**2018-1400, -1401, -1402, -1403, -1537, -1540, -1541**

# United States Court of Appeals for the Federal Circuit

FACEBOOK, INC.,

*Appellant,*

v.

WINDY CITY INNOVATIONS, LLC,

*Cross-Appellant.*

*Appeal from the United States Patent and Trademark Office, Patent Trial and Appeal Board, in Case Nos. IPR2016-01156, IPR2016-01157, IPR2016-01158, IPR2016-01159*

## APPELLANT'S OPENING BRIEF

COOLEY LLP
HEIDI L. KEEFE (hkeefe@cooley.com)
MARK R. WEINSTEIN (mweinstein@cooley.com)
ANDREW C. MACE (amace@cooley.com)
3175 Hanover Street
Palo Alto, CA 94304
(650) 843-5000 (telephone)
(650) 849-7400 (facsimile)
*Counsel for Petitioner-Appellant*

# CERTIFICATE OF INTEREST

Counsel for Appellant Facebook, Inc. certifies the following:

1. The full name of every party or amicus represented by me is: **Facebook, Inc.**

2. The name of the real party in interest (if the party named in the caption is not the real party in interest) represented by me is: **The party named in the caption, Facebook, Inc., is the real party in interest.**

3. All parent corporations and any publicly held companies that own 10 percent or more of the stock of the party or amicus curiae represented by me are: **There are no such corporations or companies.**

4. The names of all law firms and the partners or associates that appeared for the party or amicus now represented by me in the trial court or agency or are expected to appear in this court and who are not already listed on the docket for the current case:

   **Cooley LLP: Andrew C. Mace**

5. The following cases are pending in a court or agency and will directly affect or be directly affected by this court's decision in the pending appeal:

   ***Windy City Innovations, LLC v. Facebook, Inc.*, Case No. 4:16-cv-01730-YGR (N.D. Cal.)**

   ***Windy City Innovations, LLC v. Facebook, Inc.*, Case Nos. 2018-1543, 2018-1544, 2018-1545 (Fed. Cir.), in which the patent owner Windy City appealed from IPR proceeding nos. IPR2016-01067, IPR2016-01141 and IPR2016-01155. The appeal was dismissed on May 14, 2018.**

Dated: May 21, 2018

By: /s/ Heidi L. Keefe
Heidi L. Keefe
Cooley LLP

## Table of Contents

**Page**

**Table of Contents**
**(continued)**

**Page**

# TABLE OF AUTHORITIES

**Page(s)**

## CASES

## REGULATIONS

## STATEMENT OF RELATED CASES

In accordance with Federal Circuit Rule 47.5, counsel for Appellant Facebook, Inc. ("Facebook") states:

1. Facebook is unaware of any other appeal in or from IPR proceeding Nos. IPR2016-01156, IPR2016-01157, IPR2016-01158, IPR2016-01159, IPR2017-00659 and IPR2017-00709 in this Court or any other appellate court.

2. The following cases are pending and may directly affect or be directly affected by the Court's decision in the pending appeal:

(1) *Windy City Innovations, LLC v. Facebook, Inc.*, Case No. 4:16-cv-01730-YGR (N.D. Cal.) ("District Court Litigation"). The District Court Litigation is a currently ongoing patent suit in which U.S. Patent Nos. 8,407,356, 8,458,245, 8,473,552 and 8,694,657 are asserted by the patent owner/appellee Windy City.

(2) *Windy City Innovations, LLC v. Facebook, Inc.*, Case Nos. 2018-1543, 2018-1544, 2018-1545 (Fed. Cir.), in which the patent owner Windy City appealed from IPR proceeding nos. IPR2016-01067, IPR2016-01141 and IPR2016-01155. The appeal was dismissed on May 14, 2018.

## JURISDICTIONAL STATEMENT

Facebook appeals the Final Written Decisions by the Patent Trial and Appeal Board ("Board" or "PTAB") in four *inter partes* review proceedings conducted pursuant to 35 U.S.C. §§ 6 and 318(a) for U.S. Patent Nos. 8,458,245 ("'245 patent"), 8,694,657 ("'657 patent"), 8,473,552 ("'552 patent"), and 8,407,356 ("'356 patent") (IPR2016-01156, IPR2016-01159, IPR2016-01158, and IPR2016-01157, respectively). The Board issued Final Written Decisions in each proceeding, all dated December 6, 2017, concluding that Facebook had not shown by a preponderance of the evidence that the following claims were unpatentable:

(1) claims 1-15, 17-19 and 22-25 of the ’245 patent;

(2) claims 203, 209, 215 and 221 of the ’657 patent;

(3) claims 1, 4, 6, 8, 9 and 18-58 of ’552 patent; and

(4) claims 14 and 33 of the ’356 patent.[1]

Facebook filed timely notices of appeal on January 10, 2018. This Court has subject matter jurisdiction pursuant to 35 U.S.C. § 141(c) and 28 U.S.C. § 1295(a)(4)(A).

## INTRODUCTION

All four of the patents in the appeal involve communication on the Internet using acknowledged old technology like chat rooms. All of the appealed claims are unpatentable when a proper understanding of the primary prior art reference, Roseman, is applied under a proper claim construction. Each appealed final decision presents slightly different issues regarding the mistakes committed by the Board, so each is discussed in detail in turn below.

[1] The Final Written Decisions for the ’657, ’552, and ’356 patents also found various claims are unpatentable. Facebook does not appeal those findings.

## STATEMENT OF THE ISSUES

1. Did the Board err in its Final Written Decision in IPR2016-01156 finding that claims 1-15, 17-19 and 22-25 of the ’245 patent were not unpatentable as obvious under 35 U.S.C. § 103(a) over the instituted grounds?

2. Did the Board err in its Final Written Decision in IPR2016-01159 finding that claims 203, 209, 215 and 221 of the ’657 patent were not unpatentable as obvious under 35 U.S.C. § 103(a) over the instituted grounds?

3. Did the Board err in its Final Written Decision in IPR2016-01158 finding that claims 1, 4, 6, 8, 9 and 18-58 of the ’552 patent were not unpatentable as obvious under 35 U.S.C. § 103(a) over the instituted grounds?

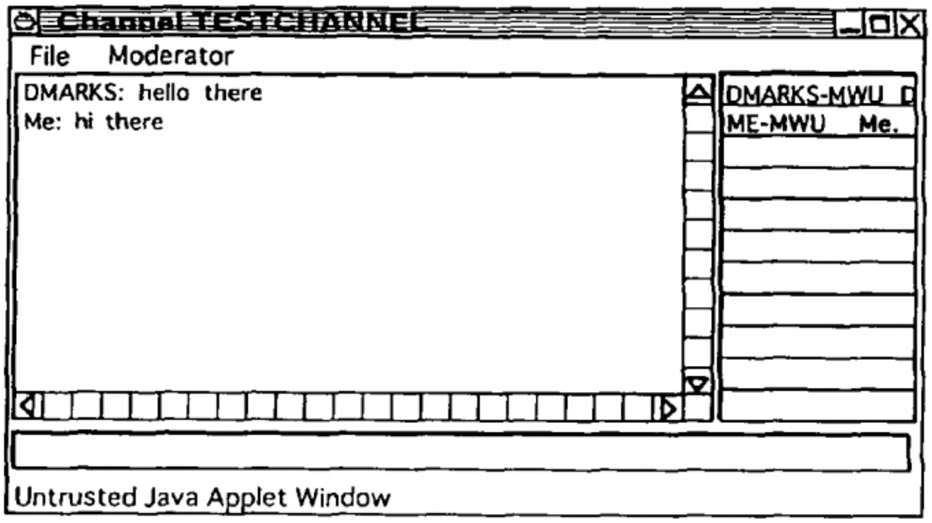
4. Did the Board err in its Final Written Decision in IPR2016-01157 finding that claims 14 and 33 of the ’356 patent were not unpatentable as obvious under 35 U.S.C. § 103(a) over the instituted grounds?

