UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Facebook, Inc.
Petitioner

v.

Windy City Innovations, LLC
Patent Owner

U.S. Patent No. 8,694,657

TITLE: REAL TIME COMMUNICATIONS SYSTEM

DECLARATION OF TAL LAVIAN, PH.D.

Table of Contents

Page

Page

Table of Contents
(continued)

Page

I, Tal Lavian, Ph.D., declare as follows:

I. INTRODUCTION AND QUALIFICATIONS

A. Summary of My Opinions

1. U.S. Patent No. 8,694,657 purports to describe a computerized technique for facilitating real-time communication between individuals using computers connected via the Internet. As I will explain below, the challenged claims do not recite any feature that would have been regarded as novel or non-obvious to a person of ordinary skill in the art. By April 1996 (the earliest priority date of the ’657 patent), real-time collaboration over computer networks was well-known, including video/audio conferencing, whiteboarding, and messaging. One of these references, U.S. Patent No. 6,608,636 to Robert D. Roseman, was filed more than four years before the earliest priority date for the ’657 patent. Roseman discloses a networked “virtual conferencing” system that discloses all of the supposedly inventive features of the ’657 patent. As I will explain below, all of the challenged claims would have been obvious based on the prior art.

B. Qualifications and Experience

2. I have more than 25 years of experience in the networking, telecommunications, Internet, and software fields. I received a Ph.D. in Computer Science from the University of California at Berkeley in 2006 and obtained a Master’s of Science (“M.Sc.”) degree in Electrical Engineering from Tel Aviv

University, Israel, in 1996. In 1987, I obtained a Bachelor of Science ("B.Sc.") in Mathematics and Computer Science, also from Tel Aviv University.

3. I am currently employed by the University of California at Berkeley and was appointed as a lecturer and Industry Fellow in the Center of Entrepreneurship and Technology ("CET") as part of UC Berkeley College of Engineering. I have been with the University of California at Berkeley since 2000 where I served as Berkeley Industry Fellow, Lecturer, Visiting Scientist, Ph.D. Candidate, and Nortel's Scientist Liaison, where some positions and projects were done concurrently, others sequentially.

4. I have more than 25 years of experience as a scientist, educator and technologist, and much of my experience relates to computer networking technologies. For eleven years from 1996 to 2007, I worked for Bay Networks and Nortel Networks. Bay Networks was in the business of making and selling computer network hardware and software. Nortel Networks acquired Bay Networks in 1998, and I continued to work at Nortel after the acquisition. Throughout my tenure at Bay and Nortel, I held positions including Principal Scientist, Principal Architect, Principal Engineer, Senior Software Engineer, and led the development and research involving a number of networking technologies. I led the efforts of Java technologies at Bay Networks and Nortel Networks. In

addition, during 1999-2001, I served as the President of the Silicon Valley Java User Group with over 800 active members from many companies in the Silicon Valley.

5. Prior to that, from 1994 to 1995, I worked as a software engineer and team leader for Aptel Communications, designing and developing mobile wireless devices and network software products. From 1990 to 1993, I worked as a software engineer and team leader at Scitex Ltd., where I developed system and network communications tools (mostly in C and C++).

6. I have extensive experience in communications technologies including routing and switching architectures and protocols, including Multi-Protocol Label Switching Networks, Layer 2 and Layer 3 Virtual Private Networks, and Pseudowire technologies. Much of my work for Nortel Networks (mentioned above) involved the research and development of these technologies. For example, I wrote software for Bay Networks and Nortel Networks switches and routers, developed network technologies for the Accelar 8600 family of switches and routers, the OPTera 3500 SONET switches, the OPTera 5000 DWDM family, and the Alteon L4-7 switching product family. I wrote software for Java based device management including software interface to the device

management and network management for the Accelar routing switch family network management system.

7. I am named as a co-inventor on more than 80 issued patents and I co-authored more than 25 scientific publications, journal articles, and peer-reviewed papers. Furthermore, I am a Senior Member of the Institute of Electrical and Electronics Engineers ("IEEE").

8. I currently serve as a Principal Scientist at my company Telecomm Net Consulting Inc., where I develop network communication technologies and provide research and consulting in advanced technologies, mainly in computer networking and Internet technologies. In addition, I serve as a Co-Founder and Chief Technology Officer (CTO) of VisuMenu, Inc., where I design and develop architecture of visual IVR technologies for smartphones and wireless mobile devices in the area of network communications.

9. Additional details of my background are set forth in my curriculum vitae, attached as **Exhibit A** to this Declaration, which provides a more complete description of my educational background and work experience. I am being compensated for the time I have spent on this matter at the rate of $400 per hour. My compensation does not depend in any way upon the outcome of this

proceeding. I hold no interest in the Petitioner (Facebook, Inc.) or the patent owner (Windy City Innovations, LLC).

C. Materials Considered

10. The analysis that I provide in this Declaration is based on my education and experience in the field of computer systems, as well as the documents I have considered including U.S. Patent No. 8,694,657 ("'657 patent") **[Ex. 1001]**, which states on its face that it issued from an application filed on September 20, 1999, which in turn claims priority to back to an earlier application filed on April 1, 1996. For purposes of this Declaration, I have assumed April 1996 as the relevant priority date.

11. I reviewed various documents dated prior to April 1996 describing the state of the art at the time of the alleged invention of the '657 patent. As explained below, some of these documents are relied upon as actually disclosing the limitations of the '657 patent, while others are being relied upon primarily for background purposes. The prior art documents that I rely upon in this Declaration as actually disclosing the limitations of the claims are:

Exhibit No.	Title of Document
1003	U.S. Patent No. 6,608,636 to Robert D. Roseman
1004	EP 0621532 A1 to Eugene Rissanen, published on April 13, 1994

Exhibit No.	Title of Document
1005	Ronald J. Vetter, *Videoconferencing on the Internet*, Computer, IEEE Computer Society, Vol. 28, No. 1, at pp. 77-79 (Jan. 1995)
1006	Excepts from Mary Ann Pike et al., *Using Mosaic* (1994)
1007	Excerpts from Tom Lichty, *The Official America Online for Macintosh Membership Kit & Tour Guide* (2d ed. 1994)

This Declaration also cites the following additional prior art documents for purposes of describing the relevant technology, including the relevant state of the art at the time of the alleged invention of the ’657 patent:

Exhibit No.	Title of Document
1008	Tim Berners-Lee et al., Request for Comments (RFC) 1738, Uniform Resource Locators (URL), Dec. 1994
1009	James Coates, *A Mailbox in Cyberspace Brings World to Your PC*, Chicago Tribune, Mar. 1995

II. PERSON OF ORDINARY SKILL IN THE ART

12. I understand that an assessment of claims of the ’657 patent should be undertaken from the perspective of a person of ordinary skill in the art as of the earliest claimed priority date, which I understand is April 1996.

13. In my opinion, a person of ordinary skill in the art as of April 1996 would possess 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. This could have included, for example, experience implementing systems for communicating over Local Area Networks (LANs) and Wide Area Networks (WANs), such as the Internet.

14. Although my qualifications and experience exceed those of the hypothetical person having ordinary skill in the art defined above, my analysis and opinions regarding the ’657 patent have been based on the perspective of a person of ordinary skill in the art as of April 1996.

III. CLAIM CONSTRUCTION

15. I have been informed by counsel that invalidity analysis is a two-step process. In the first step, the scope and meaning of a claim is determined by construing the terms of that claim. In the second step, the claim as interpreted is compared to the prior art. Thus, before I address the application of the prior art to the claims of the ’657 patent in **Part IV** below, I provide constructions for certain terms in those claims.

16. I have been informed by counsel that the ’657 patent expired on April 1, 2016. I have been informed by counsel that a claim in an expired patent subject to *inter partes* review must be construed by applying the claim construction principles outlined by the Federal Circuit’s decision in *Philips v. AWH Corp.*,

which is similar to the manner in which the scope of a claim is determined in litigation. I apply this standard in my analysis below.

A. "token"

17. Each independent claim recites a database that provides a "repository of tokens" used to perform user authentication. Claim 189, for example, recites a "database which serves as a repository of tokens for other programs to access." The written description accordingly describes a "token" as a piece of information associated with user identity. As explained in the specification:

> With regard to the arbitrating of the controller computer **3** is directed by the controller computer program **2** to <u>use "identity tokens", which are pieces of information associated with user identity</u>. 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.

('657, 7:49-54 (underlining added).) The specification goes on to describe several purposes for tokens, including "to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process" ('657, 7:60-61), "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" ('657, 8:2-4), 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." ('657, 8:7-9.)

18. Based on the definitional language in the written description, I have construed "**token**" as a "**piece of information associated with user identity**."

B. "pointer"

19. The term "pointer" appears in independent claims 189 and 465. "Pointers" are well-known in computer science and exist at all levels of computer system design – from the lower microprocessor levels to the higher levels where application programs execute. To persons of ordinary skill in the art, a "pointer" is simply a piece of information that "points to," or references, other information.

20. The written description provides only the following mention of pointers, which identifies a Uniform Resource Locator 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**.

('657, Ex. 1001, 5:11-16.) Based on this description, the term "pointer" should be construed as a "**piece of information that points to or references other information**."

IV. APPLICATION OF THE PRIOR ART TO THE CLAIMS OF THE ’657 PATENT

21. I have reviewed and analyzed the prior art references and materials listed in **Part I.C** above. In my opinion, each and every limitation of claims 189, 202, 203, 208, 209, 214, 215, 220, 221, 465, 476, 477, 481, 482, 486, 487, 491 and 492 is disclosed by the following references: (1) U.S. Patent No. 6,608,636 to Robert D. Roseman (“Roseman”) **[Ex. 1003]**; (2) EP 0621532 A1 to Eugene Rissanen, published on April 13, 1994 (“Rissanen”) **[Ex. 1004]**; (3) Ronald J. Vetter, *Videoconferencing on the Internet*, IEEE Computer, Vol. 28, No. 1, at pp. 77-79 (Jan. 1995) (“Vetter”) **[Ex. 1005]**; and (4) Mary Ann Pike et al., *Using Mosaic* (1994) (“Pike”) **[Ex. 1006]**.

