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. 8,473,552

TITLE: COMMUNICATIONS SYSTEM

DECLARATION OF TAL LAVIAN, PH.D.

Table of Contents

Page

I. INTRODUCTION AND QUALIFICATIONS 1

A. Summary of My Opinions 1

B. Qualifications and Experience 2

C. Materials Considered 5

II. PERSON OF ORDINARY SKILL IN THE ART 6

III. CLAIM CONSTRUCTION 7

A. "token" 8

B. "pointer" 9

C. "pointer-triggered message" 10

IV. APPLICATION OF THE PRIOR ART TO THE CLAIMS 12

A. Brief Description and Summary of the Prior Art 14

1. Roseman [Ex. 1003] 14

2. Rissanen [Ex. 1004] 18

3. Vetter [Ex. 1005] 20

4. Pike [Ex. 1006] 21

5. Lichty [Ex. 1007] 22

D. Each Limitation of Claims 1-61 & 64 Is Disclosed by the Prior Art 23

1. Claim 2 23

a. Preamble 23

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 1[a]) 50

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 1[b]) 54

Table of Contents
(continued)

Page

d. "permitting at least the first user identity and the second user identity to form a group" (claim 1[c]) 54

e. "permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group" (claim 1[d]) 55

f. "at least some of the communications include messages comprising more than one data type" (claim 1[e]) 56

g. "at least some other of the communications include a pointer that produces a pointer-triggered message on demand" (claim 1[f]) 57

2. Claims 1, 10, 18, 50, 54, 58, 59 & 64 (Independent Claims) 62

a. Independent Claim 1 62

b. Independent Claim 10 66

c. Independent Claim 18 69

d. Independent Claim 50 72

e. Independent Claim 54 75

f. Independent Claim 58 78

g. Independent Claim 59 81

h. Independent Claim 64 87

3. Claims 3, 5, 7, 11, 13, 15, 21, 24, 28, 32, 36, 40, 44 & 55 (Claims Regarding Data Representing or Comprising Sound/Audio, Video and/or Graphics) 90

4. Claims 4, 6, 8, 9 (Claims Regarding Presenting Multimedia Based on Stored Authorization) 91

5. Claims 12, 14, 16, 17, 20, 23, 26, 27, 30, 31, 34, 35, 38, 39, 42, 43, 46, 47, 48, 49, 52 & 53 ("Member-Associated Image" Claims) 92

Table of Contents
(continued)

Page

6. Claims 19, 22, 25, 29, 33, 37, 41, 45 & 51 ("Pointer-Triggered Message" Claims) 93

7. Claims 56 & 57 94

V. CONCLUSION.....99

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

I. INTRODUCTION AND QUALIFICATIONS

A. Summary of My Opinions

1. U.S. Patent No. 8,473,552 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 '552 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 '552 patent. Roseman discloses a networked "virtual conferencing" system that discloses all of the supposedly inventive features of the '552 patent.

2. The remaining features in the claims recite functionalities that were standard Internet features such as using Uniform Resource Locators (URLs) to locate and retrieve content from the Internet. These features were built-in features of web browsers no later than 1994, including the Mosaic web browser discussed

in Mary Ann Pike et al., *Using Mosaic* (1994). As I will explain below, all of the challenged claims would have been obvious based on the prior art.

B. Qualifications and Experience

3. 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.

4. 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.

5. 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.

6. 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++).

7. 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.

8. 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").

9. 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.

10. 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

11. 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. 8,473,552 ("'552 patent") **[Ex. 1001]**, which states on its face that it issued from an application filed on August 24, 2006, 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.

12. I reviewed various documents dated prior to April 1996 describing the state of the art at the time of the alleged invention of the '552 patent. As explained below, some of these documents are relied upon as actually disclosing the limitations of the '552 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
1005	Ronald J. Vetter, *Videoconferencing on the Internet*, Computer, IEEE Computer Society, Vol. 28, No. 1, at pp.77-79 (Jan. 1995)
1006	Excerpts 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 ’552 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

13. I understand that an assessment of claims of the ’552 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.

14. 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.

15. 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 '552 patent have been based on the perspective of a person of ordinary skill in the art as of April 1996.

III. CLAIM CONSTRUCTION

16. 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 '552 patent in **Part IV** below, I provide constructions for certain terms in those claims.

17. I have been informed by counsel that a claim in an unexpired patent subject to *inter partes* review must be given its "broadest reasonable construction in light of the specification of the patent in which it appears," which is different from the manner in which the scope of a claim is determined in litigation. I apply the "broadest reasonable construction" standard in my analysis below.

A. "token"

18. Each independent claim recites a database that provides a "repository of tokens." The written description describes a "token" as a piece of information associated with a 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 use "identity tokens", which are pieces of information associated with user identity. The pieces of information are stored in memory **11** in a control computer database, along with personal information about the user, such as the user's age.

('552, 7:61-66.) 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" ('552, 8:6-7), "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" ('552, 8:15-18), 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." ('552, 8:21-23.)

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

B. "pointer"

20. The term "pointer" appears in each independent claim. "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.

21. 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**.

('552, 5:25-30.) Based on this description, the term "**pointer**" should be construed as a "**piece of information that points to or references other information**."

C. "pointer-triggered message"

22. The term "pointer-triggered" is recited various claims. As explained previously, the written description identifies a URL as an example of a pointer. I could not locate the term "pointer-triggered," or even the term "trigger," in the written description.

23. In my opinion, the term "pointer-triggered" generally refers to a message whose content is referenced – and thus may be obtained – by a pointer such as a URL. As noted in the passage quoted above, "URLs can point to pre-stored audio and video communications, which the Controller Computer **3** can fetch and communicate to the Participator Computers **5**." ('552, 5:27-30.) The written description identifies several examples of how this might occur. First, it describes an embodiment in which a received message contains a URL, to which the software on the participator computer can respond by executing an external data viewer, but "only upon demand of the operator of the participator software":

> If a URL is detected at Block **116**, Block **118** invokes an external data type viewer only on demand of the operator of the participator software, and otherwise Block **120** stores the reference for future use by the operator of the participator software, or treats the reference as an externally handled multimedia type (at the user's option).

('552, 7:38-43.) The patent describes another example in which a multimedia message containing a URL is sent, and the participator software attempts to present the message in a readable way:

> The controller computer **5** now passes the URL to the channel members. This participator software **4** performs two actions in response to the graphical multimedia display request. The first is to put the name of the URL onto the transcript of the group's channel, so that it can be read by group members. The second response is to have the participator software show the data associated with the graphical multimedia message in a human interpretable way (at FIG. 25). To do this, the participator software **6** either uses built in rules to decide how the graphical multimedia data is to be presented, or locates another program suitable to present the data. In this case, the software **6** is utilizing Netscape Navigator™, a program for displaying graphical multimedia documents specified by a URL (at FIG. 26). Inside the Navigator window, the graphical multimedia content, the home page of AIS, is shown.

('552, 10:44-59.)

24. As noted above, the patent expressly describes an embodiment in which an external viewer to view content referenced by a URL is invoked "only on demand of the operator of the participator software" ('552, 7:38-43), so in my opinion, the term "**pointer-triggered**" under its broadest reasonable construction should not be construed to require that the content be obtained automatically

(without any user action). It should also encompass, under its broadest reasonable construction, the scenario in which a user activates the pointer (for example by clicking the URL), causing the computer to invoke the pointer and obtain the content to which it refers. In my opinion, the broadest reasonable construction of "**pointer-triggered message**" is a "**message that allows its recipient to obtain content via a pointer**."