## STATEMENT OF THE CASE AND FACTS

### I. THE CHALLENGED PATENTS

The four patents at issue here share a common specification and claim priority to a patent application filed on April 1, 1996. (Appx226, Appx263, Appx299, Appx337.) The patents, entitled “Real Time Communications System” or “Communications System,” disclose methods for allowing users to communicate over a computer-based network such as the Internet. In one embodiment shown in Figure 14, users communicate through a “chat room”-like user interface:

FIG. 14



DMARKS: hello there
Me: hi there

(Appx237, Fig. 14.)[2] The chat room window shown in Figure 14 allows two users (*i.e.*, the viewing user and DMARKS) to communicate with each other. The window "has three regions: the bottom region, where responses are entered; the largest region, where a transcript of the communication is followed; and the rightmost region, which lists the group's current members." (Appx254, 9:32-35.) Whenever a member of the group types a message into the window, the message is transmitted to a central "controller computer" **5**, which in turn routes the message to the "participator computers" **4** of the other members. (Appx254, 9:45-52.) Aside from text, users can communicate other types of data including multimedia content. (Appx252, 5:36-41; Appx250, 2:15-17 ("It is still a further object of the present

[2] Because all four patents share a common specification, where the patents are discussed collectively, a citation is provided to the '245 patent for convenience.

invention to provide a chat capability suitable for handling graphical, textual, and multimedia information in a platform independent manner.”).)

The specification freely acknowledges that chat room communications were not new. The Background of the Invention acknowledges that existing “[c]hat room communications can be mere text, such as that offered locally on a file server, or can involve graphics and certain multimedia capability, as exemplified by such Internet service providers as America On Line.” (Appx250, 1:41-45.) The specification nevertheless complains that existing chat services such as America Online were not adaptable to the Internet “at least in part because Internet [sic] was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications.” (Appx250, 1:46-50.)

Although this complaint regarding the Internet is untrue (*see e.g.*, Appx432-433 (discussing prior art Vetter reference)), the specification purports to overcome the supposed limitations of the prior art through a computer system involving a “controller computer” linked to a plurality of “participator computers” by a “connection such as the Internet.” (Appx250, 2:21-27; Appx228, Fig. 1.) Two features of the system described in the specification are relevant to the issues in this appeal: **(1)** the ability to handle “out-of-band” multimedia information (information that a receiving computer may be unable to present), and **(2)** the ability to control the dissemination of information among participator computers (a technique the patents generally refer to as "censorship" of content).

### A. Handling "Out-of-Band" Multimedia Information

The specification acknowledges that, from time to time, a member may receive a communication that includes multimedia content (such as an image) that its participator computer may be unable to present. The specification refers to this non-presentable information as "out-of-band" multimedia information. (Appx253, 7:34-40.) To address this scenario, the participator computer first "tests whether [it] is an internally handlable [sic] multimedia type." (Appx253, 7:36-38; Appx233, Fig. 6 (Step 102).) If it is, the image may be displayed or other actions may be taken. (Appx233, Fig. 6 (Step 114); Appx253, 7:44-50.)

But if the participator computer cannot internally handle the multimedia type, the computer attempts to locate a suitable "**agent**" for presenting the multimedia information. (Appx253, 7:38-43.) If the participator computer locates such an agent, it uses it to present the multimedia information to the user. (Appx253, 7:41-43 ("If the agent is found in Block **106** [of Figure 6], the logic flows to Block **110**, which invokes the agent with a data reference to present the data.").)

All of the issues surrounding the present appeal with respect to the '245 patent (IPR2016-01156) revolve around this "out-of-band" feature. All challenged independent claims of the '245 patent (*i.e.* claims 1, 7, and 19) recite a computer apparatus in which a "second participator computer" receives a communication via the Internet, and each of these claims attempts to capture this "out-of-band" feature. With respect to claim 1, it recites the following step:

> the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication, and otherwise presenting the communication independent of the first of the independent participator computers and the computer

(Appx260, 21:54-63 (Claim 1).) Independent claims 7 and 19 recite substantially the same step. (Appx260, 22:39-42 (Claim 7); Appx261, 23:36-44 (Claim 19).)

The Board's decision on the '245 patent rested entirely on its decision that the prior art did not disclose the step of internally determining whether or not the second of the participator computers can present the communication. As explained in detail below, the Board's decision on this point is erroneous and lacks support in the evidentiary record.

### B. "Censorship" of Content

The specification also discloses techniques for controlling what is communicated among the members of a group. As the specification explains, the software in the controller computer **3** uses "identity tokens," or pieces of information associated with user identity, to arbitrate or moderate what is said in a group. (Appx253, 7:56-60, 8:6-14, 8:36-38.) As the specification further explains:

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system **1** by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.
>
> With regard to controlling communications in a group (which is in essence a collection of user identities), control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages.

(Appx253, 8:36-50.) All of the issues in this appeal relating to the other three patents ('657, '552, '356) revolve around limitations generally relating to the "censorship" feature of the alleged invention. As Facebook will explain below, the Board's decision on these points is based on an erroneously narrow claim interpretation.

## II. THE RELEVANT PRIOR ART CITED IN THE IPR PETITIONS

Facebook filed IPR petitions against the '245, '657, '552, and '356 patents in December 2016, challenging various claims as obvious based on several prior art references. The Board instituted IPR on all claims challenged in these petitions.

### A. Roseman

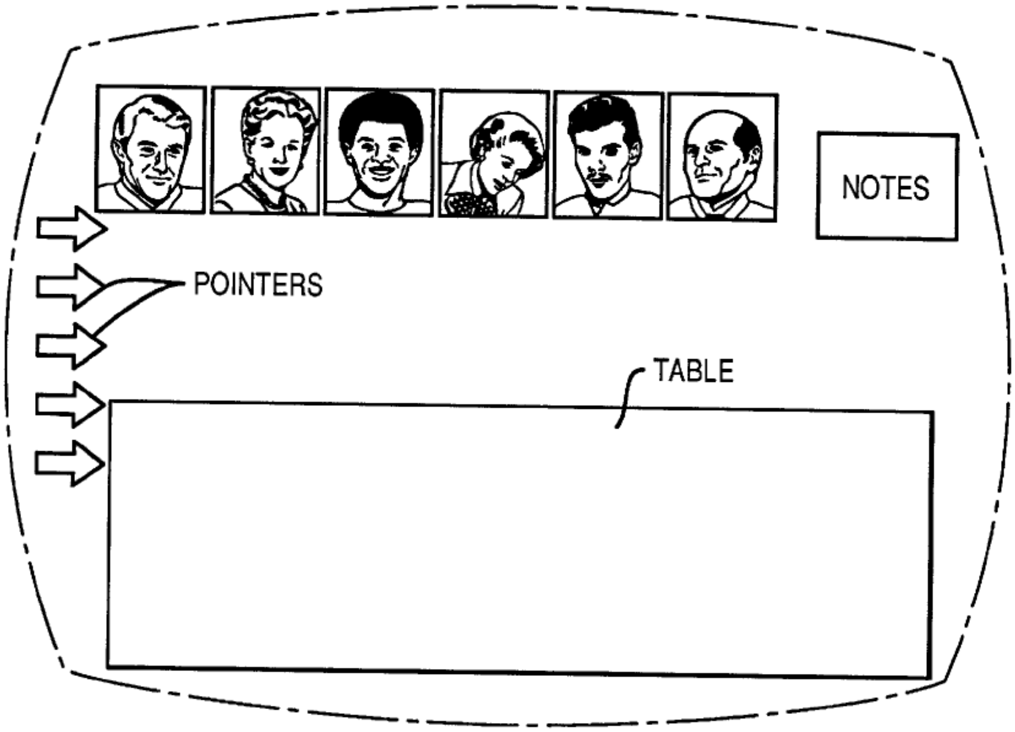
Facebook's petitions all cited U.S. Patent No. 6,608,636 to Robert D. Roseman ("Roseman") as the base reference disclosing the majority of the claim limitations across all four patents. Roseman, entitled "Server Based Virtual Conferencing," discloses a system for allowing users to collaborate in real time over a computer network. (Appx1195-1227.)

Roseman, using the real-world analogy of a physical conference, discloses "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." (Appx1219, 1:28-31.) This virtual conferencing system "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." (Appx1219, 1:20-23.)

Each conference participant has its own "local computer," which communicates with a server that Roseman calls a "host computer." (Appx1219, 1:34-41, 2:64-65.) "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)." (Appx1219, 1:37-41; *see also* Appx1220, 3:14-19.)

A user in Roseman can create 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. (Appx1220, 3:22-56.) Once the parameters of the virtual conference are specified, the host computer "creates the conference room. The host does this by creating a common image, such as that shown in FIG. 9." (Appx1222, 7:30-32.)