22. As shown below, each limitation of the challenged claims is disclosed by the prior art discussed in this Declaration. In particular: (1) method claims 189, 202, 203, 208, 209, 214, 215, 220 and 221 are obvious over Roseman in view of Rissanen and Vetter, in further view of Pike (URLs). Most of my analysis will focus on independent claim 189 and selected dependent claims, to which I turn first below. The remaining claims discussed in this declaration, *i.e.*, claims 465, 476, 477, 481, 482, 486, 487, 491 and 492 are “apparatus” claims that recite substantially the same requirements as the method claims mentioned above, so in

the interests of brevity, I will refer back to my analysis of the method claims where appropriate.

23. I am informed that Roseman qualifies as prior art because it issued from an application filed on May 13, 1992, which is several years before the earliest application to which the ’657 patent can claim priority (April 1, 1996). I am also informed that Vetter, Rissanen, and Pike qualify as prior art because they were published more than one year before April 1, 1996.

24. Before explaining how the prior art applies to the claims, I will briefly summarize each piece of art and provide an overview of how I have applied it.

A. Brief Description and Summary of the Prior Art

1. Roseman [Ex. 1003]

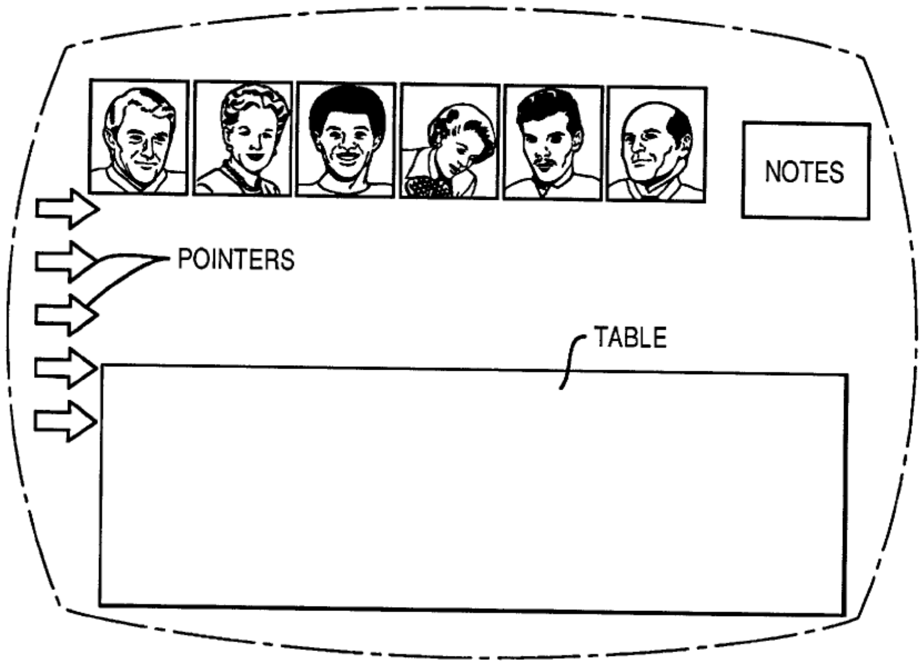
25. Roseman, entitled “Server Based Virtual Conferencing,” discloses a system for creating a virtual conference room that allows participants to collaborate in real time over a computer network. My Declaration cites Roseman for the majority of the limitations in the challenged claims, and relies on the other references (Vetter, Rissanen and Pike) only for a few limitations to the extent not disclosed in Roseman.

26. 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, 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.)

27. A user in Roseman creates a virtual conference room by clicking an appropriate icon, identifying the participants of the conference room and providing other information such as the rules that govern the conference. (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 Roseman virtual conference room is shown in Figure 9 below:

FIG. 9



(Roseman, Fig. 9.)

28. 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 my discussion of the claims below.

29. 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.").) "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.) These conference room "keys," as I will explain below, correspond to the "tokens" recited in the independent claims.

30. Roseman also discloses a database that stores the keys for the conference room. In particular, Roseman explains that "[t]he meeting room 'knows' about each key and its invitation level." (Roseman, 9:49-50.) The "meeting room," in turn, is stored on the host computer. (Roseman, 9:61-63 ("Meeting Facilitator (or Requestor) creates [sic] meeting room <u>on a host computer</u> which is accessible to all Invitees.") (underlining added), *see also id.* 12:16-18 ("The conference room itself is actually a combination of stored data and computer programs.").) More details about Roseman are set forth below.

2. Rissanen [Ex. 1004]

31. The challenged independent claims of the ’657 patent recite “**a database which serves as a repository of tokens for other programs to access**.” As I 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.

32. Rissanen, entitled “Password Verification System,” discloses a technique for user authentication using passwords stored in a database. My Declaration relies on 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 (“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.") (underlining added).) Rissanen also discloses that user login and password information may be stored in a database. (Rissanen, 2:22-29 ("In accordance with an embodiment of the preferred invention, a computer controlled database is linked to a telecommunication network with which users are provided password controlled access. 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.") (underlining added).) Although Rissanen also describes a technique for using spoken voice passwords, I have cited it for basic teachings relating to database storage of passwords of any form.

33. As I will explain in detail below, the user and password information in the database in Rissanen is analogous to the conference room "key" in Roseman. It would have been obvious to a person of ordinary skill in the art 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.

3. Vetter [Ex. 1005]

34. Certain independent claims of the ’657 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 disclose that those WANs include the Internet. (Roseman, Ex. 1003, 1:37-41, *see also id.* 3:14-19.)

35. Vetter, entitled “Videoconferencing on the Internet,” discloses software tools for enabling videoconferencing over the Internet. I have cited Vetter for the proposition that using the Internet to send information to meeting participant computers in Roseman would have been obvious to a person of ordinary skill in the art. Vetter discloses that “[v]ideoconferences are becoming increasingly frequent on the Internet,” and that “[r]eadily 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 easily than ever . . .” (Vetter, Ex. 1005, at p. 77.)

36. As I will explain below, the recitation of the “Internet” does not provide any non-obvious distinction over Roseman. Vetter confirms adding transmission over the Internet to Roseman would have been obvious to a person of

ordinary skill in the art, and a person of ordinary skill in the art would have had ample motivations to combine Roseman with Vetter.

4. Pike [Ex. 1006]

37. 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 1-2.) I have cited Pike in connection with claims that 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).

38. 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 (icon representing private message).) Roseman does not disclose the mechanics of how the pointer works, and does not expressly disclose a URL.

39. The specification of the '657 patent does not define the term "pointer" but identifies a URL as an example. ('657, 5:11-16.) For convenience and consistency, I have cited Pike for claims reciting a "URL," and in the event it is argued that "pointer" requires something akin to an Internet URL, for the

dependent claims that require a "pointer." As I will explain below, the "pointer" and "URL" limitations in the challenged claims would have been obvious in view Pike **[Ex. 1006]**.

40. URLs are used today to identify hundreds of millions of resources located on the Internet, and were clearly not an invention of the '657 patent. Pike, which was published in 1994, provides an introductory section describing basic Internet concepts such as URLs. (Pike, Ex. 1006, at 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.*) Pike goes onto describe the familiar URL syntax and how URLs identify documents that can be retrieved from other computers. (*Id.* at 38-39.) As I will demonstrate below, it would have been obvious to a person of ordinary skill in the art to adapt known URL techniques to Roseman.

5. Lichty [Ex. 1007]

41. Lichty, entitled *The Official America Online for Macintosh Membership Kit & Tour Guide* (2d ed. 1994), is a book describing aspects of the

service known as "America Online." Lichty describes "chat room" features, analogous to the virtual conference rooms of Roseman, that allowed users to send real-time messages to each other over a computer network. (Lichty, *e.g.*, pp. 252-278.) I cite Lichty in connection with claim limitations recited in each independent claim related to censoring data. Lichty describes a "chat room" functionality that allows individual users to "censor" other users in the chat room. For example, a user in a chat room can decide to "ignore" other users and thus no longer receive communications from them. (Lichty, pp. 269, 510 (definition of "Ignore").) As I explain below, it would have been obvious to a person of ordinary skill in the art to add this feature to the system of Roseman.

C. Each Limitation of Claims 189, 202, 203, 208, 209, 214, 215, 220, 221, 465, 476, 477, 481, 482, 486, 487, 491 and 492 Is Disclosed by the Prior Art

1. Claim 189

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

42. Roseman in view of Vetter discloses each aspect of the preamble of claim 189. Because of the length of the preamble, I will break up the claim

language into pieces to ensure that I cover all of the limitations the language potentially imposes.[1]

43. First, Roseman discloses "[**a**] **method of communicating . . . by using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access**," as recited in the first part of the preamble. Roseman discloses a virtual conferencing system in which users (*e.g.*, conference participants) communicate 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.)

---

[1] I am informed by counsel that a claim preamble does not always impose a limitation on the claim. It is unnecessary for me to determine whether the preamble is limiting because the prior art nevertheless discloses it.

Further details on how Roseman discloses communication among users is set forth in the discussion of later claim limitations.

44. The preamble of claim 189 continues by reciting that the computer system "**including 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 networked server computer, which Roseman calls the "host computer" or "host":

> These individual [participant] systems are located at different geographic locations, and, when a virtual conference is to be held, <u>become connected to a central, host, computer (or multiplicity of host computers)</u> 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.").)

45. 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).)

46. The passages above show that the "**keys**" in Roseman qualify as "**tokens**" because keys are pieces of information associated with a user identity,

that control whether a user has permission to enter a conference room. Roseman confirms that a key is a "piece of information" by stating that "the 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.").)

47. Roseman also confirms that a "key" is associated with a 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 or not 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. <u>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</u>.") (underlining added).) The "keys" therefore qualify as "**tokens**."

48. 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 <u>on a host computer</u> 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).)

49. 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” because the host computer stores the keys issued to invitees that control access to the room.

50. 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. In my opinion, this does not provide any distinction between Roseman and the claim. A person of ordinary skill in the art would have understood the claimed “database” in this context to simply refer to a stored collection of tokens. The ’657 patent does not provide any detail about the claimed “database” except stating that the tokens “are stored in memory in a control computer database, along with personal information about the user, such as the user’s age.” (’657, 7:52-54.) The patent does not specify any details regarding

the storage of tokens in a database and does require that the database be any particular type, such as relational.

51. In any event, even if one were to argue that Roseman does not sufficiently disclose the claimed "database which serves as a repository of tokens," the addition of a database to Roseman would have been trivially obvious to a person of ordinary skill in the art. Database technologies predated the '657 patent by decades, and it was known to use databases to store user identity and authentication information ("tokens"). 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, at 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, 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).)