IV. APPLICATION OF THE PRIOR ART TO THE CLAIMS

25. I have reviewed and analyzed the prior art references and materials listed in **Part I.B** above. In my opinion, each and every limitation of claims 1-61 and 64 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]**; **(4)** Mary Ann Pike et al., *Using Mosaic* (1994) ("Pike") **[Ex. 1006]**; and **(5)** Tom Lichty, *The Official America Online for Macintosh Membership Kit & Tour Guide* (2nd ed.) (1994) ("Lichty") **[Ex. 1007]**. As shown below, each limitation of claims 1-61 and 64 is disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

26. Before delving into the analysis of the claim limitations, a few observations should be made. I have cited five prior art references, but Roseman is the base reference that discloses the majority of the claim limitations. My citation to the other four prior art references concerns claim limitations that relate to small implementation details. For example, I cite Rissanen to show that the tokens in Roseman could be stored in a "database," Vetter to show that Roseman could have been adapted to communicate over the "Internet," Pike to show that Roseman could have used Internet URLs, and Lichty for its explanation of known content filtering features. These details would have been seen as so trivial to a person of ordinary skill in the art by April 1996 that these additional prior art references arguably were not even required to show obviousness.

27. I also observe that the claims of the '552 patent reveal significant redundancy and duplication – later-recited claims often recite substantially the same and in many cases identical language as earlier claims. I will therefore devote a significant part of my analysis to the earlier independent claims (starting with claim 2, which is representative), and in the interests of brevity and to avoid repetition, refer back to that analysis to the extent it applies to later claims.

A. Brief Description and Summary of the Prior Art

28. I am informed that all of the references cited in this Declaration properly qualify as "prior art" for purposes of the '552 patent. I am informed that Roseman qualifies as prior art because it issued from an application filed on May 13, 1992, almost four years before the earliest application to which the '552 patent can claim priority (April 1, 1996). I am also informed that Vetter, Rissanen, Pike and Lichty qualify as prior art because they were published more than one year before April 1, 1996. Before explaining how the prior art applies to the claims, I will briefly summarize reference and provide an overview of how I have applied it.

1. Roseman [Ex. 1003]

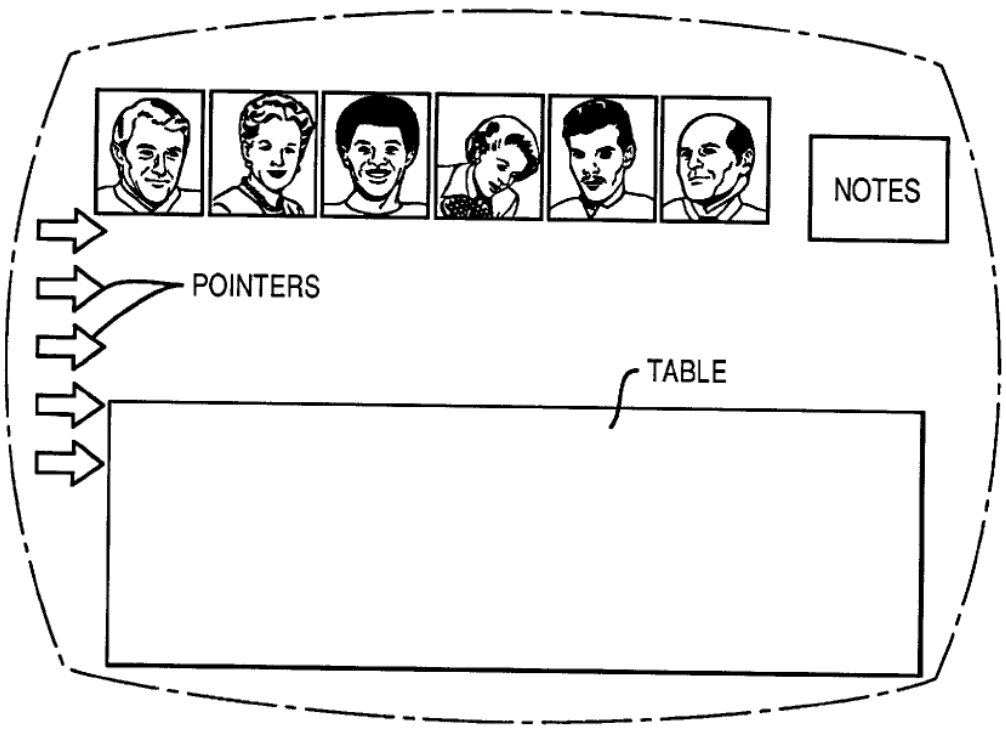
29. Roseman, entitled "Server Based Virtual Conferencing," discloses a system for creating a virtual conference room that allows participants to collaborate in real time over a computer network. My Declaration cites Roseman for the majority of the limitations in the challenged claims, and relies on the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

30. 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, 1:34-37, 2:64-3:7.) 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.)

31. 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.)

32. 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.

33. 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.

34. 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."), 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]

35. Each independent claim of the '552 patent recites "**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.

36. 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, at 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 user information and passwords of any form.

37. As I will explain in detail below, the user and password information in the database in Rissanen is analogous to the conference room "keys" in Roseman. It would have been obvious to 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]

38. Each independent claim of the '552 patent also recites the step of sending and/or receiving communications "**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. 1001, 1:34-41, 3:14-19.)

39. 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.)

40. 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]

41. 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 information communicated between computers can include a "pointer" (such as an Internet URL) that allows a message to be produced on demand.

42. 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 detailed mechanics of how the pointer works and does not mention URLs. In the event it is argued that the "pointer" and "pointer-triggered" limitations require something functionally equivalent to an Internet URL, these limitations would have been obvious to a person of ordinary skill in the art in view Pike**.**

43. URLs are used today to identify hundreds of millions of resources located on the Internet, and were clearly not an invention of the '552 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]

44. 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.

D. Each Limitation of Claims 1-61 & 64 Is Disclosed by the Prior Art

45. The '552 patent recites a total of nine independent claims. Because no claims depend from independent claim 1, for purposes of my analysis, I begin with independent claim 2, from which seven claims depend. I then address the remaining eight independent claims, whose limitations substantially overlap with each other, before addressing the challenged dependent claims of the patent.

1. Claim 2

a. Preamble

46. Claim 2 recites a lengthy preamble, reproduced in full below:

> 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, wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,

> wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network, and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer.

('552, 21:52-22:5.)

47. Roseman, in combination with Rissanen, Vetter, Pike and Lichty, discloses each aspect of the preamble of claim 2. Because of the length of the preamble, I will break up the claim language into pieces to help ensure that I cover all of the limitations the language potentially imposes.[1]

[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.

i. "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"

48. First, Roseman, in combination with Rissanen and Vetter, disclose "**[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**." As explained below, to the extent not disclosed by Roseman, I rely on Vetter for the requirement that communicating occur "via an Internet network" and on Rissanen for a "database."

49. Roseman discloses this limitation in the form of a computer system for virtual conferencing in which users (e.g. conference participants) communicate over a network (such as a Wide Area Network or "WAN"). 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.)

50. 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, become connected to a central, host, computer (or multiplicity of host computers) via the proper combination of Local Area Networks (LANs) and Wide Area Networks (WANs).

(Roseman, 3:14-19, 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.").)

51. 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).)

52. 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.").)

53. 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. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.") (underlining added).) The "keys" therefore qualify as "**tokens**."