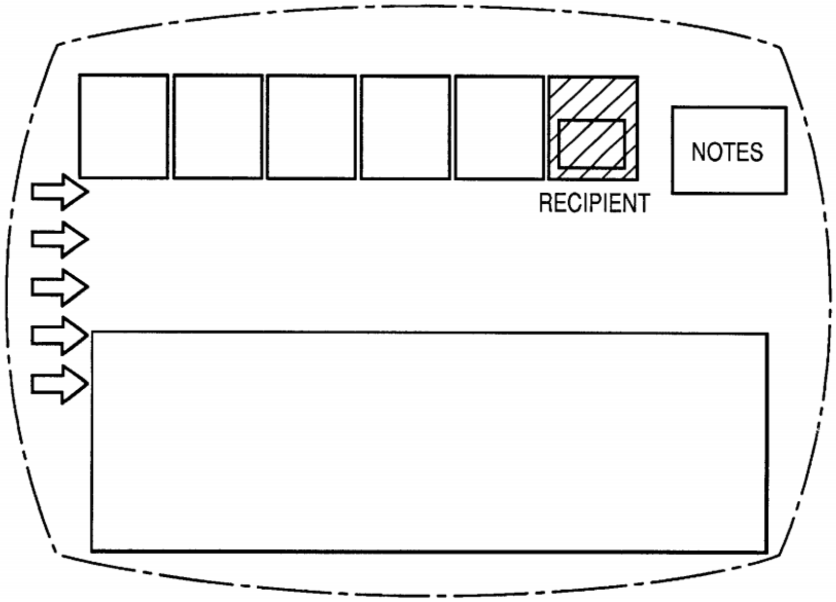
FIG. 9



(Appx1204, Fig. 9.) The virtual conference room shown in Figure 9 above "includes a picture of each invitee, a 'table,' and the room decor." (Appx1222, 7:32-34.) "The pictures of the invitees can be the actual images seen by the [sic] each invitee's closeup camera, or can be a photograph taken from the host's memory." (Appx1222, 7:35-38.)

The virtual conference room provides a number of different ways for conference participants to communicate with each other. For example, Roseman discloses a note-passing feature in which a first participant can send a private note to a second participant. The first participant simply drags a note onto the picture of another participant in the virtual conference room, and the note is transmitted to that participant. (Appx1223, 9:26-31; Appx1205, Fig. 12.) The receiving participant, in turn, sees the note on top of his or her picture as shown in Figure 12:

FIG. 12



(Appx1205, Fig. 12.) The recipient can then drag the note from the virtual conference room into a private viewing area on the recipient's local computer, and then double-click the note to privately view it. (Appx1223, 9:28-31.)

A participant can also share information in a conference by dragging a document (data file) from his local computer onto the "table" of the virtual conference room. (Appx1224, 11:18-22.) Figures 10 and 11 of Roseman illustrate how this feature works:

FIG. 10

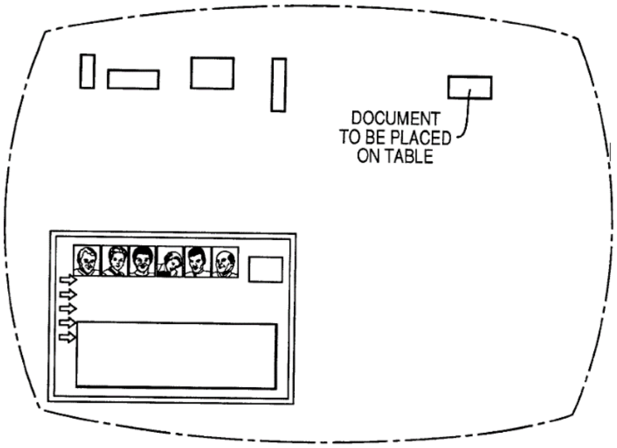
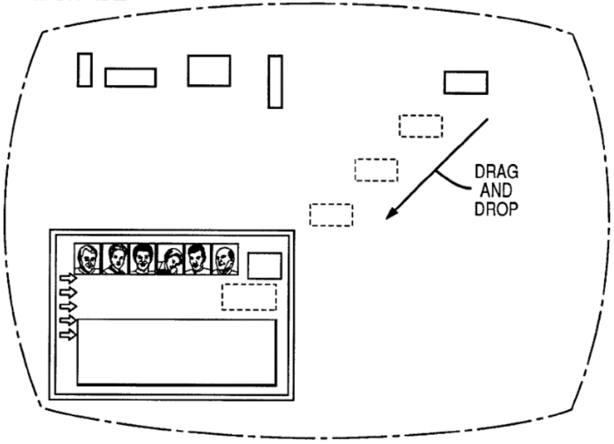


FIG. 11



(Appx1204-1205, Figs. 10 & 11.) As explained in Roseman:

> Each invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it. To place a document on the table, an Invitee performs a "drag-and-drop." That is, the invitee shrinks the window of the conference room to the size shown in FIG. 10. The private work area outside the window displays the icons representing the invitee's programs and data files. The Invitee drags an icon onto the table, as shown in FIG. 11, and double-clicks (or actuates) the icon. The icon blooms into an image dictated by the type of file which the icon represents (graphic, text, etc.)

(Appx1222, 8:1-13.) Similar to the note-passing feature above, a participant who receives a document can perform a "drag-and-drop" operation to view the document outside the virtual conference room. (Appx1212, Fig. 16C.)

Roseman also discloses various ways of controlling the conduct of conference room participants. For example, a host can act as a moderator by placing a limit on the total time each participant can speak, or by requesting a vote as to whether a participant should be permitted to continue speaking. (Appx1224, 12:29-45.) Conference rooms can also specify that certain procedures must be followed before allowing a participant to speak. (Appx1224, 11:38-47.)

Roseman also discloses a security mechanism in which users must be invited and have an appropriate "key" to enter the conference room. (Appx1223, *e.g.*, 9:34-55, 10:61-64 ("To open a door with a key, the user drops the key onto the door lock. If the key is valid and the user has the authority to use the key, the door opens and the user is admitted to the room.").) Roseman also discloses a database that stores the keys for the conference room. (Appx1223, 9:49-50.)

### B. Additional References Relevant to the '245 Patent

As explained previously, the Board upheld the challenged claims of the '245 patent (IPR2016-01156) based entirely on the "out-of-band" feature of claims 1, 7 and 19, reciting a second participator computer that "**internally determines**" whether a communication can be presented, and if not, "**obtains an agent**" for presenting the communication. With respect to this feature, Facebook's IPR petition cited Roseman in combination with two additional references – Pike and Westaway.[3]

### 1. Pike

*Using Mosaic*, by Mary Ann Pike et al. ("Pike"), is a 1994 textbook describing NCSA Mosaic, one of the early browser programs for accessing the World Wide Web. (Appx1246-1397.)

From time to time, a user may encounter content on the Internet that cannot be displayed by the user's web browser software. Pike addresses this scenario by describing the ability for the web browser to use external software viewers to display content that the web browser itself cannot present. (Appx428 (citing Appx1320-1321).) As Pike explains:

> Mosaic is a *multimedia application*, which means that you can view files containing a number of different types of media—pictures, sound, and animation. While Mosaic for Windows displays normal Web documents, you may want to obtain additional software to handle things such as pictures, sounds, and animations (movies).

(Appx1361 (under "Viewing Multimedia Files") (italics in original); *see also* Appx1320 (under "Multimedia Viewers").)

[3] Facebook's IPR petitions as to the '657, '552 and '356 patents also cited to Pike but for an entirely different reason – to show that the Uniform Resource Locators (URLs) in Pike disclosed the "pointer" and "pointer-triggered" limitations in the challenged claims of those patents. (Appx5472-5473; Appx3720-3721; Appx2131-2132.) Because the Board did not find any deficiency with respect to these limitations, or Pike's disclosure of them, they need not be further discussed.

Pike lists several examples of such viewer software programs, including for viewing PostScript documents, GIF and JPEG graphic images, MPEG movies, and audio files. (Appx428-429 (citing Appx1321).) Once an external viewer has been installed, it is invoked automatically to view the files:

> After you have a viewer installed and Mosaic knows where to find it and what type of files it displays, you can load files of that type and Mosaic automatically starts the viewer to display them.

(Appx1361 (under "Viewing Multimedia Files").)

### 2. Westaway

Facebook also cited to U.S. Patent No. 5,226,176 to William D. Westaway et al. ("Westaway"), which discloses a technique for automatically obtaining a software agent. (Appx1398-1405.) Westaway describes a method for obtaining software over a network "[i]n the event an agent requires certain software for execution, and the software is not available on the agent's local hard disk drive or internal memory." (Appx429 (citing Appx1403, 1:24-27).)