52. ***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. A skilled artisan would understand that the user identity and password information in Rissanen is analogous to the "keys" in Roseman, and would be motivated to make this combination. In fact, a person of ordinary skill in the art reading Roseman would have found it plainly apparent that the host computer would store and maintain a copy of the keys issued to invitees in order to verify the stored key against a key provided by a user seeking access. A person of ordinary skill in the art would have understood that the key verification step in Roseman might not function properly if the host computer could not store and retrieve previously-issued key information to determine validity when a user presents a key seeking access to a conference room. (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.

53. In short, a person of ordinary skill in the art would have found nothing inventive or non-obvious about the idea of storing "keys" in database. As noted previously, Rissanen goes on to describe a more advanced technique for storing and recognizing spoken (voice) passwords, but these additional details would not have discouraged my proposed combination. I have relied upon Rissanen for its basic disclosures relating to the ability to store "tokens" in a database, and as such, it does not matter if the passwords are text, audio, or some other media. A person of ordinary skill in the art would have found the basic teachings relating to the storage of user information and passwords applicable to any system that requires user authentication as a prerequisite to access, such as Roseman.

54. Roseman also 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 <u>a combination of stored data and</u>

<u>computer programs</u>." (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.

55. 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.

56. The preamble of claim 189 recites, "**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 my discussion of element 189**[a]**, below.

57. The preamble of claim 189 recites, "**thereby affording information to each of a <u>plurality of participator computers</u> which are otherwise independent of each other**." Each meeting participant in Roseman has a participator computer, which Roseman calls a "local computer." (Roseman, 1:34-37 ("Two (or more) parties each operate their own local computers. The computers have associated video cameras, speaker-type telephones, and pointing devices (such as 'mouses')."); *id.*, 2:64-65 ("Every office is equipped with the following equipment: a computer (termed a 'local computer' herein) . . . .").) The participants' local computers can run conventional operating systems and environments such as Microsoft Windows. (Roseman, 12:1-8.)

58. Each local computer in Roseman is "**otherwise independent of each other**" because the 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 I explain below, to adapt Roseman to the Internet such that the Internet is the only network shared by the individual local computers.

59. The participator computers in Roseman are therefore "otherwise independent of each other," as recited in the preamble.

60. The preamble also recites a "method of communicating **via an 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 an example of a Wide Area Network (WAN), but Roseman does not expressly mention the Internet.

61. Nevertheless, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill. 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).)

62. 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 sending information to participator computers via the Internet network.

63. ***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 virtual conferencing system of Roseman in which the host (server) and participant computers communicate via the Internet. Vetter provides an express motivation for this combination by confirming that "[v]ideoconferences are becoming increasingly frequent on the Internet" (*id.* at 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 one of the largest networks for connecting remote computers (if not the largest), making it the obvious Wide Area Network (WAN) for use with Roseman to connect the host and participant computers.

64. Vetter also discloses that the increasing popularity of videoconferencing was fueled by the fact that, as of January 1995, "[t]he

price/performance" of hardware devices had finally reached a level in which widespread deployment was possible. (*Id.*) A person of ordinary skill in the art would have understood that the ratio of price-to-performance would have continued to improve, making videoconferencing even more attractive in April 1996 than it was in January 1995 when Vetter was published.

65. 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, but none of those issues would have discouraged my proposed combination. Vetter describes issues such as maintaining software and hardware configurations, coordinating when individuals at a site should speak, audio feedback caused by participants leaving their microphones open, delays in whiteboard performance, and network performance of video streams. (*Id.* at p. 78-79.) None of these issues would have discouraged my proposed combination. Most of the problems identified by Vetter are directly attributable to using Internet videoconferencing in a very unique classroom context. Vetter even acknowledges that "these tools may not have been designed for such an environment, but my goal is to point out important issues in distance-learning video/audio applications." (*Id.* at p. 78 (top of page).) Vetter nevertheless ends on a decidedly positive note by confirming that

"video and audio conferencing are an increasingly important way of carrying out collaborative group work." (*Id.* at p. 79 (right column).)

66. A person of ordinary skill in the art would have understood that the videoconferencing system of Roseman involves a simpler conferencing setup with a smaller number of participants, which could avoid or at least reduce the severity of all of the issues encountered by Vetter. A person of ordinary skill in the art would also have understood that network performance in a real-time conferencing application depends on a multiplicity of different factors including the speed of the connections, the number of participants, the amount and type of information being sent, and many other factors. A person of ordinary skill in the art would have understood that performance considerations are a fact-of-life in any conferencing system (including to this day), and as such, the network performance issues identified by Vetter would not have discouraged a skilled artisan from using the Internet to support the type of conferencing functions disclosed in Roseman. In my opinion, therefore, Roseman and Vetter disclose and render obvious this claim limitation.

67. Having addressed the preamble of claim 189, I will now turn to the remaining limitations of claim 189.

b. "affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity" (Claim 189[a])

68. Roseman discloses authenticating at least "**a first user identity**" and "**a second user identity**" as recited in this claim limitation and in the following claim limitation. Roseman discloses that a conference may have multiple invitees. (*See* Roseman, Fig. 9 (showing conference having six participants).) Each invited 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. <u>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</u>. The other users in the room are alerted to a new presence and receive any relevant information.

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

69. Roseman confirms that this validation and authorization process involves authenticating a "**user identity**." For example, 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, as confirmed by the permissions that prohibit sharing or assignment of the key. "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.) Roseman therefore discloses "authenticating a first user identity" as recited in claim 1

70. 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 a single invitee, it would have been obvious to a person of ordinary skill that the same procedure would be invoked for multiple invitees. 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.)

71. A person of ordinary skill in the art would have found it obvious that the process of entering a conference room would be repeated for all invitees who received a key.

72. 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 [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, 11:10-17.) 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 conference 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").)

73. Roseman discloses several other ways of sending ("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. The parties can communicate, until they terminate whisper mode." (Roseman, 9:22-25.)
- 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.)

74. The types of information described above are communicated ("afforded") responsive to the participant being authenticated because the participant would otherwise not be able to receive such information.

75. 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 conversions 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 participant. For example, if the first participant was not party to a private conversation or note between two other participants, the first participant's computer would receive only "some" (but not all) of the information available in the virtual conference/meeting room.

76. Finally, this claim limitation recites "affording some of the information to a first of the participator computers **via the Internet network**." As discussed above for the preamble of claim 189, 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 an example of a Wide Area Network (WAN), but Roseman does not expressly mention the Internet.

77. Nevertheless, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill by combining the teaching of Vetter with Roseman. As discussed previously, 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).

c. "affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity" (Claim 189[b])

78. 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 189**[a]** would apply to the participator computer of any other conference/meeting participant. The system of Roseman could therefore send "some of the information to a second of the participator computers via the Internet network," for the same reasons as above.

d. "determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications" (claim 189[c])

79. Roseman discloses determining whether the first and second authenticated users are able to form a group to send and receive real-time communications.

80. In Roseman, the host uses “keys” to determine whether a user can form a group conference in a conference room: “The meeting room ‘knows’ about each key and its initiation level. Persons with improper keys are not admitted to the room.” (Roseman, 9:49-51). To enter a conference room, the user “drops the key onto the door lock” and if “the key is valid and the user has the authority to use the key,” the “user is admitted to the room.” (Roseman, 10:61-64). The conference room may have other users, who “are alerted to a new presence and receive any relevant information.” (Roseman, 10:64-65).

81. Roseman also describes the formation of “committee” or “child rooms.” (Roseman, 10:18-23). The child room “is created in the same way as the parent room” and may have unique “door locks.” (Roseman, 10:19-20). A user can not join the group in a child room if that user cannot enter the parent room. (Roseman, 10:22-23).

82. Roseman further describes a group formed by two participants “whispering” to one another. (Roseman, 9:16-17). The “whisper mode” forms a group “audio connection between the two whispering parties, and between nobody else” where the two whispering parties can communicate. (Roseman, 9:22-25). Roseman also discloses the passing of a private note between a group of two users. (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 a group of two participants of the conference that is not shared with other participants.

83. The final aspect of this claim limitation requires that the group is formed "to send and to receive **real-time communications**." Roseman discloses that real-time messages are communicated within the group by placing documents on the table and moving 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.)

84. 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).) This further confirms that the messages exchanged during a conference are "real-time messages," as recited in the claim.

e. "determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the user identity has been determined by an other of the user identities" (claim 189[d])

85. Because of the length of this claim limitation, I will address portions of the language to ensure that I cover all of its limitations.

86. I start with the phrase, "**the data presenting at least one of a pointer, video, audio, a graphic, and multimedia**," which is disclosed by Roseman. While this claim language requires only "at least one" of the enumerated types of data, as I discuss below, Roseman discloses all five recited types of data.

87. **Pointer:** As I explained previously, the term "pointer" refers to a piece of information that points to, or references, other information. 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 invoked, the host computer causes the content to appear on the tables of each conference participant.

88. 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 square icon similarly serves as a pointer because it points to, or references, the underlying note content, and retrieves and produces the content on demand from the host computer.

89. The specification of the '657 patent does not define "pointer" but uses a Uniform Resource Locator (URL) as an example of a pointer. ('657, 5:11-16.) In my opinion, 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]**.

90. Pike is a textbook describing the NCSA Mosaic web browser. (Pike, at 1-2.) Pike provides an introductory section describing several basic and familiar Internet concepts, such as hypertext links and 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.

91. 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. As explained previously for the preamble of claim 189, Vetter expressly 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. Pike further confirms that by

its publication in 1994, "the Internet has exploded on the computer scene as a topic of national interest." (Pike, Ex. 1006, at 1.)

92. It would have required no leap of inventiveness for a person of ordinary skill in the art to use the ubiquitous Internet URL to identify content stored on the host computer of Roseman which, upon activation, would retrieve the requested content and transmit it to meeting participant computers over the Internet. 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* 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.

93. Moreover, it was well-known to send messages containing Internet URLs. Pike describes a technique for allowing a user to send URLs for interesting Internet resources in email messages to other people. (Pike, at p. 121.) This capability was well-known because, in part, it was one of the original design goals of the URL. As explained in Request for Comments 1738 by Tim Berners-Lee (December 1994), the famous standard that defined the syntax of URLs, "there are

many occasions when URLs are included in other kinds of text; examples include electronic mail, USENET news messages, or printed on paper." (RFC 1738, Ex. 1008, at p. 22.) RFC 1738 describes techniques for embedding URLs into textual messages so they can be easily used. (*Id.*) By March 1995, URLs were being regularly distributed by businesses, government agencies, academic institutions, and individuals. (Ex. 1009.)