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

55. 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.

56. 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 understand the claimed "database" under its broadest reasonable construction to simply refer to a stored collection of tokens. The '552 patent does not provide any detail about the claimed "database" except stating that the tokens "are stored in memory **11** in a control computer database, along with personal information about the user, such as the user's age." ('552, 7:64-66.) 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.

57. 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 '552 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, 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, 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).)

58. ***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 have understood that the user identity and password information in Rissanen is analogous to the "keys" in Roseman, and would have been 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 a "**database**" 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.

59. 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 a "**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 the "tokens" of Roseman in a database, and as such, it does not matter if the tokens 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 in a database applicable to any system that requires user authentication as a prerequisite to access, such as Roseman.

60. 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 a combination of stored data and computer programs." (Roseman, 12:16-18 (underlining added).) Moreover, in

order to access a conference room, the host computer presents a virtual "hallway" containing "doors," each door representing a different conference/meeting room. (Roseman, 9:63-65 ("The meeting room door is accessible from a hallway which has doors to other meeting rooms."), 10:28-29 ("Meeting rooms are child rooms of the hallway.").) Each meeting room therefore contains a number of computer programs, and each meeting room itself can be thought of as a program. These programs access the repository of keys when a user presents a key to obtain access to a conference room.

61. 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.

62. Finally, this portion of the claim preamble recites 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."

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

64. 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.

65. ***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) computer 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.

66. 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.

67. 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).)

68. 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 conferencing functions disclosed in Roseman. In my opinion, therefore, Roseman and Vetter disclose and render obvious this limitation.

ii. "thereby affording information to each of a plurality of participator computers which are otherwise independent of each other"

69. The preamble of claim 2 next recites, "**thereby affording information to each of a plurality of participator computers which are otherwise independent of each other**." Turning first to the step of "**affording information**," 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 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 2**[b]**, below.

70. Roseman also discloses affording information to "**each of a plurality of participator computers**." 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.)

71. Finally, 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 discussed above, to adapt Roseman to the Internet such that the Internet is the only network shared by the individual local computers. The participator computers in Roseman are therefore "otherwise independent of each other," as recited in the preamble.

iii. "wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives"

72. The preamble of claim 2 next recites, "**wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives**." Roseman discloses this limitation.

73. As noted previously, 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 publicly 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.

74. 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.

75. 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.

76. 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.)

77. 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."

iv. "wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members"

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

79. Turning first to the limitation, "**wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system**," 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, "the host makes an audio connection between the two whispering parties, and between nobody else," thus confirming that the host ("controller computer system") 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 by the controller computer system."

80. The next portion of the preamble 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 from another of the members.**" 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.)

v. "wherein at least some of the communications are received in real time via the Internet network"

81. The preamble of claim 2 next recites, "**wherein at least some of the communications are received in real time via the Internet network**." Roseman discloses that "at least some" communications within the group of the interactively connected participator computers are received in real time, such as placing documents on the table and movements from the electronic pencil, among others:

> 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.)

82. All of these interactions involve "communications received in real-time" 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 communications are received during a conference "in real time," as recited in the claim.

83. In addition, as explained above, these communications are received "**via the Internet network**" for the reasons explained for an earlier portion of the preamble. In particular, 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). Nevertheless, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill, as I explained earlier.

vi. "wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer"

84. The last portion of the preamble of claim 2 is disclosed by the videoconferencing software on the local computer, which executes the Whisper Mode feature. Roseman explains that, to activate Whisper Mode, "one party can click onto the picture of another" and "the host makes an audio connection between the two whispering parties, and between nobody else." (Roseman, 9:16-23 (emphasis added).) The host computer determines, therefore, that each other user identity is not one of the whispering parties, and thus the local computers for each of those user identities will not present the audio data to those users. (Roseman, 9:16 ("Any participant can whisper to another, without being-heard by others."),

15:8-9 ("HOST PROVIDES EXCLUSIVE VOICE LINK BETWEEN THE TWO PARTICIPANTS") (capital letters in original).)

85. 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.*)

86. Lichty provides a method for screening out ("censoring") certain messages from being received by a chat room participant. For example, a participant can prevent AOL from having messages from another recipient appear on the recipient's screen. (Lichty, pp. 269 ("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.").)

87. ***Rationale and Motivation to Combine***: It would have been obvious to a person of ordinary skill in the art adapt Roseman to provide the features of Lichty described above, predictably resulting in the virtual conference system of Roseman

in which at least one participant is "censored" from receiving audio data. This feature would allow a meeting participant in Roseman, for example, to block audio communications from identified individuals.

88. 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.

89. 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.

90. 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.

91. Having addressed the preamble of claim 2, I will now address the remaining claim limitations.

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 1[a])

92. Roseman next discloses that, after the first user identity has been authenticated and the participant is allowed to enter the conference room, the host computer transmits ("affords") some of the information from the conference room to that participant's computer. In particular, if the key is valid and the participant user has authority to use it, he or she may enter the conference room.

> 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</u>

> door opens and the user is admitted to the room. The other users in the room are alerted to a new presence and receive any relevant information.

(Roseman, 10:61-65 (underlining added).) This results in the host computer communicating with the participator computer:

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

(Roseman, 11:10-17; *see also id.*, 1:43-46 ("The host computer generates a common video screen, which it distributes to the parties: they see the drawings at their own local computers.").) 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 to the participant computer "**responsive to**" the participant being authenticated and allowed to enter the conference room

93. Once inside the conference, Roseman discloses multiple ways of communicating ("affording") some of the information to a first meeting participant. For example:

> 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").)

94. 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.)

95. 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.

96. Finally, this claim limitation recites "affording some of the information to a first of the participator computers **via the Internet network**." As I explained earlier, Roseman discloses that the host and participant computers may be connected via a Wide Area Network (WAN), and a person of ordinary skill in the art would have understood that the Internet is an example of a Wide Area Network (WAN). (Roseman, 3:14-19, 1:37-41.) Nevertheless, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill as I explained above.

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 1[b])

97. This limitation is substantially identical to the previous limitation except that it pertains to the "second of the participator computers" and the "second user identity." The analysis for the previous limitation applies with full force here. As explained above, Roseman discloses that a conference can contain multiple participants who receive and share information. Because the features described in Roseman are available to multiple conference participants, the same analysis for the "first participator computer" in claim 1**[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. "permitting at least the first user identity and the second user identity to form a group" (claim 1[c])

98. Roseman discloses "permitting at least the first user identity and the second user identity to form a group," *e.g.*, a group of participants who can join a virtual conference room. As explained earlier, 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.) Creating a virtual conference room involves identifying the participants of the conference room. (Roseman, 3:22-56.) 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.)

e. "permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group" (claim 1[d])

99. As explained previously, the virtual conferencing system in Roseman permits conference participants at their respective local computers to communicate in real time with other participants. (Roseman, 2:38-47; *see also id*. 7:54-8:5, 8:41-46, 12:26-28.) As explained above, these communications are sent "**via the Internet network**" for the reasons explained for an earlier portion of the preamble. In particular, 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). Nevertheless, adapting the virtual conferencing system of Roseman to communicate over the Internet would have been obvious to a person of ordinary skill, as I explained earlier.

f. "at least some of the communications include messages comprising more than one data type" (claim 1[e])

100. As explained below, Roseman makes clear that at least four types of content (sound, video, graphic, multimedia) may be communicated to conference participants.