Facebook's IPR petition cited Westaway in combination with Pike in the event the Board narrowly interpreted the "**obtaining an agent**" step of claims 1, 7, and 19 to require that the second participator software obtain the agent *automatically* and without any user intervention. (Appx459.) Because this issue was not addressed or relied upon by the Board in its Final Written Decision on the '245 patent, no further discussion of Westaway is warranted.

### C. Additional References Relevant to the ’657 and ’552 Patent “Censorship” Features

#### 1. Lichty

For certain challenged claims of the ’657 and ’552 patents, Facebook relied on Roseman in combination with a textbook by Tom Lichty, *The Official America Online for Macintosh Membership Kit & Tour Guide* (2nd ed. 1995) (“Lichty”). Lichty describes aspects of a popular network-based service known as “America Online.” (Appx1409-1529; Appx5473.)

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. (Appx5473 (citing Appx1479-1505).) One such feature allows an America Online member to block communications from specified other members. Lichty explains that “[i]f you wish to exclude a member’s comments (or those of all of the members in a 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.” (Appx1496; Appx5473.) A member can also use the “Ignore” feature to block communications from another member who has become disruptive. (Appx1515 (definition of “Ignore”).)[4] As explained in detail below, Lichty discloses claimed “censorship”

[4] The IPR petitions as to the ’245, ’657, ’552, and ’356 patents also cited the Rissanen and Vetter references, respectively, for the claimed “database” and

features in the ’657 patent under a proper interpretation of the claims. (For the ’552 and ’356 patents, the disclosures of Roseman, not Lichty, are at issue.)

## III. THE IPR PROCEEDINGS

### A. The ’245 Patent (IPR2016-01156)

On December 6, 2017, the Board issued a Final Written Decision finding that Facebook had not shown by a preponderance of the evidence that the challenged claims of the ’245 patent (1-15, 17-19, and 22-25) were unpatentable. (Appx34.) The Board’s decision rested on its conclusion that the prior art did not disclose the limitation of independent claim 1, “**the second of said participator computers internally determines whether or not the second of the participator computers can present the communication**.” (Appx25-32.)

Facebook’s IPR petition explained in detail why this limitation would have been obvious to a person of ordinary skill in the art. Facebook acknowledged that Roseman itself did not disclose the step of internally determining whether or not the participator computer could present the communication, but explained that this feature was disclosed by Pike and Westaway. (Appx457-463; Appx1155-1160, ¶¶93-100.) The Board agreed in its Institution Decision that Pike discloses this

communication via the “Internet.” Because the Board did not find any deficiency in Rissanen and Vetter for any of the limitations for which they were cited, those references need not be discussed in detail.

feature (Appx560-561), and did not retreat from that position in its Final Written Decision.

Facebook also explained why a person of ordinary skill in the art would have found it obvious to combine Roseman with Pike and Westaway. Among other things, Facebook pointed to the well-known problem of receiving a document that cannot be opened for lack of the software needed to view it:

> Persons of ordinary skill in the art would have appreciated that in any computing system, it was routine that a user could receive a document from someone else but be unable to open or access it because the user lacked the correct software (or perhaps even the correct version of the software). Anyone who attempted to read a Microsoft Word document using WordPerfect (or vice versa), without a document format converter, would have been aware of this problem. This problem was exacerbated by wide area computer networks such as the Internet, which made it easier to exchange different types of documents from a rapidly expanding number of Internet users.
>
> These considerations would have been particularly applicable to Roseman. As noted, the system of Roseman allows a meeting participant to "drag-and-drop" an icon of a document onto the table of the virtual conference room. Roseman places no limits on what that document could be; it could be any file stored on the participant's local computer.

(Appx1160-1162, ¶¶102-103; Appx462-463.) Facebook also explained that "[i]t would have been abundantly obvious to one of ordinary skill in the art that the performance and execution of the virtual conference of Roseman could be improved using the viewer software applications described in Pike, to be obtained using the software retrieval techniques taught by Westaway." (Appx1161-1162, ¶103; Appx463.)

The Board nevertheless rejected the combination of Roseman, Pike and Westaway with respect to the "internally determines" step. Notably, the Board never disputed that Pike actually discloses a participator computer that "**internally determines**" whether a communication can be presented, and if not, "**obtains an agent**" for presenting the communication.

The Final Written Decision instead rejected the combination based on a different rationale – that the teachings in Pike were not applicable to the system of Roseman. The gist of the Board's position was that the host (server) computer of Roseman performs all of the processing required for display of content at the participant local computers. Because a local computer need not perform ***any*** processing to display content (under the Board's reasoning), the local computer would have no need for the external agent/viewer capability disclosed in Pike.

In particular, the Board asserted that the system of Roseman "processes images at the host, not the local computers," and that "[t]he most logical reading of Roseman is that its local computers already have software sufficient to render the common image that the host provides to them." (Appx29.) The Board further asserted:

> At most, Petitioner's contentions establish that a skilled artisan applying Pike's and Westaway's teachings to

> Roseman's system would have modified Roseman's host to seek out appropriate software to process communications it otherwise could not present. Petitioner has not shown that a skilled artisan would have further modified Roseman's system to move this processing from the host to each individual local computer and has not provided any persuasive reason to make such a modification.

(Appx31.) For the same reasons as claim 1, the Board found that Facebook had not shown unpatentability of independent claims 7 and 19, which disclose substantially the same "internally determines" step. (Appx31-32.) As explained in detail below, the Board's key misstep was the inaccurate assumption that the system in Roseman performs all processing of content at the *host*.

### B. The '657 Patent (IPR2016-01159)

On December 6, 2017, the Board issued a Final Written Decision finding that claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 were unpatentable, but upholding dependent claims 203, 209, 215, and 221. The Board's decision rested entirely on a "censorship" limitation in these four claims.

Independent claim 189 recites a method of communicating via an Internet network that includes a step of "**determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia**." Facebook argued that this limitation was disclosed by Roseman and Lichty because both references disclosed techniques for blocking unwanted communications from potentially disruptive users. The Board agreed, finding the censorship limitation to be disclosed by Roseman and Lichty. (Appx195-197.)

But the Board upheld dependent claims 203, 209, 215 and 221 based on limitations found in dependent claims 202, 208, 214, and 220, which depend from independent claim 189:[5]

> 202. The method of claim 189, wherein the determining whether the first user identity is censored includes **determining that the first user identity is censored from the sending of the data presenting the <u>video</u>**.
>
> 208. The method of claim 189, wherein the determining whether the first user identity is censored includes **determining that the first user identity is censored from the sending of the data presenting the <u>audio</u>**.
>
> 214. The method of claim 189, wherein the determining whether the first user identity is censored includes **determining that the first user identity is censored from the sending of the data presenting the <u>graphic</u>**.
>
> 220. The method of claim 189, wherein the determining whether the first user identity is censored includes **determining that the first user identity is censored from the sending of the data presenting the <u>multimedia</u>**.

(Appx384-385 (emphasis added).) As shown these claims are similar to each other and differ only with respect to the type of data in the communication.

[5] The IPR petitions on the ’657 patent did not list claims 202, 208, 214, and 220 among the challenged claims. Their limitations were nevertheless relevant because Facebook did challenge claims 203, 209, 215 and 221, which depended, respectively, from claims 202, 208, 214, and 220. (Appx7264.)

The Board found that Roseman and Lichty did not disclose these claims because, according to the Board, these claims require that the censorship *determination* itself be based on *the type of content* being communicated:

> Roseman describes censoring users from sending all communications based on a determination that the user is conducting a filibuster. Ex. 1003, 12:29–45. Petitioner points to no description in Roseman of determining that a user is censored from sending a particular type of data—it is all or nothing. Likewise, Lichty describes an ignore feature for blocking all communications from a disruptive user, regardless of data type—again, all or nothing. Ex. 1007, 269, 510. We find that Roseman and Lichty do not teach determining that a user is censored from sending certain types of data.

(Appx202.) The Board essentially concluded that claims 202, 208, 214, and 220 require that the system *selectively and exclusively censor*, respectively, video, audio, graphic, and multimedia, from the communication. (Appx201 ("For example, Petitioner does not contend that Roseman and Lichty teach censoring a user from sending video data, but permitting the user to send audio data.").)