94. By April 1996, therefore, a person of ordinary skill in the art would have found nothing non-obvious about adapting Roseman to send a message containing an Internet URL to meeting participants. Roseman specifically discloses that a document placed on the table of the conference room can include "text" (8:2) and thus, a person of ordinary skill in the art would have understood that such a document could have contained an Internet URL. In my opinion, therefore, the "pointer" limitations in these claims do not provide any meaningful distinction over the prior art.

95. **<u>Audio and Video</u>**: As explained in Roseman: "When a user enters a room with other occupants, the data connection is made. <u>Audio and video connections are made</u> 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.) When the meeting begins, the host can send each participant a picture of each invitee as captured by the local computer's camera. (See Roseman, 7:35-38 ("The pictures of the invitees can be the actual images seen by the each invitee's close-up camera . . . .").)

96. **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).) The meeting organizer can specify the décor for the virtual conference room, including "[w]hat paintings are on the walls" (Roseman, 3:40-41.)

97. **Multimedia**: The '657 patent does not define the word "multimedia," but in ordinary parlance, it simply refers to content that combines different types of

media (such as graphics, text, video, audio, etc.). The patent describes a web page displayed in a browser window with graphics and text (Fig. 26) as an example of a "graphical multimedia message." ('657, 3:32-34; *see also id*., 10:41-43 ("Inside the Navigator window, the graphical multimedia content, the home page of AIS, is shown.").)

98. 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.").)

99. Roseman therefore discloses "data presenting at least one of a pointer, video, audio, a graphic, and multimedia."

100. I now address the limitation "**determining whether the first user identity is individually censored from sending data in the communications** . . . **by determining whether a respective at least one parameter corresponding to the user identity has been determined by an other of the user identities.**" This is disclosed in Roseman by the Whisper Mode feature of the virtual conference. Roseman explains that, to activate Whisper Mode, "one party can click onto the picture of another." (Roseman, 9:17-18.) This action signals to the host computer that a conference participant ("**an other of the user identities**") has determined to exclude other conference participants ("**the user identity**") from his or her private communication link. Roseman confirms that the host computer is capable of determining changes in user properties as a result of a selection to initiate private communication:

> [O]ne party can click onto the picture of another. The picture becomes grayed, or otherwise different from the others, as shown in FIG. 13. In addition, a prominent message is displayed on both parties' displays,

such as "Whisper Mode is Active."

(Roseman, 9:17-21.) Roseman therefore discloses "determining whether a respective at least one parameter corresponding to the user identity has been determined by an other of the user identities."

101. After a click to initiate Whisper Mode is detected, "the host makes an audio connection between the two whispering parties, and between nobody else." (Roseman, 9:16-23 (underlining added).) The host computer determines, therefore, that each other user identity in the virtual conference is not one of the whispering parties, and thus each of the other user identities is individually censored from sending audio data using the exclusive communication link between the two whispering parties. (Roseman, 9:16, 15:8-9 ("HOST PROVIDES EXCLUSIVE VOICE LINK BETWEEN THE TWO PARTICIPANTS") (capital letters in original).)

102. While Roseman discloses this limitation, it would also have been obvious to a person of ordinary skill in the art in view of Lichty. Lichty describes "chat room" services provided by America Online that are closely analogous to the virtual conference room features of Roseman. (Lichty, *e.g.*, pp. 252-278.) Like Roseman, a "chat room" provides a forum for multiple participants to communicate in real-time with each other over a computer network. (*Id.*)

103. Lichty provides a method for screening out ("censoring") certain messages from being sent by a chat room participant to another participant. Lichty explains that a first member ("**an other of the user identities**") can determine to ignore a second member ("**the user identity**"):

> If you wish to exclude a member's comments (or those of all members in the conversation in which you're not interested), select the member's name in the People in this Room window and click the Ignore button. From then on, that member's text will not appear on your screen.

(Lichty, pp. 269.) One of ordinary skill in the art would have understood that the chat system is capable of recognizing when the user properties of the second participant has changed as a result of being ignored by the first member, and would accordingly prevent the second member from sending further comments to the first member.

104. ***Rationale and Motivation to Combine***: It would have been obvious to a person of ordinary skill in the art to adapt Roseman to provide the features of Lichty described above, predictably resulting in the virtual conference system of Roseman in which participants can be "censored" from sending audio data. This feature would allow a meeting participant in Roseman, for example, to block audio communications from identified individuals.

105. As stated above, Lichty and Roseman are analogous references in the same field of providing real-time communication to groups of computer users connected to a network. In fact, the analogous nature of these references is confirmed by the fact that they use "censorship" features to address the same challenges with real-time communications. Lichty explains that its censorship feature "is most useful when the chat of another member becomes disruptive in the chat room." (*Id.* at 510 (definition of "Ignore").) Lichty calls this feature as "a real boon when chats get busy" (Lichty, p. 269), thus providing a further express motivation to combine.

106. Roseman identifies a similar problem by acknowledging that, like Lichty, one participant may attempt to disrupt or dominate a conference by talking excessively, and thus, may need have his or her communications blocked. (Roseman, 12:29-45.) Roseman also notes that a meeting participant's interest in another participant's communications may vary. (Roseman, 11:46-47 ("An 'Interest Meter' might show the interest level of the listeners to a speaker.").) A person of ordinary skill in the art, therefore, would have recognized that the two references address the common problem of how to deal with potentially unwanted communications from conference participants. A person of ordinary skill in the art

would have recognized that Lichty's solution to that problem would have been fully applicable to the system of Roseman.

107. A person of ordinary skill in the art would have found the features of Lichty to be a natural addition to the other virtual conferencing features of Roseman. A person of ordinary skill in the art, therefore, would have been amply motivated to add Lichty's censorship feature to Roseman.

108. Now to the next limitation.

f. "if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer" (claim 189[e])

109. Given the length of this claim limitation, I break my discussion up into several parts. First, the claim limitation recites **"if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator computer.**"

110. The discussion of Claim 189[c] illustrates several ways that Roseman discloses the formation of groups and facilitating the sending of communications that are not censored. Examples of sending communications that are not censored within the groups that are formed include conference rooms that are controlled by keys, "committee" or "child rooms" of parent conference rooms, and communications between two individuals in "Whisper Mode" or by the passage of passed notes.

111. As discussed above for claim 189[d], Roseman in view of Lichty discloses several ways communications may be censored, including a Whisper Mode and an Ignore feature.

112. The next part of this limitation recites "**wherein the sending is in real time and via the Internet network**." As discussed above for claim 189[c], Roseman describes several methods by which real-time messages are communicated with the group that is formed. For instance, Roseman discloses that real-time messages are communicated within the group by placing documents on the table and moving the electronic pencil, among others. Roseman confirms that these messages are communicated in real-time because the messages are communicated to participants as the underlying events occur:

> 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.)

113. This part of the limitation also requires that the sending is "**via the Internet network**." As discussed above in the discussion of the preamble of claim 189, 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 an example of a Wide Area Network (WAN), but Roseman does not expressly mention the Internet. As discussed above, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill by combining the teaching of Vetter with Roseman. As discussed previously, 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).

114. The final part of this limitation recites "**and wherein the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer.**" In the '657 patent, Internet URLs are described an example of a "pointer" to information. ('657, 5:11-16).

115. As noted above, the icon in Roseman, when invoked by the second participant computer, causes the second computer to fetch and receive the underlying content. Pike confirms that the pointer could be a URL, which could be used to download the document content from the host computer over the Internet in real-time when the URL is invoked. In fact, this limitation is little more than a recitation of basic Internet URL functionality. (Pike, at p. 43 ("When you view a document on the WWW, you are actually retrieving it from somewhere on the Internet. When you do this, you are making demands on the Internet host that is providing the information, and also on the network itself.").)

116. While Roseman does not expressly discuss internet URLs, Roseman's discussion of pointers would render these claims obvious in view of the teachings of Pike **[Ex. 1006]**.

g. "if the user identity is censored from sending of the data, not allowing sending the data that is censored from the first participator computer to the second participator computer." (claim 189[f])

117. As explained previously in claim 189[d], when a user is censored from sending data, such as when the host computer determines when to censor content sent by participants by acting as a conference "moderator" and regulating when and/or how long participants can speak during the conference, that user is not allowed to send data from the first participator computer to the second participator computer.

2. Claim 202 (first user identity is censored from the sending of data presenting the video)

118. Claim 202 is dependent on claim 189, reciting "wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video." Roseman discloses this limitation.

119. As explained previously in claim 189[d], Roseman discloses all five types of data recited in claim 189, including video data: "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.) When the meeting begins, the host can send each participant a picture of each invitee as captured by the local computer's camera. (See Roseman, 7:35-38 ("The pictures of the invitees can be the actual images seen by the each invitee's close-up camera . . . .").)

120. Moreover, as explained previously in claim 189[d], the "Whisper Mode" in Roseman discloses "determining whether the first user identity is censored . . . from the sending of the data." In addition, Roseman in view of Lichty discloses this same limitation with Lichty's screening out ("censoring") of certain messages from being sent by a chat room participant to another participant. As explained for claim 189[d], it would have been obvious to a person of ordinary skill in the art to adapt Roseman to provide the features of Lichty described above,

predictably resulting in the virtual conference system of Roseman in which participants can be "censored" from sending data.

3. Claim 203 (two client software alternatives)

121. Claim 203 is dependent on claim 202, reciting "wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications." Roseman discloses this limitation.

122. Starting with the claim language "**wherein the computer system provides access via any of two client software alternatives**," Roseman discloses that the host computer is programmed to be accessible to a local computer via the conferencing software running on the local computer. Roseman confirms that the conferencing software can run on multiple computing platforms, thus disclosing "**two client software alternatives**," as claimed. For example, Roseman explains that "the local computers are utilizing Windows®, or an equivalent. 'Windows®' refers to an operating system, or 'environment,' which is publically available from Microsoft Corporation . . ." (Roseman, 12:1-5.) But Roseman also emphasizes that "the invention is not limited to systems utilizing these particular

environments," and that the graphical user interface features in Roseman "are within the skill of the art." (Roseman, 12:9-10.) Roseman therefore discloses that the local computer software could be provided for multiple computing platforms, thus disclosing at least "two client software alternatives" for accessing the host computer. It was well-known that providing a software product for multiple computing platforms (*e.g.*, Windows, Macintosh, etc.) was desirable because it makes the software more commercially attractive and increases the number of users who can use it.