101. **Sound and Video**: 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.) More specifically, "[w]hen a user enters a room with other occupants, the data connection is made. Audio and video connections are made if supported by the user, the room and the other users.." (Roseman, 11:11-13 (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.) Additionally, when the meeting begins, the host can send each participant a video 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 . . . .") (underlining added).)

102. **Text, Graphic and Sound**: Roseman discloses many ways in which text, graphic and sound 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).) Each invitee also has a graphical "pointer" that it can use to point to objects on the table. (Roseman, 7:61-64.) "With this cursor positioning, each participant can point to items which he or she verbally discusses, using the audio link." (Roseman, 7:65-67 (underlining added).)

g. "at least some other of the communications include a pointer that produces a pointer-triggered message on demand" (claim 1[f])

103. As I explained previously, a "pointer-triggered message" is a "message that allows its recipient to obtain content via a pointer," and a "pointer" is a piece of information that points to, or references, other information.

104. Roseman discloses several examples that satisfy this limitation. 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 the pointer is invoked, the file content is obtained and appears on the tables of each conference room participant, and thus "produces a pointer-triggered message on demand" as claimed.

105. 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 produces the content on demand.

106. In my opinion, the disclosures of Roseman alone disclose the claimed "pointer" and "pointer-triggered message." But in the event it is later argued or determined that "pointer" or "pointer-triggered message" requires an Internet URL or something functionally similar, or argues that the implementation of the file icon in Roseman is insufficiently described, then Roseman would render the "pointer-triggered message" limitation obvious in view of the teachings of Pike **[Ex. 1006.]**

107. 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, and a "pointer-triggered message" in

the form of a message containing a URL that causes a computer to fetch and retrieve a document from another computer.

108. ***Rationale and Motivation to Combine***: 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 a document placed on the table) included a URL that identified the location of the document on the host computer.

109. As explained previously, 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. 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 fetch the requested content and transmit it to second meeting participant computer over the Internet.

110. One of ordinary skill in the art would also 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 (thus consuming network bandwidth) unless the participant requests to view the content by invoking the URL (Pike, Ex. 1006, at 1.)

111. 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.)

112. By April 1996, therefore, a person of ordinary skill in the art would have found nothing non-obvious about adapting the document-on-the-table feature

of Roseman to send a message containing an Internet URL to meeting participants. Roseman specifically discloses that a document placed on the table can include "text" (8:2) and thus, a person of ordinary skill in the art would have understood that the document could contain an Internet URL. In my opinion, therefore, the "pointer-triggered" limitation provides no meaningful distinction over Roseman.

2. Claims 1, 10, 18, 50, 54, 58, 59 & 64 (Independent Claims)

113. As I noted above, the '552 patent recites a total of nine independent claims. As shown below, the independent claims share many common limitations, in identical or substantially similar language, with one or more other independent claims. In order to streamline my analysis, I have provided a side-by-side comparison between independent claim 2 and the remaining independent claims to highlight and focus on the differences between the claims, if any (underlining shows overlap of language).

a. Independent Claim 1

Method Claim 2	Apparatus Claim 1
2. 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,	1. Apparatus to control communication, the apparatus including: a controller computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, through an

Method Claim 2	Apparatus Claim 1
	Internet network, responsive to a respective authenticated user identity,
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,
the method including:	
affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	
(additional limitations omitted)	

Method Claim 2	Apparatus Claim 1
	the controller computer system controlling real-time communications by:
	storing each said user identity and a respective authorization to send multimedia data, the multimedia data comprising graphical data; and
	if permitted by the user identity corresponding to one of the participator computers, allowing the one of the participator computers to send multimedia data to another of the participator computers.

114. As shown in the table above, claim 1 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 1, my corresponding analysis for claim 2 applies with full force to claim 1.

115. As shown above, claim 1 recites "affording information . . . responsive to a respective authenticated user identity." This portion of claim 1 is addressed in substantially similar language later in claim 2. In particular, claim 2 recites in part, "affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity." My analysis above regarding that limitation of claim 2 applies with full force to claim 1.

116. Claim 1 also recites in part:

> the controller computer system controlling real-time communications by:
> storing each said user identity and a respective authorization to send multimedia data, the multimedia data comprising graphical data; and
> if permitted by the user identity corresponding to one of the participator computers, allowing the one of the participator computers to send multimedia data to another of the participator computers.

These limitations are disclosed by Roseman and Vissanen.

117. In particular, as explained above, Roseman discloses a virtual conferencing system that includes a host computer that enables conference participants to communicate in real time, including sending multimedia data comprising graphical data. (Roseman, 2:38-47 (underlining added); *see also id.* 7:54-8:5.) Roseman further discloses the use of keys associated with user identities for controlling admission to a particular conference. As explained for claim 2 above, the keys are stored and distributed by the host computer to potential conference participants. Each "key" that relates to the identity of the participant and provides the permissions allowing access to the conference room. (Roseman, 9:34-55 (underlining added); *see also id.*, 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 (emphasis added).) Thus, Roseman discloses these limitations of claim 1 because a user identity that is not authorized to access a room cannot send multimedia data to conference participants. As explained above, to the extent there is any question that Roseman discloses storing key information at the host computer, doing so would have been obvious to a person of ordinary skill in the art in view of Rissanen.

b. Independent Claim 10

Method Claim 2	Apparatus Claim 10
2. 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,	10. Apparatus to communicate via an Internet network, the apparatus 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, in communication with each of the participator computers responsive to a respective authenticated user identity,
	wherein the computer system permits at least a first of the participator computers and a second of the participator computers to form a group in which members can send communications in real time via the Internet network, and

Method Claim 2	Apparatus Claim 10
	receive communications from another of the members,
(See last limitation of claim 2)	wherein at least one of the communications includes a message comprising more than one data type, and at least one of the communications includes a pointer that produces a pointer-triggered message on demand;
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer.
the method including:	

Method Claim 2	Apparatus Claim 10
affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	
affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity;	
permitting at least the first user identity and the second user identity to form a group;	
and permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group,	
wherein at least some of the communications include messages comprising more than one data type, and at least some other of the communications include a pointer that produces a pointer-triggered message on demand.	

118. As shown in the table above, claim 10 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 10, my corresponding analysis for claim 2 applies with full force to claim 10.

119. As to the differences in claim language, claim 10 does not add anything that was not already addressed. Claim 10 recites "a computer system . . .

in communication with each of the participator computers responsive to a respective authenticated user identity" (underlining added). As explained previously, Roseman discloses a virtual conferencing system in which local computers are in communication with a host computer providing a virtual conference room, provided that the users of each local computer successfully authenticates using a key.

120. Claim 10 also recites "wherein the computer system permits at least a first of the participator computers and a second of the participator computers to form a group in which members can send communications in real time via the Internet network, and receive communications from another of the members." This limitation also does not add anything not previously discussed. As explained earlier, Roseman discloses a host computer that permits local computers to form groups in the form of conferences, child conferences, and Whisper Mode communications. In each of these types of groups, members can send communications in real time via the Internet and receive communications from other members. As I noted earlier, to the extent that Roseman does not disclose use of the Internet, it would have been obvious in view of Vetter.

c. Independent Claim 18

Method Claim 2	Apparatus Claim 18

Method Claim 2	Apparatus Claim 18
2. 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,	18. An apparatus to communicate via an Internet network, the apparatus including: a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the computer system in communication with each of the participator computers, responsive to a respective authenticated user identity, wherein the computer system:
	stores, for a first of the user identities, a respective authorization associated with multimedia data communication, and allows the participator computers to send in real time via the Internet network, and, based on the respective authorization, cause the multimedia data to be presented at one of the participator computers corresponding to a second of the user identities;
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and

Method Claim 2	**Apparatus Claim 18**
receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer.
the method including:	
affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	
(additional limitations omitted)	

121. As shown in the table above, claim 18 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 18, my corresponding analysis for claim 2 applies with full force to claim 18.