But the Board's conclusion was based on a fundamental misreading of the claims. As explained in detail below, the claims do not recite any kind of content-based censorship; they simply specify the type of data that the communication in independent claim 189 must contain.

### C. The ’552 Patent (IPR2016-01158)

On December 6, 2017, the Board issued a Final Written Decision finding that claims 2, 3, 5, 7, 10-17, 59, and 64 are unpatentable, but not claims 1, 4, 6, 8, 9, and 18-58. The Board focused on limitations in claim 1 (and similar limitations in claims 4, 6, 8, 9, 18, 50, 54 and 58) that recited “**storing each said user identity and a respective authorization to send multimedia 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**.” (Appx147-152.)

The Board stated that Facebook failed to show that “a key [in Roseman] that grants admission [to a conference room] also includes an authorization to send multimedia data in that conference room. Roseman’s key simply grants access to a conference room.” (Appx148.) As to claim 18, the Board also stated that Facebook did not “include any additional argument as to why Roseman teaches ‘the computer system: stores, for a first of the user identities, a respective authorization associated with multimedia data communication’” or “how Roseman teaches ‘*based* on the respective authorization, cause the multimedia data to be presented’ at a participator computer corresponding to a second user identity.” (Appx149.) As explained below, the Board misinterpreted the claim language, but even under that incorrect interpretation, the prior art nonetheless renders the claims obvious.

### D. The ’356 Patent (IPR2016-01157)

On December 6, 2017, the Board issued a Final Written Decision finding that Facebook had not shown by a preponderance of the evidence that claims 14 and 33 were unpatentable. (Appx94.) The Board focused on limitations in claims 14 and 33 of “determin[es/ing] censorship of the content.” In the Board’s view, because the term “censorship” was “modified by the term ‘of the content,’” the phrase “determining censorship of the content” was narrower than “censorship” generally and meant “determining whether to communicate content based on characteristics of the content.” (Appx47-48.) Similar to its approach with the ’657 patent discussed above, the Board concluded that Facebook had failed to show that Roseman taught “determining whether to communicate content based on characteristics of the content.” (Appx89-90.)

Instead, according to the Board, “[w]hen Roseman’s host acts as a moderator, it prevents a user from speaking without regard to characteristics of the content.” (Appx90.) As explained below, the Board erred by interpreting claims 14 and 33 to require censorship based on characteristics of the content.

## SUMMARY OF ARGUMENT

The Board’s patentability findings should be reversed. The findings were based on erroneous and unsupported interpretations of the claim language and a misunderstanding of the disclosures of the prior art.

With respect to the ’245 patent, the Board’s decision rests on the erroneous assumption that Roseman discloses a system in which the local (participant) computer would never need to perform any processing in order to display content received during a meeting. But the Board overlooked key teachings in Roseman that demonstrate that local (participator) computers can receive *actual* data files from the host (server) computer, thus making the teachings of Pike and Westaway relevant. Because the Board’s decision to uphold the challenged claims of the ’245 patent was based entirely on a misreading of Roseman, the decision lacks substantial evidence support and must be reversed.

The Board’s errors with respect to the other challenged patents boil down to classic questions of claim construction reviewed *de novo* by this Court.

As to the ’657 patent, the Board adopted a narrow construction of dependent claims 202, 208, 214 and 220 that cannot be reconciled with the plain claim language. For example, claim 202 recites the step of “determining that the first user identity is censored from the sending of the data presenting **the video**.” The Board narrowly interpreted this language to require censoring of ***only the video portion*** of a communication. (Appx201 (“For example, Petitioner does not contend that Roseman and Lichty teach censoring a user from sending video data, but permitting the user to send audio data.”).) But nothing in the claim language requires selectively censoring ***only*** video, or censoring ***based on*** video. The claim only requires censoring of "the data presenting the video," and it makes no difference whether that system also censors other types of data that may exist in the communication. For example, if a system simply censored all content – including video – it would meet claim 202 under its proper construction.

The Board identified nothing in the intrinsic record that could justify interpreting the claims so contrary to their plain language. Because the Board's patentability decision rests entirely on an erroneous interpretation of the "determining" step in claims 202, 208, 214 and 220, it should be reversed.

The Board made a similar claim construction error in its interpretation of certain claims of the '552 patent. Claim 1 recites the steps of "storing each said user identity and a respective authorization to send multimedia data," and if permitted by that user identity, "allowing the one of the participator computers to send multimedia data to another of the participator computers." Notably, the patent owner did not dispute that the prior art disclosed these claim limitations.

But the Board *sua sponte* confirmed these claims based on a construction of the claimed "authorization" that it did not disclose until its Final Written Decision. The Board's construction required that the claimed authorization be tailored ***specifically*** to the act of sending multimedia data. An authorization to join the group or conference of Roseman was insufficient, the Board found, even though joining the group allowed the user to send multimedia data.

But the claim language does not require the authorization relate specifically or exclusively to the act of sending multimedia data. For example, a gym member can have a keycard that allows entry into the local gym; after entering, the member can then use the exercise equipment inside. The keycard clearly provides authorization to use the exercise equipment because it allows access to the building. The same is true for Roseman – a conference participant has authorization to enter a group or conference room, and after entering the conference room, can send multimedia data. Each user identity in Roseman clearly has "a respective authorization to send multimedia data," under the correct construction.

As to the '356 patent, the Board erred when it found that step of "determin[es/ing] censorship of the content" in claims 14 and 33 narrowly requires determining whether to communicate content *based on characteristics of the content*. The latter improperly imports limitations from the specification into the claim and impermissibly rewrites it too narrowly. Under the correct interpretation of the claims, as written, that step is disclosed by Roseman.

# ARGUMENT

## I. STANDARD OF REVIEW

The ultimate interpretation of a claim term is a legal conclusion reviewed *de novo*, with any subsidiary factual findings about extrinsic evidence that underlie claim construction reviewed for substantial evidence. *Corning v. Fast Felt Corp.*, 873 F.3d 896, 901 (Fed. Cir. 2017) (citing *In re Cuozzo Speed Techs., LLC*, 793 F.3d 1268, 1280 (Fed. Cir. 2015), *aff'd sub nom. Cuozzo Speed Techs., LLC v. Lee*, —— U.S. ——, 136 S. Ct. 2131, 195 L. Ed. 2d 423 (2016)). The ultimate determination of obviousness is a question of law reviewed *de novo*, with associated factual findings reviewed for substantial evidence. *Id.* at 902.

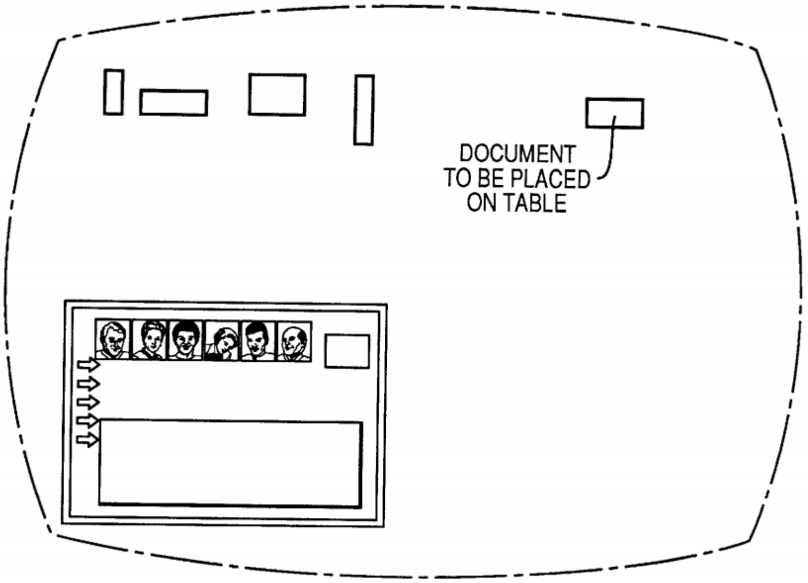
The "substantial evidence" standard does not prevent this Court from applying its own knowledge and expertise to the review of PTO decisions. As the Supreme Court has observed, "when a Federal Circuit judge reviews PTO factfinding, he or she often will examine that finding through the lens of patent-related experience—and properly so, for the Federal Circuit is a specialized court." *Dickinson v. Zurko*, 527 U.S. 150, 163 (1999).