123. A second alternative way of looking at this limitation is that the conferencing software on a particular local computer provides at least "**two client software alternatives**," which are represented by the at least two features that are available through the local computer software. One of these features, known as "Whisper Mode," allows a participant at a local computer (through the user interface) to initiate a private voice communication with another meeting participant. A second feature allows a participant at a local computer to create "committee" or child rooms within a virtual conference room. These features provide at least "**two client software alternatives**" because they involve two distinct software functionalities on the local computer, both of which provide access to the host computer in Roseman.

124. With respect to the whisper mode feature, Roseman explains that "one party can click onto the picture of another. The picture becomes grayed, or otherwise different from the others, as shown in FIG. 13. In addition, a prominent message is displayed on both parties' displays, such as 'Whisper Mode is Active.'" (Roseman, 9:16-21.) "At this time, the host makes an audio connection between the two whispering parties, and between nobody else." (Roseman, 9:22-23.) The whisper mode feature provides a "**client software alternative**" because it provides software functionality that may be chosen at the local computer ("client software alternative"), that provides access to the host ("controller computer system") in order to establish the audio connection.

125. The "child room" functionality in Roseman provides a second example of a "client software alternative." Roseman explains that the host computer is programmed to provide a child conference room to users if a participant at his or her local computer "drags his icon and other icons through the doorway into other conference room." (Roseman, 15:55-67 & Fig. 21B.) "Each child-room is created in the same way as the parent room." (Roseman, 10:19-20.)

126. Roseman also discloses pseudo-code that describes how the host computer and local computers carry out the Whisper Mode and child-room features discussed above. (Roseman, 12:66-67 ("Pseudo-code usable for programming the

host and the local computers in contained in the Appendix"), 15:6-9 & Fig. 17B (Whisper Mode), 15:55-67 & Fig. 21B (child-room feature).) These features therefore disclose the claimed "two software alternatives."

127. The remaining claim language "wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications" is also disclosed by Roseman.

128. For the first portion of this claim limitation, "**wherein both of the client software alternatives allow respective user identities to be recognized**," both Whisper Mode software and child-room software allow respective user identities to be recognized by the host computer. In particular, as explained above, to enable Whisper Mode, "<u>the host makes an audio connection between the two whispering parties</u>, and between nobody else," thus confirming that the host ("controller computer") recognizes the respective user identities of the whispering parties. (Roseman, 9:22-23 (underlining added).) As to the child-room software, Roseman explains that the host provides a child conference room for "dragged in participants," thereby recognizing user identities of the participants in the child

conference room. Both of these software alternatives, therefore, "allow the respective user identities to be recognized."

129. The next portion of the claim recites that the two client software alternatives "**allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.**" The videoconferencing software on the local computers allows users to create a group of two or more users who can send and receive communications. For example, a user of a local computer that activates the Whisper Mode software creates a two member group by selecting a particular party with whom to communicate. (Roseman, 9:16-25, 15:6-9 & Fig. 17B.) As to the child-room software, a user of a local computer who drags in other participants forms a group comprising those users. (Roseman, 10:18-23, 15:55-67 & Fig. 21B.)

4. Claim 208 (first user identity is censored from the sending of data presenting the audio)

130. Claim 208 is dependent on claim 189, reciting "wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the audio." Roseman discloses this limitation.

131. As explained above, Roseman discloses all five types of data recited in claim 189, including audio data: "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.)

132. Moreover, as explained previously in claim 189[d], the "Whisper Mode" in Roseman discloses "determining whether the first user identity is censored . . . from the sending of the data." In addition, Roseman in view of Lichty discloses this same limitation with Lichty's screening out ("censoring") of certain messages from being sent by a chat room participant to another participant. As explained for claim 189[d], it would have been obvious to a person of ordinary skill in the art to adapt Roseman to provide the features of Lichty described above, predictably resulting in the virtual conference system of Roseman in which participants can be "censored" from sending data.

5. Claim 209 (two client software alternatives)

133. Dependent claim 209 recites the identical limitation as dependent claim 203.

203. The method of claim 202, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.	209. The method of claim 208, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

134. My analysis of claim 203 applies with full force here.

6. Claim 214 (first user identity is censored from the sending of data presenting the graphic)

135. Claim 214 is dependent on claim 189, reciting "wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the graphic." Roseman discloses this limitation.

136. As explained above for claim 189[d], Roseman discloses all five types of data recited in claim 189, including graphic data. 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).) The meeting organizer can specify the décor for the virtual conference room, including "[w]hat paintings are on the walls" (Roseman, 3:40-41.)

137. Moreover, as explained previously in claim 189[d], the "Whisper Mode" in Roseman discloses "determining whether the first user identity is censored . . . from the sending of the data." In addition, Roseman in view of Lichty discloses this same limitation with Lichty's screening out ("censoring") of certain messages from being sent by a chat room participant to another participant. As explained for claim 189[d], it would have been obvious to a person of ordinary skill in the art to adapt Roseman to provide the features of Lichty described above, predictably resulting in the virtual conference system of Roseman in which participants can be "censored" from sending data.

7. Claim 215 (two client software alternatives)

138. Dependent claim 215 recites the identical limitation as dependent claim 203.

203. The method of claim 202, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.	215. The method of claim 214, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

139. My analysis of claim 203 applies with full force here.

8. Claim 220 (first user identity is censored from the sending of data presenting the multimedia)

140. Claim 220 is dependent on claim 189, reciting "wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the multimedia." Roseman discloses this limitation

141. As explained above for claim 189[d], Roseman discloses all five types of data recited in claim 189, including multimedia data. 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.").)

142. Moreover, as explained previously in claim 189[d], the "Whisper Mode" in Roseman discloses "determining whether the first user identity is censored . . . from the sending of the data." In addition, Roseman in view of

Lichty discloses this same limitation with Lichty's screening out ("censoring") of certain messages from being sent by a chat room participant to another participant. As explained for claim 189[d], it would have been obvious to a person of ordinary skill in the art to adapt Roseman to provide the features of Lichty described above, predictably resulting in the virtual conference system of Roseman in which participants can be "censored" from sending data.

9. Claim 221 (two client software alternatives)

143. Dependent claim 220 recites the identical limitation as dependent claim 203.

203. The method of claim 202, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.	221. The method of claim 220, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

144. My analysis of claim 203 applies with full force here.

10. Claim 465 (Apparatus Corresponding to Claim 189)

145. Claim 465 recites an apparatus with substantially similar limitations as claim 189. I have provided a side-by-side comparison below which shows that all of the limitations of claim 465 are recited, using substantially similar language, as claim 189 (underlining showing overlap of language):

Method Claim 189	Apparatus Claim 465
189. A method of communicating via an Internet network by using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method including:	[p1] 465 An Internet network communications system, the system including: a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other,
[a] affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	[p2] the computer system in communication with a first of the participator computers responsive to a first authenticated user identity
[b] affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity; and	[p3] and with a second of the participator computers responsive to a second authenticated user identity, wherein the computer system

Method Claim 189	**Apparatus Claim 465**
[c] determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications; and	[a] determines whether the first user identity and the second of the user identity are able to form a group to send and to receive real-time communications; and
[d] determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and	[b] determines whether the first user identity, is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and
[e] if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein, for the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer, and	[c] if the user identities are determined to be able to form the group, forms the group and facilitates sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer; and

Method Claim 189	**Apparatus Claim 465**
[f] if the first user identity is censored from the sending of the data, not allowing sending the data that is censored from the first participator computer to the second participator computer.	[d] if the first user identity is censored from sending the data, does not facilitate sending the data that is censored from the first participator computer to the second participator computer.

146. As shown above, other than the fact that claim 465 does not recite the two "affording" limitations of claims 189**[a]** and **[b]**, the differences between claim 189 and 465 consist largely of insubstantial verb tense differences based on the fact that claim 189 is a method and claim 465 an apparatus claim. As I explained in connection with claim 189 above, this claim is obvious over Roseman in view of Rissanen, Vetter, Pike and Lichty. 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 465 for the same reasons as claim 189.

11. Claims 476, 481, 486, and 491 (the data presents the video, audio, graphic and multimedia)

147. These claims depend from claim 465 discussed above and each specifically recites presenting one of the five types of data recited in claim 189[d] and claim 465[b]: video, audio, graphic, or multimedia.

Method Claim Limitation 189[d]	**Dependent Claims**
189[d] determining whether the first user identity is individually censored from sending data in the communications, the **data presenting** at least one of a pointer, **video**, **audio**, a **graphic**, and **multimedia** by determining whether a respective at least one parameter corresponding to the user identity has been determined by an other of the user identities	476. The system of claim 465, wherein **data presents** the **video**.
	481. The system of claim 465, wherein the **data presents** the **audio**.
	486. The system of claim 465, wherein the **data presents** the **graphic**.
	491. The system of claim 465, wherein the **data presents** the **multimedia**.

Apparatus Claim Limitation 465[b]	**Dependent Claims**
465[b] determines whether the first user identity, is individually censored from sending data in the communications, the **data presenting** at least one of a pointer, **video**, **audio**, a **graphic**, and **multimedia** by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and	476. The system of claim 465, wherein **data presents** the **video**.
	481. The system of claim 465, wherein the **data presents** the **audio**.
	486. The system of claim 465, wherein the **data presents** the **graphic**.
	491. The system of claim 465, wherein the **data presents** the **multimedia**.

148. As explained in detail above for claim 189[d] and 465[b], Roseman discloses presenting all five types of data recited in the claim, including video, audio, graphic and multimedia. My analysis of claims 189 and 465 applies with full force here.

149. To the extent it is argued that claims 476, 481, 486, and 491 require determining whether the first user identity is individually censored from sending the type of data recited in each claim, my analysis of claims 202, 208, 214, and 220, respectively, applies with full force to these claims.

202. The method of claim 189, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of <u>the data presenting the video</u>.	476. The system of claim 465, wherein <u>data presents the video</u>.
208. The method of claim 189, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of <u>the data presenting the audio</u>.	481. The system of claim 465, wherein <u>the data presents the audio</u>.
214. The method of claim 189, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of <u>the data presenting the graphic</u>.	486. The system of claim 465, wherein <u>the data presents the graphic</u>.
220. The method of claim 189, wherein	491. The system of claim 465, wherein

the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the multimedia.	the data presents the multimedia.