122. As to the differences in claim language, claim 18 does not add anything that was not already addressed. Claim 18 is substantially an amalgam of claim 1 and claim 2. As explained above, Roseman discloses "the computer

system in communication with each of the participator computers" because the host computer of the virtual conferencing system communicates with each local (participator) computer. As to the step of "affording information . . . responsive to a respective authenticated user identity," as explained above, this step is addressed in substantially similar language later in claim 2 ("affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity").

123. Claim 18 further recites limitations regarding storing authorization and allowing participator computers to send multimedia data that are substantially similar to limitations discussed above for claim 1 ("storing each said user identity and a respective authorization to send multimedia data"; "if permitted . . . allowing the one of the participator computers to send multimedia data"). My analysis above for claim 1 as to these limitations accordingly applies with full force to claim 18.

d. Independent Claim 50

Method Claim 2	Apparatus Claim 50
2. 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	50. Apparatus to send multimedia data, the apparatus including: a controller computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information

Method Claim 2	Apparatus Claim 50
to each of a plurality of participator computers which are otherwise independent of each other,	to each of a plurality of participator computers which are otherwise independent of each other, the participator computers communicatively connected to the controller computer system through an Internet network in association with an authenticated user identity, wherein the controller computer system controls real-time communications among the participator computers by:
	associating with the user identities a respective authorization to communicate multimedia data;
	and sending multimedia data representing at least one of a pointer, video, audio, graphic, and multimedia if permitted by the respective authorization;
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,

Method Claim 2	**Apparatus Claim 50**
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer.
(additional limitations omitted)	

124. As shown in the table above, claim 50 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 50, my corresponding analysis for claim 2 applies with full force to claim 50.

125. As to the differences in claim language, claim 50 does not add anything that was not already addressed. Claim 50 recites that "the participator computers communicatively connected to the controller computer system through an Internet network in association with an authenticated user identity." As already amply discussed, Roseman discloses local computers that connect via a host computer provided that any required key successfully authenticates a user to enter a virtual conference room. To the extent that Roseman does not disclose

connecting "through an Internet network," it would have been obvious in view of Vetter, as explained previously.

126. Claim 50 also recites, "wherein the controller computer system controls real-time communications among the participator computers by: associating with the user identities a respective authorization to communicate multimedia data; and sending multimedia data representing at least one of a pointer, video, audio, graphic, and multimedia if permitted by the respective authorization." These limitations are substantially similar to limitations in claim 1 regarding storing authorization and allowing participator computers to send multimedia data ("storing each said user identity and a respective authorization to send multimedia data"; "if permitted . . . allowing the one of the participator computers to send multimedia data"). My analysis above for claim 1 as to these limitations accordingly applies with full force to claim 50.

e. Independent Claim 54

Method Claim 2	Method Claim 54
2. 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	54. A method to sending of multimedia 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

Method Claim 2	Method Claim 54
independent of each other,	independent of each other,
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,
the method including:	the method including:
affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;
affording some of the information to a second of the participator computers via the Internet network, responsive to an	and affording some of the information to a second of the participator computers via the Internet network, responsive to

Method Claim 2	Method Claim 54
authenticated second user identity;	an authenticated second user identity;
permitting at least the first user identity and the second user identity to form a group;	
and permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group,	
wherein at least some of the communications include messages comprising more than one data type, and at least some other of the communications include a pointer that produces a pointer-triggered message on demand.	
	associating the user identities with a respective authorization to communicate multimedia data;
	and sending communications in real time, via an Internet network, from the first participator computer to the second participator computer, if permitted by the authorization of the user identity corresponding to the first participator computer.

127. As shown in the table above, claim 54 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 54, my corresponding analysis for claim 2 applies with full force to claim 54.

128. As to the differences in claim language, claim 54 does not add anything that was not already addressed. Claim 54 is substantially an amalgam of claims 1 and 2. As shown above, claim 54 recites limitations regarding authorization to send multimedia data and sending multimedia data if permitted. These limitations are substantially similar to limitations in claim 1 regarding storing authorization and allowing participator computers to send multimedia data ("storing each said user identity and a respective authorization to send multimedia data"; "if permitted . . . allowing the one of the participator computers to send multimedia data"). My analysis above for claim 1 as to these limitations accordingly applies with full force to claim 54.

f. Independent Claim 58

Method Claim 2	Method Claim 58
2. 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,	58. A method to send multimedia messages via an Internet network, the method including: communicatively connecting a controller computer system, the controller 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, to each of the participator computers responsive to receiving information associated with a respective

Method Claim 2	Method Claim 58
	authenticated user identity,
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,
(additional limitations omitted)	
	wherein the controller computer system sends the multimedia messages by:
	associating with each of the user identities a respective authorization to communicate multimedia data; and
	sending communications in real time, via

Method Claim 2	Method Claim 58
	an Internet network, from a first participator computer to a second participator computers, if permitted solely by the respective authorization of the user identity of the first participator computer.

129. As shown in the table above, claim 58 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 58, my corresponding analysis for claim 2 applies with full force to claim 58.

130. As to the differences in claim language, claim 58 does not add anything that was not already addressed. Claim 58, like claim 54, is substantially an amalgam of claims 1 and 2. Claim 58 recites "communicatively connecting . . . to each of the participator computers responsive to receiving information associated with a respective authenticated user identity." As already explained amply, Roseman discloses a host computer that connects to local (participator) computers for carrying out a virtual conference provided that any required key successfully authenticates a user to enter the virtual conference room.

131. As shown above, claim 58 also recites limitations regarding authorization to communicate multimedia data and communicating multimedia data if permitted. These limitations are substantially similar to limitations in claim

1 regarding storing authorization and allowing participator computers to send multimedia data ("storing each said user identity and a respective authorization to send multimedia data"; "if permitted . . . allowing the one of the participator computers to send multimedia data"). My analysis above for claim 1 as to these limitations accordingly applies with full force to claim 58.

g. Independent Claim 59

Method Claim 2	System Claim 59
2. 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,	59. Computerized human communication arbitrating and distributing system, the system including: a controller computer system, the controller computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other and linked to the controller system through the Internet,
	the controller computer system arbitrating in accordance with predefined rules including a test for an authenticated user identity corresponding to a respective user, which ones of the participator computers can be a member in one of a plurality of groups in which members distribute, in accordance with the predefined rules, the user messages in real time to the respective ones of the participator computers;

Method Claim 2	**System Claim 59**
	wherein at least some of the user messages are multimedia messages;
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	and wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer.
(additional limitations omitted)	

132. As shown in the table above, claim 59 and claim 2 share a large number of identical or substantially identical claim limitations. As to the

underlined portions of claim 59, my corresponding analysis for claim 2 applies with full force to claim 59.