## II. The Patentability Finding for the '245 Patent Should Be Reversed

The Board's decision as to the '245 patent rests on the false assumption that the local (participant) computers in Roseman would have no reason to perform processing of content in order to display it. Under the Board's view, the host (server) in Roseman generates a "common image" for all local computers, and that common image provides the sole means to view content shared in a conference. The local computers, under this view, would never encounter content types they could not present, and thus, would never need to obtain an agent or viewer as disclosed in Pike. (Appx29-30 ("The most logical reading of Roseman is that its local computers already have software sufficient to render the common image that the host provides to them.”).) But simply because the host in Roseman creates a “common image” does not mean that every item of content shared in the virtual conference room is delivered through that image.

The Board’s analysis overlooked at least two instances in which content shared in a virtual conference room can be accessed by local participant computers *outside* the context of the virtual conference room software running on the local computer. This outside area is shown in Figure 10:

FIG. 10



(Appx1204, Fig. 10.) Roseman explains that each local computer uses a standard operating system such as Microsoft Windows or an equivalent. (Appx1224, 12:1-5.) With reference to Figure 10 above, the window on the bottom left of the screen shows the virtual conference room. Roseman explains that “[t]he private work area outside the window displays the icons representing the invitee's programs and data files." (Appx1222, 8:7-9.) These files thus exist outside the virtual conference room application (such as on the user's "desktop").

Roseman allows a participant to "drag" a data file from this outside private area into the conference room to share the file with other participants. (Appx1224, 11:20-22 ("This might be done by dragging an icon of the object from the outside (users non-'meeting room' windows) onto the table.").) Roseman also refers to the area outside the virtual conference room window as a "private viewing area," which can be used to view private notes outside the conference room. (Appx1223, 9:28-31 ("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.").)

These two embodiments – note passing and document sharing – provide two clear examples of how a *local* computer in Roseman can access and process shared communications. These embodiments thus disprove the key premise behind the Board's decision – that Roseman "processes images at the host, not the local computers." (Appx29.)

### A. Note-Passing Feature

The note-passing feature in Roseman allows a conference participant to send a private note to another participant, which only the recipient can view. (Appx454.)

Roseman explains that "[w]hen the other party [recipient] 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*." (Appx1223, 9:28-31 (emphasis added).)

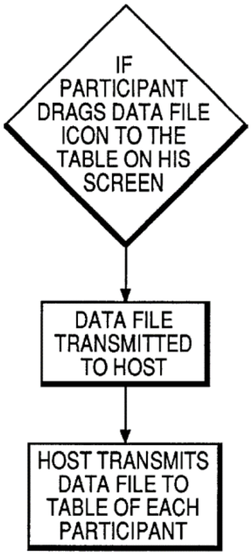
In other words, the note recipient must drag the received note outside of the conference room window in order to privately view it. This provides a clear example of content shared in Roseman that must be processed and viewed on the local computer outside the local conference room software, and thus, not delivered in the "common image" it receives from the host.

And Roseman makes clear the private note-passing feature could not work any other way. If a recipient attempted to access a private note from ***within*** the virtual conference room, that note would be seen by the other participants of the conference. (Appx1222, 7:55-57 ("The table is a common display area which is shown to, and available for work by, each Invitee."); Appx1219, 2:38-47 ("In the invention, the participants share a common virtual conference table. Each participant can (1) place a document onto the table electronically… All other participants see the preceding … event[] as [it] occur[s].").) In other words, for a private note recipient to view the note *privately*, the recipient must drag it outside the conference room window and open it on the recipient's local computer. (Appx1223, 9:28-31 ("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.”).)

### B. Document Drag-and-Drop Feature

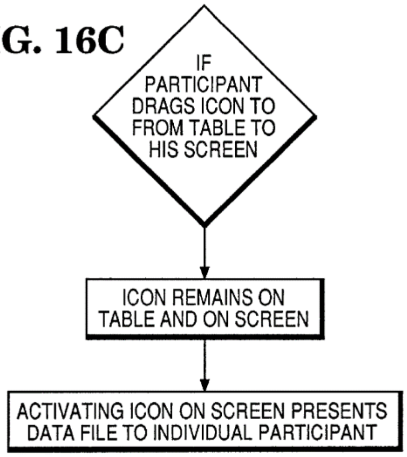
Roseman discloses a second drag-and-drop feature that demonstrates how the local computers in Roseman process files for display. As noted previously, a user can drag a data file from outside the conference room window (e.g., from the user’s desktop) onto the table of the conference room. This functionality is shown in the flowchart in Figure 16A (at right). (Appx1212, Fig. 16A.) Critically, each step in Figure 16A shows that *the actual data file* (“DATA FILE”) the participant dragged from his screen into the conference room – not a common image or representation of it generated by the host – is transmitted to each conference participant. Nothing in Roseman suggests that the host interprets the “DATA FILE” and generates a common image representation of it for transmission to the local computers. Roseman instead sends the *actual data file itself* to the local computers.

FIG. 16A


IF PARTICIPANT DRAGS DATA FILE ICON TO THE TABLE ON HIS SCREEN
DATA FILE TRANSMITTED TO HOST
HOST TRANSMITS DATA FILE TO TABLE OF EACH PARTICIPANT

This is confirmed by Figure 16C, which shows that another participant, after receiving the "DATA FILE" shared during the conference, can drag the file into his or her private work or viewing area (his "screen"). The last step in Figure 16C shows that the data file can be activated from the recipient's *screen* (outside the conference), which presents the file "to the *individual* participant." (Appx1212, Fig. 16C; Appx1225, 14:62-67.)

FIG. 16C


IF PARTICIPANT DRAGS ICON TO FROM TABLE TO HIS SCREEN
ICON REMAINS ON TABLE AND ON SCREEN
ACTIVATING ICON ON SCREEN PRESENTS DATA FILE TO INDIVIDUAL PARTICIPANT

As explained above in the context of note-passing, the fact that the data file is presented to the "individual participant" (Appx1212, Fig. 16C), and not all conference participants, confirms that the participant has accessed the file on her local computer from outside the conference room software.[6] And Roseman makes

[6] This is also confirmed by Roseman's mechanism for terminating a conference. Roseman explains that when a conference has ended, one of the first things the host does is notify each participant of the latest modifications to the data files. (Appx1217, Fig. 22A ("HOST SENDS LATEST MODIFICATION OF EACH DATA FILE TO EACH PARTICIPANT").) The host can then destroy the data files if the conference initiator prefers. (Appx1218, Fig. 22B ("HOST DESTROYS CONFERENCE ROOM ATTRIBUTES AND FILES").) It would make no sense to notify conference room participants of recent changes to the data files after a conference ends if, as the Board seemed to believe, the data files could only be accessed during a conference through the host-generated common image. The notification in Roseman clearly contemplates that the data files are accessible to the participants' local computers after termination of the conference and even after the host deletes those its copies of those files. This further confirms that the local computers of conference participants receive *the actual data files* and not simply a host-generated screen representation of them.

clear that this occurs by the typical way that any Microsoft Windows user could recognize – by double-clicking the file's icon to open the appropriate application on the local computer. (Appx1224, 12:11-13 ("For example, implementation of dragging-and-dropping, double-clicking to actuate a program, or to cause an icon to bloom into a screen, etc, is within the skill of the art.") (emphasis added).) Facebook's expert explained that "Roseman places no limits on what that document could be; it could be any file stored on the participant's local computer." (Appx1161, ¶103.)

### C. The Note-Passing and Document Sharing Features of Roseman Undermine the Key Premise of the Board's Decision

The record thus contradicts the key premise behind the Board's decision – that Roseman "processes images at the host, not the local computers," and thus, "its local computers already have software sufficient to render the common image that the host provides to them." (Appx29.) The features discussed above provide at least two ways in which documents shared in a conference can be stored and processed on local (participant) computers, *outside* the local computer's conference room software and the "common image" received from the host.

The Board's erroneous assumption that Roseman "processes images at the host, not the local computers" was the foundation to its entire Final Written Decision. This assumption provided the sole basis for the Board's conclusion that a person of ordinary skill in the art would not have found the teachings of Pike and

Westaway applicable to Roseman. Because that assumption was incorrect, the Board’s decision on the ’245 patent must be reversed.

Once a file is accessed by a local (participant) computer in Roseman, outside the conference room software – as Roseman clearly discloses can occur – it would have been obvious that the local computer could check to determine whether it had the appropriate software to present the document, as disclosed in Pike and Westaway and accepted by the Board as noted above. Because the “internally determining” step was the sole basis on which the Board distinguished the challenged claims of the ’245 patent from the prior art, this Court should reverse the Board’s decision and conclude that the challenged claims are unpatentable.