12. Claims 477, 482, 487 and 492 (two client software alternatives)

150. These claims respectively depend from claims 476, 481, 486 and 491. Each of claims 477, 482, 487 and 492 recites the same limitation: "wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications." As explained in detail above for claim 203, Roseman discloses this limitation and my analysis of claim 203 applies with full force here.

151. Finally, in my opinion, the disclosures of Roseman, Rissanen, Vetter and Pike provide sufficiently detailed disclosures to enable a person of ordinary skill in the art to make the combinations explained above without undue experimentation. The references themselves make clear that the technologies involved were well known to persons of ordinary skill in the art and even commercially available. For example, as noted above, I rely on Roseman for the

majority of the limitations in the challenged claims. Roseman specifically identifies "[c]ommercially [a]vailable [e]quipment for use in invention," including screen sharing software, electronic mail software, video conferencing products, computer-controlled telephones, graphics devices and other equipment. (Roseman, 12:46-65.) Although I understand that the disclosures in an issued U.S. patent (such as Roseman) are presumed enabling, in my opinion, Roseman provides sufficient detail to build the virtual conference room it discloses.

152. I also rely upon Vetter, Rissanen and Pike for trivial concepts that were well known to persons of ordinary skill in the art by April 1996 (to the extent not already disclosed in Roseman). Rissanen, which I refer to for its teachings regarding using a database to store tokens, explains that the system can use "a general purpose IBM computer" (Rissanen, 4:32-35) and that the database can be "any one of well known disk, tape, solid state or other type of storage device" (Rissanen, 5:9-10). More generally, by April 1996, commercially-available, off-the-shelf databases such as Oracle, Sybase and Berkeley DB were in wide use, and information regarding their setup and operation widely available, such that persons of ordinary skill in the art would have been capable of using one to store tokens for other programs to access without undue experimentation. Similarly, Vetter explains that "<u>[r]eadily available software tools</u> enable real-time audio and video

channels as well as shared whiteboards that allow groups to collaborate on distributed group work" and specifically identifies a number of "available conferencing tools," including Collage, CU-SeeMe, CU-SeeMe Reflector, IVS, MBone, Nevot (Network Voice Terminal), NV (Net Video), SD (Session Director), VAT (Visual Audio Tool) and WB (Whiteboard). (Vetter, Ex. 1005, at p. 77, 78.) More generally, the Internet has been widely used since at least the 1980s. (Pike, Ex. 1006, at 8-10.) Operating systems such as UNIX, which were widely distributed long before April 1996, enabled computers to communicate via the Internet (such software libraries for creating UDP and TCP socket connections). Finally, as to the straightforward concept of URLs, the use of URLs in network-based communications was firmly in place by April 1996 and would not have required undue experimentation by a person of ordinary skill in the art in a combination with any of the references I rely on in this Declaration.

V. CONCLUSION

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

the invalidity of the '657 patent claims at issue and/or offer testimony in support of this Declaration.

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

Dated: January 12, 2017

Respectfully submitted,

Tal Lavian
Jan 12, 2017

Tal Lavian, Ph.D.
Sunnyvale, California

EXHIBIT A

Tal Lavian, Ph.D.

http://telecommnet.com
http://cs.berkeley.edu/~tlavian
tlavian@telecommnet.com

1640 Mariani Dr.
Sunnyvale, CA 94087
(408)-209-9112

Research and Consulting:Telecommunications,Network Communications, and Mobile Wireless Technologies

Scientist, educator, and technologist with over 25years of experience; co-author on over 25 scientific publications, journal articles, and peer-reviewed papers; named inventor on over 100 issued and filed patents; industry fellow and lecturer at UC Berkeley Engineering–Center for Entrepreneurship and Technology (CET)

EDUCATION

- **Ph.D.**, Computer Science specializing in networking and communications, UC Berkeley
- **M.Sc.**, Electrical Engineering, Tel Aviv University
- **B.Sc.**, Mathematics and Computer Science, Tel Aviv University

EXPERTISE

Network communications, telecommunications, Internet protocols, and mobile wireless:

- **Communication networks:** Internet protocols; TCP/IP suite; TCP; UDP; IP; VoIP; Ethernet; network protocols; network software applications; data link, network, and transport layers (L2, L3, L4)
- **Internet software:** Internet software applications; distributed computing; cloud computing; Web applications; FTP; HTTP; Java; client server; file transfer; multicast; streaming media
- **Routing/switching:** LAN; WAN; VPN; routing protocols; RIP; BGP; MPLS; OSPF; IS-IS; DNS; QoS; switching; packet switching; network infrastructure; network communication architectures
- **Mobile wireless:** wireless LAN; 802.11; cellular systems; mobile devices; smartphone technologies

ACCOMPLISHMENTS

- Selected as principal investigator for three US Department of Defense (DARPA) projects
- Directed research project on networking computation for the US Air Force Research Lab (AFRL)
- Led and developed the first network resourcescheduling service for grid computing
- Administered wireless research project for an undisclosed US federal agency
- Managed and engineered the first demonstrated transatlantic dynamic allocation of 10Gbs Lambdas as a grid service
- Spearheaded the development of the first demonstrated wire-speed active network on commercial hardware
- Invented over 100 patents; over 50 prosecuted *pro se* in front of the USPTO
- Created and chaired Nortel Networks' EDN Patent Committee

PROFESSIONAL EXPERIENCE

University of California, Berkeley, Berkeley, California 2000-Present
Berkeley Industry Fellow, Lecturer, Visiting Scientist, Ph.D. Candidate, Nortel's Scientist Liaison
Some positions and projects were concurrent, others sequential

- Serves as an industry fellow and lecturer at the Center for Entrepreneurship and Technology (CET).
- Studied network services, telecommunication systems and software, communications infrastructure, and data centers
- Developed long-term technology for the enterprise market, integrating communication and computing technologies
- Conducted research projects in data centers (RAD Labs), telecommunication infrastructure (SAHARA), and wireless systems (ICEBERG)
- Acted as scientific liaison between Nortel Research Lab and UC Berkeley, providing tangible value in advanced technologies
- Earned a Ph.D. in Computer Science with a specialization in communications and networking

TelecommNet Consulting, Inc.(Innovations-IP) Sunnyvale, California 2006-Present
Principal Scientist

- Consults in the areas of network communications, telecommunications, Internet protocols, and smartphone mobile wireless devices
- Provides architecture and system consultation for projects relating to computer networks, mobile wireless devices, and Internet web technologies
- Acts as an expert witness in network communications patent infringement lawsuits

VisuMenu, Inc., Sunnyvale, California 2010-Present
Co- Founder and Chief Technology Officer (CTO)

- Designs and develops architecture and system of visual IVR technologies for smartphones and wireless mobile devices in the area of network communications
- Designs crawler/spider system for IVR / PBX using Asterisk, SIP, and VoIP
- Deploys the system as cloud networking and cloud computing utilizing Amazon Web Services

Ixia, Santa Clara, California 2008 - 2008
Communications Consultant

- Researched and developed advanced network communications testing technologies:
  • IxNetwork/IxN2X — tested IP routing and switching devices and broadband access equipment. Provided traffic generation and emulation for the full range of protocols: routing, MPLS, layer 2/3 VPNs, carrier Ethernet, broadband access, and data center bridging
  • IxLoad — quickly and accurately modeled high-volume video, data, and voice subscribers and servers to test real-world performance of multiservice delivery and security platforms
  • IxCatapult — emulated a broad range of wireless access and core protocols to test wireless components and systems that, when combined with IxLoad, provides an end-to-end solution for testing wireless service quality
  • IxVeriWave — employed a client-centric model to test Wi-Fi and wireless LAN networks by generating repeatable large-scale, real-world test scenarios that are virtually impossible to create by any other means

• Test automation — provided simple, comprehensive lab automation to help test engineering teams create, organize, catalog, and schedule execution of tests

Nortel Networks, Santa Clara, California 1996 - 2007
Originally employed by Bay Networks, which was acquired by Nortel Networks
Principal Scientist, Principal Architect, Principal Engineer, Senior Software Engineer

- Held scientific and research roles at Nortel Labs, Bay Architecture Labs, and in the office of the CTO

Principal Investigator for US Department of Defense (DARPA) Projects
- Conceived, proposed, and completed three research projects: active networks, DWDM-RAM, and a networking computation project for Air Force Research Lab (AFRL)
- Led a wireless research project for an undisclosed US federal agency

Academic and Industrial Researcher
- Analyzed new technologies to reduce risks associated with R&D investment
- Spearheaded research collaboration with leading universities and professors at UC Berkeley, Northwestern University, University of Amsterdam, and University of Technology, Sydney
- Evaluated competitive products relative to Nortel's products and technology
- Proactively identified prospective business ideas, which led to new networking products
- Predicted technological trends through researching the technological horizon and academic sphere
- Designed software for switches, routers, and network communications devices
- Developed systems and architectures for switches, routers, and network management
- Researched and developed the following projects:
  - Data-Center Communications: network and server orchestration 2006-2007
  - DRAC: SOA-facilitated L1/L2/L3 network dynamic controller 2003-2007
  - Omega: classified wireless project for undisclosed US Federal Agency 2006-2006
  - Open platform: project for the US Air Force Research Laboratory (AFRL) 2005-2005
  - Network resource orchestration for Web services workflows 2004-2005
  - Proxy study between Web/grids services and network services 2004-2004
  - Streaming content replication: real-time A/V media multicast at edge 2003-2004
  - DWDM-RAM: US DARPA-funded program on agile optical transport 2003-2004
  - Packet capturing and forwarding service on IP and Ethernet traffic 2002-2003
  - CO2: content-aware agile networking 2001-2003
  - Active networks: US DARPA-funded research program 1999-2002
  - ORE: programmable network service platform 1998-2002
  - JVM platform: Java on network devices 1998-2001
  - Web-based device management: network device management 1996-1997

Technology Innovator and Patent Leader
- Created and chaired Nortel Networks' EDN Patent Committee
- Facilitated continuous stream of innovative ideas and their conversion into intellectual property rights
- Developed intellectual property assets through invention and analysis of existing technology portfolios