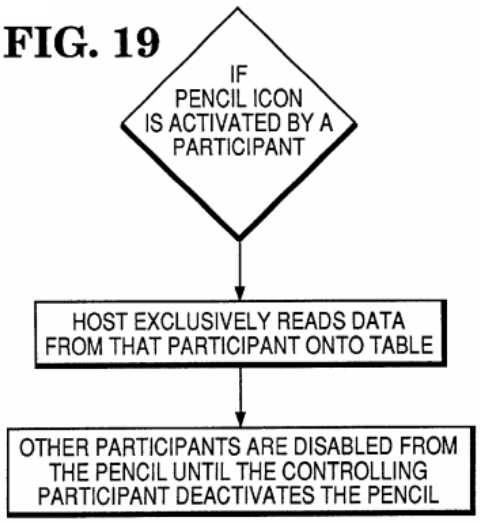
133. As to the differences in claim language, claim 59 does not add anything that was not already addressed. Claim 59 recites that participator computers are "linked to the controller system through the Internet." As explained above, Roseman, alone or with Vetter, discloses local (participator) computers that connect may connect over the Internet to a host computer storing a virtual conference room.

134. Claim 59 also recites limitations regarding (1) arbitrating which participator computers can be a member of a group and (2) distributing messages to participator computers in real time, both in accordance with predefined rules. These limitations are disclosed by Roseman. As already discussed, a conference initiator in Roseman can invite selected users to a virtual conference room and issues keys to each of those users that are checked by the host computer such that only those users may join the conference. Roseman also discloses that the controller software on the host computer uses "predefined rules" for members to distribute "user messages in real time to the respective ones of the participator computers." For example, a conference requester specifies a number of things upon creating a conference, such as "[w]hat rules govern the conduct of the

meeting," "[d]oes the Requester have absolute control of the voice and message interaction among the participants," or "[i]s the meeting a brainstorming free-for-all, where numerous people can speak at once?" (Roseman, 3:52-56.) These predefined rules are further described as follows:

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

(Roseman, 11:38-46 (underlining added).) Roseman therefore discloses predefined rules that may be used to "distribute . . . user messages in real time to the respective ones of the participator computers." A person of ordinary skill in the art would have understood that the rules described above are enforced out through software functionality on the host computer ("controller software on the controller computer"). (*See* Roseman, 1:50-52 ("The host controls many of the events occurring



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

135. Roseman discloses many other examples of "predefined rules" enforced by the host computer that separately and independently satisfy this limitation. For example, Roseman teaches a "pencil" tool that allows a participant to "write" in the conference room. As shown in Figure 19 (to the right), when a participant activates the pencil feature, other participants may not use the pencil until the controlling participant is finished. This provides another example of "predefined rules" for "distribut[ing] . . . user messages in real time to the respective ones of the participator computers," as recited in the claim.

136. Additionally, as described previously, a participant can enter "Whisper Mode" to engage in a private voice conversation with another participant. (Roseman, 9:16-25.) "At this time, the host makes an audio connection between the two whispering parties, and between nobody else. The parties can communicate, until they terminate whisper mode." (Roseman, 9:22-25 (underlining added).)

137. Second, a participant can pass a private textual note to another participant. (Roseman, 9:26-31.) "When the other party sees the note on his picture, as in Figure 12, he can drag it to a private viewing area, double-click it,

and read it. No other people are aware of the passed note." (Roseman, 9:28-31 (underlining added).) The privacy of the note is enforced by software functionality on the host. (Roseman, 15:12-15 & Fig. 17C ("HOST TRANSMITS NOTE TO IDENTIFIED PARTICIPANT ONLY.") (capital letters in original).)

138. In both of these examples, Roseman discloses a means of privately sharing information between two participants of the conference that is not shared with other participants. These features provide a further example of predefined rules that determine what information will be provided to which participant computer – in other words, "distribut[ing], in accordance with the predefined rules, the user messages in real time to the respective ones of the participator computers," as recited in the claim.

139. All of these functionalities involve software running on the host computer, *i.e.* "controller computer system," as claimed. Roseman confirms as much by including an Appendix with "[p]seudo-code usable for programming the host and the local computers," which is "considered self-explanatory" and also "presented in flow-chart format in FIG. 15, et seq." (Roseman, 12:66-13:2.) That pseudo-code describes how the host computer carries out the Whisper Mode, note-passing and pencil features discussed above. (Roseman, 15:6-9 & Fig. 17B

(Whisper Mode), 15:10-13 & Fig. 17C (private note-passing), 15:21-27 & Fig. 19 (pencil).)

h. Independent Claim 64

Method Claim 2	Method Claim 64
2. 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,	64. A method of 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,
wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,	wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives,
wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,	wherein both of the two client software alternatives allow the respective user identities to be recognized by the controller computer system and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications from another of the members, wherein at least some of the communications are received in real time via the Internet network,
and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from	and wherein the at least one of client software alternatives allows the controller computer system to determine whether at least one of the user identities, individually, is censored from

Method Claim 2	Method Claim 64
data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,	data representing at least one of a pointer, video, audio, graphic, and multimedia such that the data that is censored is not presented by the corresponding participator computer,
the method including:	the method including:
affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;	affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;
affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity;	affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity;
permitting at least the first user identity and the second user identity to form a group;	
and permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group,	
wherein at least some of the communications include messages comprising more than one data type, and at least some other of the communications include a pointer that produces a pointer-triggered message on demand.	
	and arbitrating, in accordance with predefined rules including a test for an authenticated user identity, which ones of the participator computers can be a

Method Claim 2	Method Claim 64
	member in one of a plurality of groups in which members distribute, via predefined rules, the messages in real time to the respective ones of the participator computers, wherein at least some of the user messages are multimedia messages.

140. As shown in the table above, claim 64 and claim 2 share a large number of identical or substantially identical claim limitations. As to the underlined portions of claim 64, my corresponding analysis for claim 2 applies with full force to claim 64.

141. As to the differences in claim language, claim 64 does not add anything that was not already addressed. Claim 64 is substantially an amalgam of claim 2 and claim 59. Like claim 59, claim 64 similarly recites limitations regarding (1) arbitrating which participator computers can be a member of a group and (2) distributing messages to participator computers in real time, both in accordance with (or "via") predefined rules. My analysis above for claim 59 therefore applies with full force to claim 64.

3. Claims 3, 5, 7, 11, 13, 15, 21, 24, 28, 32, 36, 40, 44 & 55 (Claims Regarding Data Representing or Comprising Sound/Audio, Video and/or Graphics)

142. Dependent claims 3, 5, 7, 11, 13, 15, 21, 24, 28, 32, 36, 40, 44 and 55 all recite similar limitations regarding whether messages or communications represent or comprise sound/audio, video and/or graphic data and thus will be treated together (claim 55 similarly recites messages containing more than one data type). In particular, these claims recite:

> 3. The method of claim 2, wherein at least one of the messages includes data representing sound.
>
> 5. The method of claim 2, wherein at least one of the messages includes data representing video.
>
> 7. The method of claim 2, wherein at least one of the messages includes data representing sound and video.
>
> 11. The apparatus of claim 10, wherein at least one of the messages includes data representing sound.
>
> 13. The apparatus of claim 10, wherein at least one of the messages includes data representing video.
>
> 15. The apparatus of claim 10, wherein at least one of the messages includes data representing sound and video.
>
> 21. The apparatus of claim 18, wherein the multimedia data comprises graphic data.
>
> 24. The apparatus of claim 18, wherein the multimedia data comprises audio data.

