

First, as explained above for claim 1, Vetter discloses the ability to use the Internet to enable videoconferencing features similar to Roseman. A person of ordinary skill in the art would have understood that, once a system is communicating over the Internet, the URL is a preferred means to identify resources on the Internet. (*Id.*)

Second, it was well-known to send messages containing Internet URLs. (Lavian Decl. ¶ 123.) In fact, Pike describes a technique for allowing a user to send email messages to others with URLs of interesting Internet resources. (Pike, at p. 121.) In fact, easily sending URLs in electronic messages was a key design goal for the people who invented the URL. (Lavian Decl. ¶¶ 123, 124.) By March 1995, URLs were being regularly distributed by large number of businesses, government agencies, academic institutions, and individuals. (Ex. 1012.)

Third, one of ordinary skill in the art would have recognized that use of the URL method, as taught by Pike, would be particularly advantageous in the context of the Internet and known bandwidth restrictions that existed at the time of the alleged invention. (*See id.* (citing Pike, Ex. 1006, at p. 43 (top of page)).) This is because the file content need not be communicated from the host computer to the participant (this consuming network bandwidth) unless the participant requests to view the content by invoking the URL. (*Id.*) It would have required no leap of inventiveness for a person of ordinary skill in the art to use the ubiquitous Internet URL with the system of Roseman.

Roseman specifically discloses that a document placed on the table of the conference room can include “text” (Roseman, 8:2) and thus, a person of ordinary skill in the art would have understood that such text could have been an Internet URL. (*Id.* ¶ 124.) By April 1996, therefore, a person of ordinary skill in the art

would have found adapting Roseman to send a message containing an Internet URL to meeting participants to be trivially obvious. (*Id.*)

D. Ground 3: Claims 18 and 25 Are Obvious Over Roseman in view of Rissanen and Vetter, in further view of Gosling

Dependent claims 18 and 25 recite that the controller software comprises “a JAVA™ application.” These claims add nothing of patentable significance. As explained by Dr. Lavian, Java was a known programming language that could be used to build application software. (Lavian Decl. ¶ 131.) A person of ordinary skill in the art would have been motivated to use Java for a variety of reasons, the main one being that Java compiled programs were “portable” and thus could execute on any kind of CPU. (Gosling, Ex. 1007, at p. 115.) By using Java for the host computer software in Roseman, the developer would be freed from the burden of having to rewrite or change the application in the event of a change in the type of CPU or computer architecture. (Lavian Decl. ¶ 56.)

VI. CONCLUSION

The Petitioner respectfully requests institution of *inter partes* review of claims 1-9, 12, 14-28, 31 and 33-37 and a finding that they are unpatentable.

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

Dated: January 7, 2017

Respectfully submitted,

By: /Joseph A. Micallef
Joseph A. Micallef
USPTO Reg. No. 39,772
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: 202-736-8492
Facsimile: 202-736-8711
iprnotices@sidley.com

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

CERTIFICATE OF COMPLIANCE WITH WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), I certify that this petition complies with the type-volume limits of 37 C.F.R. § 42.24(a)(1)(i) because it contains 12,742 words, excluding the parts of this petition that are exempted by 37 C.F.R. § 42.24(a), according to the word-processing system used to prepare this petition.

Dated: January 7, 2017

By: /Joseph A. Micallef
Joseph A. Micallef
USPTO Reg. No. 39,772
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Telephone: 202-736-8492
Facsimile: 202-736-8711
iprnotices@sidley.com

Petition for *Inter Partes* Review of
U.S. Patent No. 8,407,356

CERTIFICATE OF SERVICE

I hereby certify that on this 7th day of January, 2017, a copy of this Petition, including all attachments, appendices and exhibits, has been served in its entirety in the manner indicated below on the following:

Peter K. Trzyna, ESQ.
PO BOX 7131
Chicago IL 60680
Pkt-law@sbcglobal.net
Pktlawoffice@gmail.com

U.S. Mail Priority Express & Email

Peter Lambrianakos
Brown Rudnick LLP
7 Times Square
New York, NY 10036
plambrianakos@brownrudnick.com
afabricant@brownrudnick.com
vrubino@brownrudnick.com

Federal Express & Email

Bradley W. Caldwell
Jason D. Cassady
John Austin Curry
Warren J. McCarty
CALDWELL CASSADY & CURRY
2101 Cedar Springs Road, Suite 1000
Dallas, Texas 75201
bcaldwell@caldwelcc.com
jcassady@caldwelcc.com
acurry@caldwelcc.com
wmccarty@caldwelcc.com

Federal Express & Email

Dated: January 7, 2017

Respectfully submitted,

/ Joseph A. Micallef /
Joseph A. Micallef
Registration No. 39,772
Attorney for Petitioner