## III. The Patentability Finding for the ’657 Patent Should Be Reversed

### A. Facebook Established that Roseman and Lichty Disclose and Render Obvious the “Determining” Steps of Claims 202, 208, 214 and 220

Claims 202, 208, 214 and 220 of the ’657 patent depend from independent claim 189. The Board correctly found that claim 189 is unpatentable over Roseman in view of Rissanen, Vetter, Pike and Lichty. (Appx180-199.)

Claim 189 recites in part “determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by another of the user identities." (Appx383-384, 36:66-37:5].) Facebook explained how this limitation as a whole is disclosed by and obvious over Roseman and Lichty, and the Board agreed. (Appx7302-7305; Appx196-197.) Facebook further explained how the prior art discloses each of the five types of data recited in the limitation (i.e., a pointer, video, audio, a graphic, and multimedia), and the Board agreed. (Appx7296-7301; Appx5494-5500; Appx195-196 ("Petitioner argues that Roseman describes several examples of presenting data of different types. . . . We agree that these are specific examples of data presenting at least one of a pointer, video, audio, a graphic, and multimedia.").)

Claims 202, 208, 214 and 220 narrow this limitation by each reciting censorship regarding one of the types of data recited in claim 189: claim 202 recites video, claim 208 recites audio, claim 214 recites a graphic, and claim 220 recites multimedia. Critically, each dependent claim's requirement of determining that a user is censored does not require determining the type of data. Instead, each claim simply adds an express requirement for the particular type of data recited. For example, while a disclosure in the prior art of any one of the five types of data is sufficient to meet claim 189, claim 202 is not met unless the user is actually censored and the data is video. Thus, Facebook explained how Roseman and Lichty disclose the limitations that these claims add to claim 189:

> The Petition cited Lichty for its disclosure of its censoring feature, and relied on the host in Roseman to carry out the other features of the

> claim, including the transmission of video, audio, content, graphic or multimedia content. Accordingly, *under the combination of Roseman and Lichty, when a first user is blocked from sending data to a second user via the censoring features of Lichty, that user is blocked from sending video, audio, graphic or multimedia content, whatever the case may be. The claims require nothing more.*

(Appx5895 (internal citations omitted) (emphasis added).)

### B. The Board's Interpretation of the "Determining" Steps in Claims 202, 208, 214 and 220 was Too Narrow

The Board erred when it concluded that the "determining" steps of claims 202, 208, 214 and 220 narrowly require "determining whether the first user identity is censored from sending particular types of data." (Appx201.) The Board's erroneous interpretation was based on a misinterpretation of both the plain language of the claims and the specification.

The Board first reviewed the claim language itself, finding that the claims "include additional language reciting determinations *based on* data type." (Appx202 (emphasis added).) But nothing in the claims requires censorship *based on* the type of data in the communication.

More specifically claim 189 (from which these claims depend) recites the step of "determining whether the first user identity is individually censored from sending data in the communications, the data presenting **at least one of** a pointer, **video**, **audio**, **a graphic**, and **multimedia**…" Claim 189 therefore only requires that the communication contain one of those types of data. If the communication contains a video, therefore, it need not contain a pointer, audio, a graphic, or multimedia.

Dependent claims 202, 208, 214 and 220 simply specify what happens if the communication ***does*** contain one of four types of data (*i.e.*, video, audio, graphic or multimedia). Claim 202, for example, adds the step of "determining that the first user identity is censored from the sending of the data presenting **<u>the video</u>**." This claim language requires that video – to the extent it is part of the communication of claim 189 – be censored. It states nothing more, and requires nothing more.

Nothing in the claim language requires selectively censoring ***only*** video, or censoring ***based on*** video content. For example, if a system censored video and some other type of content, it could still meet claim 202. In fact, if a system censored all types of content – including video – it could still meet claim 202. So long as a system censors "the data presenting the video," it makes no difference under the claim language whether that system censors other types of data as well.

The Board's interpretation effectively improperly rewrites the claim to recite "[t]he method of claim 189, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video ***based on the data being video***."

In fact, not only is there no basis in the claim language for the Board's interpretation, other claims of the '657 patent confirm that the applicants knew how to draft claims using “based on” language but chose not to for the challenged claims. For example, claim 204 recites “[t]he method of claim 202, further including determining whether at least one of the communications is censored ***based on content***.” (Appx384, 38:27-29 (emphasis added).) Claims 202, 208, 214 and 220 could have been drafted using similar language, but they were not. The unambiguous chosen claim language should not be rewritten. *Chicago Bd. Options Exch., Inc. v. Int’l Securities Exch., LLC*, 677 F. 3d 1361, 1369 (Fed. Cir. 2012) (discussing presumption that different terms have different meanings); *Chef America, Inc. v. Lamb-Weston, Inc.*, 358 F. 3d 1371, 1374 (Fed. Cir. 2004) (observing that Federal Circuit has repeatedly declined to rewrite unambiguous patent claim language).

The same analysis applies to dependent claims 208, 214, and 220. These claims simply require that audio, graphic or multimedia data, respectively, be censored to the extent they are part of the “communication” of claim 189. They recite no requirement of selective or content-based censoring.

The Board also attempted to look to the specification for support, asserting that its interpretation was “consistent with the description in the specification that ‘[c]ensorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.’” (Appx202.) But rather than supporting the Board’s interpretation, the cited passage illustrates that the Board improperly imported a limitation from the specification into the claims.

The passage quoted by the Board makes clear that "real time control of data" can be based on more than just "type," such as "quantity" and "subject." These additional bases for censoring data meet the plain language of the claims, but they would be excluded by the Board's interpretation. *See, e.g., Hill-Rom Servs., Inc. v. Stryker Corp.*, 755 F. 3d 1367, 1372-73 (Fed. Cir. 2014) (absent clear language in the specification limiting the invention, "we do not import limitations from the specification"); *Superguide Corp. v. DirecTV Enters., Inc.*, 358 F. 3d 870, 875 (Fed. Cir. 2004) ("The written description… is not a substitute for, nor can it be used to rewrite, the chosen claim language.").

The sole reason for the Board's decision that claims 203, 209, 215 and 221 were not unpatentable over the prior art was based on its incorrect interpretation of claims 202, 208, 214 and 220. (Appx201-202.) Under a correct interpretation of those claims, Facebook demonstrated by a preponderance of the evidence that claims 203, 209, 215 and 221 are obvious.

## IV. The Patentability Finding for the '552 Patent Should Be Reversed

The Board's findings with respect to the '552 patent suffer from a similar flaw as the '657 patent.

### A. Facebook Established that Roseman Discloses the Claimed "Authorization" Steps

Claim 1 of the '552 patent recites that the "controller computer system control[s] real-time communications" by (1) "storing each said user identity and a respective authorization to send multimedia data . . ." and (2) "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."

The petition set forth how Roseman (alone or with Rissanen) discloses these steps, explaining that Roseman discloses the use of keys associated with user identities for controlling admission to a particular conference:

> [T]he 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 (underlining added).) Thus, Roseman discloses these limitations 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.

(Appx3755-3756 (emphasis in original).) As the passage above explains, the claim steps are satisfied because a user identity in Roseman that is not authorized to access a room based on stored key information cannot send multimedia data to conference room participants. That is all that the steps require.

The petition further explained that claims 4, 6, 8, 9, 18, 50, 54 and 58 recite substantially the same limitations that are disclosed by the prior art for the same reasons as claim 1. (Appx3761-3762 (claim 18); Appx3764; Appx3766-3767; Appx3769; Appx3779 (claims 4, 6, 8, 9).)

### B. The Board Incorrectly Interpreted the "Authorization" Steps

The Board erred when it concluded that the "authorization" steps of the claims narrowly require "determining ***what*** a user can do in a conference room once admitted."[7] (Appx148 (emphasis added).) The Board did not identify any support in the specification for this view. *See, e.g.*, *Hill-Rom Servs.*, 755 F. 3d at 1371 ("We depart from the plain and ordinary meaning of claim terms based on the specification in only two instances: lexicography and disavowal.").

[7] The Board initially adopted Facebook's analysis in its Institution Decision and did not discuss the "authorization" steps at the oral hearing. It was not until the Final Written Decision that the Board specifically addressed the steps and reversed course. Thus, the Board improperly changed theories without giving Facebook an opportunity to respond. *See Intellectual Ventures II LLC v. Ericsson Inc.*, 686 Fed. App'x 900, 906 (Fed. Cir. 2017).