28. The apparatus of claim 18, wherein the multimedia data comprises video data.

32. The apparatus of claim 18, wherein the multimedia data comprises graphic and audio data.

36. The apparatus of claim 18, wherein the multimedia data comprises graphic and video data.

40. The apparatus of claim 18, wherein the multimedia data comprises video and audio data.

44. The apparatus of claim 18, wherein the multimedia data comprises graphic and audio and video data.

55. The method of claim 54, wherein the communications are multimedia messages containing more than one data type.

143. The additional limitations that these claims recite have already been addressed. As explained above for claim 2, Roseman makes clear that at least four types of content (sound, video, graphic, multimedia) may be communicated to conference participants. (Roseman, 7:35-38, 9:16-25, 11:11-16, 11:44-46, 12:34-45 (sound and video), 1:42-46, 3:40-41, 8:1-4 (graphic), Abstract (multimedia).) Each of these claims is therefore fully disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

4. Claims 4, 6, 8, 9 (Claims Regarding Presenting Multimedia Based on Stored Authorization)

144. Claims 4, 6, 8 and 9 each recite "storing, for the first user identity, an authorization associated with presentation of multimedia" and "based on the

authorization, presenting the multimedia at one of the participator computers corresponding to the second user identity." Claim 9 further specifies that the "multimedia compris[es] graphic data."

145. These limitations are substantially similar to limitations discussed above for independent claim 1 ("storing each said user identity and a respective authorization to send multimedia data, the multimedia data comprising graphical data; and if permitted by the user identity corresponding to one of the participator computers, allowing the one of the participator computers to send multimedia data to another of the participator computers."). Thus, my analysis above for claim 10 applies with full force to these limitations. Each of these claims is therefore fully disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

5. Claims 12, 14, 16, 17, 20, 23, 26, 27, 30, 31, 34, 35, 38, 39, 42, 43, 46, 47, 48, 49, 52 & 53 ("Member-Associated Image" Claims)

146. Dependent claims 12, 14, 16, 17, 20, 23, 26, 27, 30, 31, 34, 35, 38, 39 42, 43, 46, 47, 48, 49, 52 and 53 all add the same limitation to the claims from which the respectively depend and thus will be treated together. In particular, each of these claims recites that "**the computer system is further programmed to provide access to a member-associated image**." This limitation is disclosed by Roseman. As I noted previously, 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 (emphasis added); *see also id.*, 7:35-38 ("The pictures of the invitees can be the actual images seen by the each invitee's close-up camera, or can be a photograph taken from the host's memory.").) Each of these claims is therefore fully disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

6. Claims 19, 22, 25, 29, 33, 37, 41, 45 & 51 ("Pointer-Triggered Message" Claims)

147. Dependent claims 19, 22, 25, 29, 33, 37, 41, 45 and 51 all add the same limitation to the claims from which the respectively depend and thus will be treated together. In particular, each of these claims recites that "the computer system is programmed to allow the participator computers to communicate, in real time communications among members of a group, a pointer that produces a pointer-triggered message on demand."[2] This limitation is substantially similar to

[2] Claims 29 and 51 each recite "members of the group," not "members of a group." Claim 45 recites "participator of computers," not "participator computers." These slight differences do not affect the applicability of my analysis to these claims.

limitations addressed above for claim 2, which recites a method of "using a computer system" "permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group, wherein . . . at least some other of the communications include a pointer that produces a pointer-triggered message on demand." My analysis for claim 2 accordingly applies with full force to the limitations added by these claims. Each of these claims is therefore fully disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

7. Claims 56 & 57

148. Claims 56 and 57 both depend from independent claim 54 and are addressed together. As explained below, neither of these claims adds subject matter that has not already been addressed in this declaration.

149. Turning first to claim 56, the claim recites:

> 56. The method of claim 54, wherein the communications contain a pointer, and that pointer is utilized on the second participator computer to request the sending of data associated with the pointer from another computer.

150. The limitations added by this claim are disclosed by Roseman. In particular, as explained previously in connection with claim 2, Roseman discloses document sharing and note passing features that satisfy this limitation. 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).)

151. Similarly, as to Roseman's note-passing feature, 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.

152. As explained previously, to the extent there is any question as to whether Roseman sufficiently discloses a "pointer" that is "utilized on the second

participator computer to request the sending of data associated with the pointer from another computer," this limitation would be obvious over Roseman in view of Pike for the reasons previously mentioned. Pike discloses a pointer in the form of a URL, which could be used to download the document content from the host computer over the Internet in real-time when the URL in invoked. In fact, this limitation is little more than a recitation of basic and known 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.").)

153. Turning to claim 57, the claim recites:

> 57. The method of claim 54, wherein some of the communications are multimedia messages containing more than one data type and some of the communications contain a pointer, and that pointer is utilized on the second participator computer to request the sending of data associated with the pointer from another computer.

154. Claim 57 is substantially an amalgam of claim 55 and claim 56. Claim 55 recites in part, "the communications are multimedia messages containing more than one data type" and claim 56, as shown above, recites basically the remainder of claim 57 addressing communications containing a pointer. Thus, for

the reasons discussed above as to each of these claims, claim 57 is fully disclosed by Roseman in view of Rissanen, Vetter, Pike and Lichty.

155. Finally, in my opinion, the disclosures of Roseman, Rissanen, Vetter, Pike and Lichty 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.

156. I also rely upon Vetter, Rissanen, Pike and Lichty 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, 13:5-14). 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 "[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" 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 as 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.

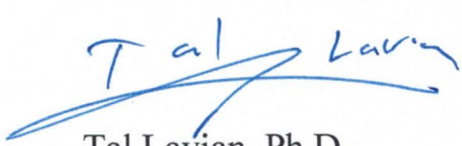
V. CONCLUSION

157. 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 '552 patent claims at issue and/or offer testimony in support of this Declaration.

158. 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: June 3, 2016

Respectfully submitted,



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 25 years of experience
- Co-author on over 25 scientific publications, journal articles, and peer-reviewed papers
- Named inventor on over 80 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; C; C++; 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

LITIGATION SUPPORT SERVICES

- Expert witness in numerous USPTO PTAB – Inter Partes Review (IPR) and CBM cases
- Expert witness in Federal courts and the ITC (over 30 cases)
- Expert reports, depositions, and courtroom testimonies
- Skilled articulation of technical material for both technical and non-technical audiences
- Product and technology analysis, patent portfolios, claim charts, patentability research
- Litigation support and technology education in patent disputes
- Past cases involved Cisco, Juniper, HP, Ericsson, Microsoft, Google, Samsung and Apple

ACCOMPLISHMENTS

- Selected as Principal Investigator for three US Department of Defense (DARPA) projects
- Led research project on networking computation for the US Air Force Research Lab (AFRL)
- Led and developed the first network resource scheduling service for grid computing
- Led 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 80 patents; over 50 prosecuted *pro se* in front of the USPTO
- Created and chaired Nortel Networks' EDN Patent Committee
- Current IEEE Senior Member

PROFESSIONAL EXPERIENCE

University of California, Berkeley, Berkeley, CA 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

Telecomm Net Consulting, Inc. (Innovations-IP) Sunnyvale, CA 2006-Present

Principal Scientist

- Consulting in the areas of network communications, telecommunications, Internet protocols, and smartphone mobile wireless devices

- Providing architecture and system consultation for software projects relating to computer networks, mobile wireless devices, Internet web technologies
- Acting as an expert witness in network communications patent infringement lawsuits

VisuMenu, Inc. – Sunnyvale, CA 2010-Present

Co- Founder and Chief Technology Officer (CTO)

- Design and develop architecture of visual IVR technologies for smartphones and wireless mobile devices in the area of network communications
- Design crawler/spider system for IVR / PBX using Asterisk, SIP and VoIP
- Deploy the system as cloud networking and cloud computing utilizing Amazon Web Services (EC2, S3, VPC, DNS, and RDS)

Ixia, Santa Clara, CA 2008-2008

Communications Consultant

- Researched and developed advanced network communications testing technologies:
  • IxNetwork/IxN2X — tests IP routing and switching devices and broadband access equipment. Provides 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 models high-volume video, data, and voice subscribers and servers to test real-world performance of multiservice delivery and security platforms.
  • IxCatapult — emulates a broad range of wireless access and core protocols to test wireless components and systems. When combined with IxLoad, provides an end-to-end solution for testing wireless service quality.
  • IxVeriWave — employs 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 — provides simple, comprehensive lab automation to help test engineering teams create, organize, catalog, and schedule execution of tests.