Aptel Communications, Netanya, Israel 1994-1995

Software Engineer, Team Leader

Start-up company focused on mobile wireless CDMA spread spectrum PCN/PCS

- Developed a mobile wireless device using an unlicensed band [Direct Sequence Spread Spectrum (DSSS)]
- Designed and managed a personal communication network (PCN) and personal communication system (PCS), which are the precursors of short text messages (SMS)
- Designed and developed network communications software products (mainly in C/C++)
- Brought a two-way paging product from concept to development

Scitex Ltd.,Herzeliya, Israel 1990-1993

Software Engineer, Team Leader

Software and hardware company acquired by Hewlett Packard (HP)

- Developed system and network communications (mainly in C/C++)
- Invented Parallel SIMD Architecture
- Participated in the Technology Innovation group

Shalev, Ramat-HaSharon, Israel 1987-1990

Start-up company

Software Engineer

- Developed real-time software and algorithms (mainly in C/C++ and Pascal)

PROFESSIONAL ASSOCIATIONS

- IEEE senior member
- IEEE CNSV co-chair, Intellectual Property SIG (2013)
- President Next Step Toastmasters (an advanced TM club in the Silicon Valley) (2013-2014)
- Technical co-chair, IEEE Hot Interconnects 2005 at Stanford University
- Member, IEEE Communications Society (COMMSOC)
- Member, IEEE Computer Society
- Member, IEEE Systems, Man, and Cybernetics Society
- Member, IEEE-USA Intellectual Property Committee
- Member, ACM, ACM Special Interest Group on Data Communication (SIGCOM)
- Member, ACM Special Interest Group on Hypertext, Hypermedia, and Web (SIGWEB)
- Member, IEEE Consultants' Network (CNSV)
- Global Member, Internet Society (ISOC)
- President Java Users Group – Silicon Valley Mountain View, CA,1999-2000
- Toastmasters International

ADVISORY BOARDS

- Quixey –search engine for wireless mobile apps
- Mytopia – mobile social games
- iLeverage – Israeli Innovations

PROFESSIONAL AWARDS

- Top Talent Award – Nortel
- Top Inventors Award – Nortel EDN
- Certified IEEE-WCET - Wireless Communications Engineering Technologies
- Toastmasters International - Competent Communicator (twice)
- Toastmasters International - Advanced Communicator Bronze

Patents and Publications

(Not an exhaustive list)

Patents Issued

US 9,184,989	Grid proxy architecture for network resources	Link
US 9,083,728	Systems and methods to support sharing and exchanging in a network	Link
US 9,021,130	Photonic line sharing for high-speed routers	Link
US 9,001,819	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,949,846	Time-value curves to provide dynamic QoS for time sensitive file transfers	Link
US 8,929,517	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,903,073	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,898,274	Grid proxy architecture for network resources	Link
US 8,880,120	Device and method for providing enhanced telephony	Link
US 8,879,703	System method and device for providing tailored services when call is on-hold	Link
US 8,879,698	Device and method for providing enhanced telephony	Link
US 8,867,708	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,787,536	Systems and methods for communicating with an interactive voice response system	Link
US 8,782,230	Method and apparatus for using a command design pattern to access and configure network elements	Link
US 8,762,963	Translation of programming code	Link
US 8,762,962	Methods and apparatus for automatic translation of a computer program language code	Link
US 8,745,573	Platform-independent application development framework	Link
US 8,731,148	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,688,796	Rating system for determining whether to accept or reject objection raised by user in social network	Link
US 8,619,793	Dynamic assignment of traffic classes to a priority queue in a packet forwarding device	Link
US 8,572,303	Portable universal communication device	Link
US 8,553,859	Device and method for providing enhanced telephony	Link

US 8,548,131	Systems and methods for communicating with an interactive voice response system	Link
US 8,537,989	Device and method for providing enhanced telephony	Link
US 8,341,257	Grid proxy architecture for network resources	Link
US 8,161,139	Method and apparatus for intelligent management of a network element	Link
US 8,146,090	Time-value curves to provide dynamic QoS for time sensitive file transfer	Link
US 8,078,708	Grid proxy architecture for network resources	Link
US 7,944,827	Content-aware dynamic network resource allocation	Link
US 7,860,999	Distributed computation in network devices	Link
US 7,734,748	Method and apparatus for intelligent management of a network element	Link
US 7,710,871	Dynamic assignment of traffic classes to a priority queue in a packet forwarding device	Link
US 7,580,349	Content-aware dynamic network resource allocation	Link
US 7,433,941	Method and apparatus for accessing network information on a network device	Link
US 7,359,993	Method and apparatus for interfacing external resources with a network element	Link
US 7,313,608	Method and apparatus for using documents written in a markup language to access and configure network elements	Link
US 7,260,621	Object-oriented network management interface	Link
US 7,237,012	Method and apparatus for classifying Java remote method invocation transport traffic	Link
US 7,127,526	Method and apparatus for dynamically loading and managing software services on a network device	Link
US 7,047,536	Method and apparatus for classifying remote procedure call transport traffic	Link
US 7,039,724	Programmable command-line interface API for managing operation of a network device	Link
US 6,976,054	Method and system for accessing low-level resources in a network device	Link
US 6,970,943	Routing architecture including a compute plane configured for high-speed processing of packets to provide application layer support	Link
US 6,950,932	Security association mediator for Java-enabled devices	Link
US 6,850,989	Method and apparatus for automatically configuring a network switch	Link

US 6,845,397	Interface method and system for accessing inner layers of a network protocol	Link
US 6,842,781	Download and processing of a network management application on a network device	Link
US 6,772,205	Executing applications on a target network device using a proxy network device	Link
US 6,564,325	Method of and apparatus for providing multi-level security access to system	Link
US 6,175,868	Method and apparatus for automatically configuring a network switch	Link
US 6,170,015	Network apparatus with Java co-processor	Link
US 8,687,777	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,681,951	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,625,756	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,594,280	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,548,135	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,406,388	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,345,835	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,223,931	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,160,215	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,155,280	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,054,952	Systems and methods for visual presentation and selection of IVR menu	Link
US 8,000,454	Systems and methods for visual presentation and selection of IVR menu	Link
EP 1,905,211	Technique for authenticating network users	Link
EP 1,142,213	Dynamic assignment of traffic classes to a priority queue in a packet forwarding device	Link
EP 1,671,460	Method and apparatus for scheduling resources on a switched underlay network	Link
CA 2,358,525	Dynamic assignment of traffic classes to a priority queue in a packet forwarding device	Link

Patent Applications Published and Pending
(Not an exhaustive list)

US 20150058490	Grid Proxy Architecture for Network Resources	Link
US 20150010136	Systems and Methods for Visual Presentation and Selection of IVR Menu	Link
US 20140379784	Method and Apparatus for Using a Command Design Pattern to Access and Configure Network Elements	Link
US 20140105025	Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device	Link
US 20140105012	Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device	Link
US 20140012991	Grid Proxy Architecture for Network Resources	Link
US 20130080898	Systems and Methods for Electronic Communications	Link
US 20130022191	Systems and Methods for Visual Presentation and Selection of IVR Menu	Link
US 20130022183	Systems and Methods for Visual Presentation and Selection of IVR Menu	Link
US 20130022181	Systems and Methods for Visual Presentation and Selection of IVR Menu	Link
US 20120180059	Time-Value Curves to Provide Dynamic QOS for Time Sensitive File Transfers	Link
US 20120063574	Systems and Methods for Visual Presentation and Selection of IVR Menu	Link
US 20110225330	Portable Universal Communication Device	Link
US 20100220616	Optimizing Network Connections	Link
US 20100217854	Method and Apparatus for Intelligent Management of a Network Element	Link
US 20100146492	Translation of Programming Code	Link
US 20100146112	Efficient Communication Techniques	Link
US 20100146111	Efficient Communication in a Network	Link
US 20090313613	Methods and Apparatus for Automatic Translation of a Computer Program Language Code	Link
US 20090313004	Platform-Independent Application Development Framework	Link
US 20090279562	Content-aware dynamic network resource allocation	Link
US 20080040630	Time-Value Curves to Provide Dynamic QoS for Time Sensitive File	Link

	Transfers	
US 20070169171	Technique for authenticating network users	Link
US 20060123481	Method and apparatus for network immunization	Link
US 20060075042	Extensible Resource Messaging Between User Applications and Network Elements in a Communication Network	Link
US 20050083960	Method and Apparatus for Transporting Parcels of Data Using Network Elements with Network Element Storage	Link
US 20050076339	Method and Apparatus for Automated Negotiation for Resources on a Switched Underlay Network	Link
US 20050076336	Method and Apparatus for Scheduling Resources on a Switched Underlay Network	Link
US 20050076173	Method And Apparatus for Preconditioning Data to Be Transferred on a Switched Underlay Network	Link
US 20050076099	Method and Apparatus for Live Streaming Media Replication in a Communication Network	Link
US 20050074529	Method and apparatus for transporting visualization information on a switched underlay network	Link
US 20040076161	Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device	Link
US 20020021701	Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device	Link
WO 2006/063052	Method and apparatus for network immunization	Link
WO 2007/008976	Technique for authenticating network users	Link
WO2000/0054460	Method and apparatus for accessing network information on a network device	Link
US 20140156556	Time-variant rating system and method thereof	Link
US 20140156758	Reliable rating system and method thereof	Link

Publications
(Not an exhaustive list)