Nortel Networks, Santa Clara, CA 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
- Developed 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
  - Open Platform: project for the US Air Force Research Laboratory (AFRL) 2005
  - Network Resource Orchestration for Web Services Workflows 2004-2005
  - Proxy Study between Web/Grids Services and Network Services 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), 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)
- 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 (present) – 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 8,688,796** Rating system for determining whether to accept or reject objection raised by user in social network
- **US 8,572,303** Portable universal communication device
- **US 8,553,859** Device and method for providing enhanced telephony
- **US 8,548,131** Systems and methods for communicating with an interactive voice response system
- **US 8,537,989** Device and method for providing enhanced telephony
- **US 8,341,257** Grid proxy architecture for network resources
- **US8,161,139** Method and apparatus for intelligent management of a network element
- **US 8,146,090** Time-value curves to provide dynamic QoS for time sensitive file transfer
- **US 8,078,708** Grid proxy architecture for network resources
- **US 7,944,827** Content-aware dynamic network resource allocation
- **US7,860,999** Distributed computation in network devices
- **US 7,734,748** Method and apparatus for intelligent management of a network element
- **US 7,710,871** Dynamic assignment of traffic classes to a priority queue in a packet forwarding device
- **US 7,580,349** Content-aware dynamic network resource allocation
- **US 7,433,941** Method and apparatus for accessing network information on a network device
- **US 7,359,993** Method and apparatus for interfacing external resources with a network element
- **US 7,313,608** Method and apparatus for using documents written in a markup language to access and configure network elements
- **US 7,260,621** Object-oriented network management interface

- **US 7,237,012** Method and apparatus for classifying Java remote method invocation transport traffic
- **US 7,127,526** Method and apparatus for dynamically loading and managing software services on a network device
- **US7,047,536** Method and apparatus for classifying remote procedure call transport traffic
- **US7,039,724** Programmable command-line interface API for managing operation of a network device
- **US6,976,054** Method and system for accessing low-level resources in a network device
- **US6,970,943** Routing architecture including a compute plane configured for high-speed processing of packets to provide application layer support
- **US6,950,932** Security association mediator for Java-enabled devices
- **US6,850,989** Method and apparatus for automatically configuring a network switch
- **US6,845,397** Interface method and system for accessing inner layers of a network protocol
- **US6,842,781** Download and processing of a network management application on a network device
- **US6,772,205** Executing applications on a target network device using a proxy network device
- **US6,564,325** Method of and apparatus for providing multi-level security access to system
- **US6,175,868** Method and apparatus for automatically configuring a network switch
- **US6,170,015** Network apparatus with Java co-processor
- **US 8,619,793** Dynamic assignment of traffic classes to a priority queue in a packet forwarding device
- **US 8687,777** Systems and methods for visual presentation and selection of IVR menu
- **US 8,681,951** Systems and methods for visual presentation and selection of IVR menu

- **US 8,625,756** Systems and methods for visual presentation and selection of IVR menu
- **US 8,594,280** Systems and methods for visual presentation and selection of IVR menu
- **US 8,548,135** Systems and methods for visual presentation and selection of IVR menu
- **US 8,406,388** Systems and methods for visual presentation and selection of IVR menu
- **US 8,345,835** Systems and methods for visual presentation and selection of IVR menu
- **US 8,223,931** Systems and methods for visual presentation and selection of IVR menu
- **US 8,160,215** Systems and methods for visual presentation and selection of IVR menu
- **US 8,155,280** Systems and methods for visual presentation and selection of IVR menu
- **US 8,054,952** Systems and methods for visual presentation and selection of IVR menu
- **US 8,000,454** Systems and methods for visual presentation and selection of IVR menu
- **EP 1,905,211** Technique for authenticating network users
- **EP 1,142,213** Dynamic assignment of traffic classes to a priority queue in a packet forwarding device
- **EP 1,671,460** Method and apparatus for scheduling resources on a switched underlay network
- **CA 2,358,525** Dynamic assignment of traffic classes to a priority queue in a packet forwarding device

Patent Applications Published and Pending:
(Not an exhaustive list)

- **US 20140105025** Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device
- **US 20140105012** Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device
- **US 20140012991** Grid Proxy Architecture for Network Resources
- **US 20130080898** Systems and Methods for Electronic Communications
- **US 20130022191** Systems and Methods for Visual Presentation and Selection of IVR Menu
- **US 20130022183** Systems and Methods for Visual Presentation and Selection of IVR Menu
- **US 20130022181** Systems and Methods for Visual Presentation and Selection of IVR Menu
- **US 20120180059** Time-Value Curves to Provide Dynamic QOS for Time Sensitive File Transfers
- **US 20120063574** Systems and Methods for Visual Presentation and Selection of IVR Menu
- **US 20110225330** Portable Universal Communication Device
- **US 20100220616** Optimizing Network Connections
- **US 20100217854** Method and Apparatus for Intelligent Management of a Network Element
- **US 20100146492** Translation of Programming Code
- **US 20100146112** Efficient Communication Techniques
- **US 20100146111** Efficient Communication in a Network
- **US 20090313613** Methods and Apparatus for Automatic Translation of a Computer Program Language Code
- **US 20090313004** Platform-Independent Application Development Framework
- **US 20090279562** Content-aware dynamic network resource allocation
- **US 20080040630** Time-Value Curves to Provide Dynamic QoS for Time Sensitive File Transfers
- **US 20070169171** Technique for authenticating network users
- **US 20060123481** Method and apparatus for network immunization
- **US 20060075042** Extensible Resource Messaging Between User Applications and Network Elements in a Communication Network

- **US 20050083960** Method and Apparatus for Transporting Parcels of Data Using Network Elements with Network Element Storage
- **US 20050076339** Method and Apparatus for Automated Negotiation for Resources on a Switched Underlay Network
- **US 20050076336** Method and Apparatus for Scheduling Resources on a Switched Underlay Network
- **US 20050076173** Method And Apparatus for Preconditioning Data to Be Transferred on a Switched Underlay Network
- **US 20050076099** Method and Apparatus for Live Streaming Media Replication in a Communication Network
- **US 20050074529** Method and apparatus for transporting visualization information on a switched underlay network
- **US 20040076161** Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device
- **US 20020021701** Dynamic Assignment of Traffic Classes to a Priority Queue in a Packet Forwarding Device
- **WO 2007/008976** Technique for Authenticating Network Users
- **WO 2006/063052** Method and apparatus for network immunization
- **WO2000/0054460** Method and apparatus for accessing network information on a network device

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: AData 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: AnArchitecture 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?