- "R&D Models for Advanced Development & Corporate Research" Understanding Six Models of Advanced R&D - Ikhlaq Sidhu, Tal Lavian, Victoria Howell - University of California, Berkeley. Accepted paper for 2015 ASEE Annual Conference and Exposition- June 2015
- "Communications Architecture in Support of Grid Computing",Tal Lavian,Scholar's Press 2013ISBN 978-3-639-51098-0.
- "Applications Drive Secure Lightpath Creation across Heterogeneous Domains, Feature Topic Optical Control Planes for Grid Networks: Opportunities, Challenges and the Vision." Gommans L.; Van Oudenaarde B.; Dijkstra F.; De Laat C.; Lavian T.; Monga I.; Taal A.; Travostino F.; Wan A.; IEEE Communications Magazine, vol. 44, no. 3, March 2006, pp. 100-106.
- *Lambda Data Grid: Communications Architecture in Support of Grid Computing*. Tal I. Lavian, Randy H. Katz; Doctoral Thesis, University of California at Berkeley. January 2006.
- "Information Switching Networks." Hoang D.B.; T. Lavian;The 4th Workshop on the Internet, *Telecommunications and Signal Processing, WITSP2005*, December 19-21, 2005, Sunshine Coast, Australia.
- "Impact of Grid Computing on Network Operators and HW Vendors." Allcock B.; Arnaud B.; Lavian T.; Papadopoulos P.B.; Hasan M.Z.; Kaplow W.; *IEEE Hot Interconnects at Stanford University 2005*, pp.89-90.
- *DWDM-RAM: A Data Intensive Grid Service Architecture Enabled by Dynamic Optical Networks*. Lavian T.; Mambretti J.; Cutrell D.; Cohen H.J; Merrill S.; Durairaj R.; Daspit P.; Monga I.; Naiksatam S.; Figueira S.; Gutierrez D.; Hoang D.B., Travostino F.; *CCGRID 2004*, pp. 762-764.
- *DWDM-RAM: An Architecture for Data Intensive Service Enabled by Next Generation Dynamic Optical Networks*. Hoang D.B.; Cohen H.; Cutrell D.; Figueira S.; Lavian T.; Mambretti J.; Monga I.; Naiksatam S.; Travostino F.; Proceedings IEEE Globecom 2004, Workshop on High-Performance Global Grid Networks, Houston, 29 Nov. to 3 Dec. 2004, pp.400-409.
- *Implementation of a Quality of Service Feedback Control Loop on Programmable Routers*. Nguyen C.; Hoang D.B.; Zhao, I.L.; Lavian, T.; Proceedings, 12th IEEE International Conference on Networks 2004. (ICON 2004) Singapore, Volume 2, 16-19 Nov. 2004, pp.578-582.
- *A Platform for Large-Scale Grid Data Service on Dynamic High-Performance Networks*. Lavian T.; Hoang D.B.; Mambretti J.; Figueira S.; Naiksatam S.; Kaushil N.; Monga I.; Durairaj R.; Cutrell D.; Merrill S.; Cohen H.; Daspit P.; Travostino F; GridNets 2004, San Jose, CA., October 2004.
- *DWDM-RAM: Enabling Grid Services with Dynamic Optical Networks*. Figueira S.; Naiksatam S.; Cohen H.; Cutrell D.; Daspit, P.; Gutierrez D.; Hoang D. B.; Lavian T.; Mambretti J.; Merrill S.; Travostino F; Proceedings, 4th IEEE/ACM International Symposium on Cluster Computing and the Grid, Chicago, USA, April 2004, pp. 707-714.
- *DWDM-RAM: Enabling Grid Services with Dynamic Optical Networks*. Figueira S.; Naiksatam S.; Cohen H.; Cutrell D.; Gutierrez D.; Hoang D.B.; Lavian T.; Mambretti J.; Merrill S.; Travostino F.; 4th IEEE/ACM International Symposium on Cluster Computing and the Grid, Chicago, USA, April 2004.
- *An Extensible, Programmable, Commercial-Grade Platform for Internet Service Architecture*. Lavian T.; Hoang D.B.; Travostino F.; Wang P.Y.; Subramanian S.; Monga I.; IEEE Transactions on Systems, Man, and Cybernetics on Technologies Promoting Computational

Intelligence, Openness and Programmability in Networks and Internet Services Volume 34, Issue 1, Feb. 2004, pp.58-68.

- *DWDM-RAM: An Architecture for Data Intensive Service Enabled by Next Generation Dynamic Optical Networks*. Lavian T.; Cutrell D.; Mambretti J.; Weinberger J.; Gutierrez D.; Naiksatam S.; Figueira S.; Hoang D. B.; Supercomputing Conference, SC2003 Igniting Innovation, Phoenix, November 2003.
- *Edge Device Multi-Unicasting for Video Streaming*. Lavian T.; Wang P.; Durairaj R.; Hoang D.; Travostino F.; Telecommunications, 2003. ICT 2003. 10th International Conference on Telecommunications, Tahiti, Volume 2, 23 Feb.-1 March, 2003 pp. 1441-1447.
- The SAHARA Model for Service Composition Across Multiple Providers. Raman B.; Agarwal S.; Chen Y.; Caesar M.; Cui W.; Lai K.; Lavian T.; Machiraju S.; Mao Z. M.; Porter G.; Roscoe T.; Subramanian L.; Suzuki T.; Zhuang S.; Joseph A. D.; Katz Y.H.; Stoica I.; Proceedings of the First International Conference on Pervasive Computing. ACM Pervasive 2002, pp. 1-14.
- *Enabling Active Flow Manipulation in Silicon-Based Network Forwarding Engines*. Lavian T.; Wang P.; Travostino F.; Subramanian S.; Duraraj R.; Hoang D.B.; Sethaput V.; Culler D.; Proceeding of the Active Networks Conference and Exposition, 2002.(DANCE) 29-30 May 2002, pp. 65-76.
- *Practical Active Network Services within Content-Aware Gateways*. Subramanian S.; Wang P.; Durairaj R.; Rasimas J.; Travostino F.; Lavian T.; Hoang D.B.; Proceeding of the DARPA Active Networks Conference and Exposition, 2002.(DANCE) 29-30 May 2002, pp. 344-354.
- *Active Networking on a Programmable Network Platform*. Wang P.Y.; Lavian T.; Duncan R.; Jaeger R.; Fourth IEEE Conference on Open Architectures and Network Programming (OPENARCH), Anchorage, April 2002.
- *Intelligent Network Services through Active Flow Manipulation*. Lavian T.; Wang P.; Travostino F.; Subramanian S.; Hoang D.B.; Sethaput V.; IEEE Intelligent Networks 2001 Workshop (IN2001), Boston, May 2001.
- *Intelligent Network Services through Active Flow Manipulation*. Lavian T.; Wang P.; Travostino F.; Subramanian S.; Hoang D.B.; Sethaput V.; Intelligent Network Workshop, 2001 IEEE 6-9 May 2001, pp.73 -82.
- *Enabling Active Flow Manipulation in Silicon-based Network Forwarding Engine*. Lavian, T.; Wang, P.; Travostino, F.; Subramanian S.; Hoang D.B.; Sethaput V.; Culler D.; Journal of Communications and Networks, March 2001, pp.78-87.
- *Active Networking on a Programmable Networking Platform*. Lavian T.; Wang P.Y.; IEEE Open Architectures and Network Programming, 2001, pp. 95-103.
- *Enabling Active Networks Services on a Gigabit Routing Switch*. Wang P.; Jaeger R.; Duncan R.; Lavian T.; Travostino F.; 2nd Workshop on Active Middleware Services, 2000.
- *Dynamic Classification in Silicon-Based Forwarding Engine Environments*. Jaeger R.; Duncan R.; Travostino F.; Lavian T.; Hollingsworth J.; Selected Papers. 10th IEEE Workshop on Metropolitan Area and Local Networks, 1999. 21-24 Nov. 1999, pp.103-109.
- *Open Programmable Architecture for Java-Enabled Network Devices*. Lavian, T.; Jaeger, R. F.; Hollingsworth, J. K.; IEEE Hot Interconnects Stanford University, August 1999, pp. 265-277.
- *Open Java SNMP MIB API*. Rob Duncan, Tal Lavian, Roy Lee, Jason Zhou, Bay Architecture Lab Technical Report TR98-038, December 1998.
- *Java-Based Open Service Interface Architecture*. Lavian T.; Lau S.; BAL TR98-010 Bay Architecture Lab Technical Report, March 1998.

- *Parallel SIMD Architecture for Color Image Processing*. Lavian T. Tel – Aviv University, Tel – Aviv, Israel, November 1995.
- *Grid Network Services, Draft-ggf-ghpn-netservices-1.0*. George Clapp, Tiziana Ferrari, Doan B. Hoang, Gigi Karmous-Edwards, Tal Lavian, Mark J. Leese, Paul Mealor, Inder Monga, Volker Sander, Franco Travostino, Global Grid Forum(GGF).
- *Project DRAC: Creating an applications-aware network*.Travostino F.; Keates R.; Lavian T.; Monga I.; Schofield B.; Nortel Technical Journal, February 2005, pp. 23-26.
- *Optical Network Infrastructure for Grid, Draft-ggf-ghpn-opticalnets-1*. Dimitra Simeonidou, Reza Nejabati, Bill St. Arnaud, Micah Beck, Peter Clarke, Doan B. Hoang, David Hutchison, Gigi Karmous-Edwards, Tal Lavian, Jason Leigh, Joe Mambretti, Volker Sander, John Strand, Franco Travostino, Global Grid Forum(GGF) GHPN Standard GFD-I.036 August 2004.
- *Popeye - Using Fine-grained Network Access Control to Support Mobile Users and Protect Intranet Hosts*. Mike Chen, Barbara Hohlt, Tal Lavian, December 2000.

Presentations and Talks

(Not an exhaustive list)

- Lambda Data Grid: An Agile Optical Platform for Grid Computing and Data-intensive Applications.
- Web Services and OGSA
- WINER Workflow Integrated Network Resource Orchestration.
- Technology & Society
- Abundant Bandwidth and how it affects us?
- Active Content Networking(ACN)
- DWDM-RAM:Enabling Grid Services with Dynamic Optical Networks
- Application-engaged Dynamic Orchestration of Optical Network Resources
- A Platform for Data Intensive Services Enabled by Next Generation Dynamic Optical Networks
- Optical Networks
- Grid Optical Network Service Architecture for Data Intensive Applications
- Optical Networking & DWDM
- OptiCal Inc.
- OptiCal & LUMOS Networks
- Optical Networking Services
- Business Models for Dynamically Provisioned Optical Networks
- Business Model Concepts for Dynamically Provisioned Optical Networks
- Optical Networks Infrastructure
- Research Challenges in agile optical networks
- Services and Applications' infrastructure for agile optical networks
- Impact on Society
- TeraGrid Communication and Computation
- Unified Device Management via Java-enabled Network Devices
- Active Network Node in Silicon-Based L3 Gigabit Routing Switch
- Active Nets Technology Transfer through High-Performance Network Devices
- Programmable Network Node: Applications
- Open Innovation via Java-enabled Network Devices
- Practical Considerations for Deploying a Java Active Networking Platform
- Open Java-Based Intelligent Agent Architecture for Adaptive Networking Devices

- Java SNMP Oplet
- Open Distributed Networking Intelligence: A New Java Paradigm
- Open Programmability
- Active Networking On A Programmable Networking Platform
- Open Networking through Programmability
- Open Programmable Architecture for Java-enabled Network Devices
- Integrating Active Networking and Commercial-Grade Routing Platforms
- Programmable Network Devices
- To be smart or not to be?