The plain language of the claimed authorization steps of the ’552 patent is broad but unambiguous. The steps simply require “storing each said user identity and a respective authorization to send multimedia 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.” This language does not require any ***separate*** determinations that a user is authorized to perform the ***specific*** act of sending multimedia data. For example, if a user is permitted to send multimedia data simply by virtue of being authorized to join a group or conference, the claim limitations are satisfied.

The petition explained that this is precisely what the prior art discloses. Roseman (alone or with Rissanen) teaches that the host stores key information for an associated user for accessing a particular conference room. (Appx3755-3756.) “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.” (Appx1223, 10:62-64.) However, “[p]ersons with improper keys are not admitted to the room.” (Appx1223, 9:50-51.) If admitted to the conference room, the user is authorized to send multimedia data to other conference participants. (Appx1222, *e.g.*, 8:1-4 (“Each Invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it.”), 8:14-15 (“Each Invitee can write on the document . . . .”), 7:55-56 (“The table is a common display area which is shown to, and available for work by, each Invitee."), 8:19-21 ("Any Invitee can pull down a note sheet, as shown in FIG. **12**, by using the pointing device, and write on the sheet.").) If not admitted, or not authorized, no data can be sent.

The "authorization" steps are therefore disclosed by Roseman (alone or with Rissanen). Notably, Windy City did not dispute that the cited prior art disclosed the "authorization" steps.

### C. The Prior Art Discloses the "Authorization" Limitations Even Under the Board's Incorrect Construction

However, even if the Board's construction were correct, the steps are nonetheless disclosed by the prior art. In particular, Roseman explains that a conference room can have both Invitees who are authorized to send multimedia data in a conference and "Spectators" who can enter a conference room but who can only observe the proceedings:

> [T]he Requester can state that "Spectators" can observe the conference. That is, any person can contact the host, obtain a list of ongoing conferences, select a conference room, enter it, and observe the proceedings.

(Appx1222, 7:21-24.) Thus, Roseman discloses that by designating a user as an Invitee to a conference, the user is being authorized to send multimedia data to other conference participants and to cause that data to be presented to those participants.

The Board's only reason for its patentability finding was based on its erroneously narrow conclusions regarding the "authorization" steps. (Appx147-

152.) As explained above, the prior art discloses these steps. This Court should therefore reverse the Board's decision and find claims 1, 4, 6, 8, 9 and 18-58 unpatentable.

## V. The Patentability Finding for the '356 Patent Should Be Reversed

### A. Facebook Established that Roseman Discloses the "Determin[es/ing] Censorship of the Content" Step of Claims 14 and 33

Claim 14 of the '356 patent depends from claim 1 and recites "[t]he method of claim **1**, further including determining censorship of the content." (Appx297, 22:21-22.) The "content" recited in claim 14 refers back to the preamble of claim 1, which recites in part "[a] method of communicating *content* among users." (Appx297, 21:30 (emphasis added).)

Facebook explained that Roseman discloses several means of censorship that satisfy the limitations of claim 14. (Appx2163-2164.) For instance, Roseman explains that a conference room could require procedural issues to be followed before allowing a vote to occur or before someone was allowed to speak. (Appx2164 (citing Appx1224, 11:40-46.) In addition, Roseman discloses that its host computer can perform censorship by acting as a conference "moderator" and regulating when and/or how long participants can speak during the conference, or preventing a disruptive participant from continuing to speak. (Appx2164 (citing Appx1224, 12:29-45.)

Facebook also noted that Roseman's disclosures mirror examples of censorship described in the '356 patent. (Appx2164 (citing Appx290, 8:41-46).) For example, the '356 patent discloses that censorship is a broad concept that can take the form of controlling whether a user can join a group in the first place as well as controlling various forms of interaction once joined in a group:

> *Censorship, which broadly encompasses control of what is said in a group*, is also arbitrated by means of the tokens. *Censorship can control of access to system 1 by identity of the user*, which is associated with the user's tokens. By checking the tokens*, a user's access can be controlled per group*, as well as in giving group priority, moderation privileges, etc.
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs--quantity, type, and subject.
> *With regard to controlling communications in a group* (which is in essence a collection of user identities)*, control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages*.

(Appx290, 8:39-53 (emphasis added).)

Facebook further noted that claim 33 is substantially the same as claim 14 and therefore disclosed by Roseman for the same reasons. (Appx2167-2168.)

### B. The Board's Claim Construction of "Determin[es/ing] Censorship of the Content" Is Too Narrow

The Board correctly found that the term "censorship" should be broadly construed as "control of what is said in a group" in accordance with definitional language in the specification. (Appx45-47.) However, the Board erred when it concluded that the step of "determin[es/ing] censorship of the content" of claims 14 and 33 narrowly requires "determining whether to communicate content *based on characteristics of the content*."[8] (Appx48 (emphasis added).) The Board's erroneous interpretation was based on a misinterpretation of both the plain language of the claims and the patent's specification.

The Board first looked to the language of the claims, asserting that "the broad term 'censorship' is modified by the term 'of the content.'" (Appx47.) The Board also compared the language of claims 14 and 33 to claims 2 and 20, which simply recite that the content includes "at least one of sound, video, pointer and multimedia content." (Appx48.) Although claims 14 and 33 do not depend from claims 2 and 20, the Board found that claims 2 and 20 "further show[] that content refers to the type of data, so that censorship of content is directed to censoring content based on characteristics such as the type of data." (Appx48.) The Board also sought support in the specification, which in its view, disclosed an example of censorship "based on the characteristics of the data itself..." (Appx47 ("This is consistent with the example in the specification, cited above, that '[c]ensorship also can use the tokens

[8] In the decision instituting IPR, the Board credited Facebook's analysis and did not construe the phrase "determin[es/ing] censorship of the content." (Appx2251-2254.) Nor was a construction for this phrase addressed subsequently until the Final Written Decision. Thus, the Board improperly changed theories without giving Facebook an opportunity to respond. *See Intellectual Ventures II*, 686 Fed. App'x at 906.

for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.'").)

The Board's claim construction is wrong as a matter of law. To begin with, because the claim language is clear, the Board should not have construed the phrase in the first place. *See, e.g.*, *Hill-Rom Servs.*, 755 F. 3d at 1371-72 ("We depart from the plain and ordinary meaning of claim terms based on the specification in only two instances: lexicography and disavowal."). However, even if it were appropriate to provide a construction to understand the application of the prior art to the claim language, the Board's construction improperly rewrites the claim and imports limitations from the specification such that the claims narrowly require "determin[es/ing] censorship of the content …*based on characteristics of the content*." (Appx48.) *See, e.g.*, *Hill-Rom Servs.*, 755 F. 3d at 1372-73 (absent clear language in the specification limiting the invention, "we do not import limitations from the specification"); *Superguide,* 358 F. 3d at 875 ("The written description . . . is not a substitute for, nor can it be used to rewrite, the chosen claim language."). Simply put, the broader concept of "censorship **of** the content" from the claim language is not the same thing as "censorship **based on** the content" which the Board erroneously added.

There is no basis in the claim language or specification to narrowly limit claims 14 and 33 to censorship "based on characteristics of the content." The claims simply require "determin[es/ing] censorship of the content." This requirement is plainly satisfied when the communication of content from a user joined in a conference room is blocked, irrespective of the characteristics of that content. To the extent that claims 2 and 20 are even relevant to the analysis,[9] they only disclose potential types of content that can be communicated.

The specification supports this reading of claims 14 and 33. As noted above, the '356 patent identifies several ways in which censorship can be carried out. Some of those ways do not involve censorship of content and others do. For example, the '356 patent states that censorship includes determining whether a user has access to the system or can join a group in the first place. (Appx290, 8:41-44.) The patent further states that, once in a group, censorship can include "the ability to see . . . a specific user." (Appx290, 8:48-52].) These forms of censorship are clearly different than "censorship of the content" described in the claims and in the specification, such as the ability to see and send messages once in a group:

> *With regard to controlling communications in a group* (which is in essence a collection of user identities), *control extends to seeing messages*, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. *Control further extends to the ability to send multimedia messages*.

[9] In *SunRace Roots Enterprise Co., Ltd. v. SRAM Corp.*, 336 F. 3d 1298 (Fed. Cir. 2003), this Court recognized that the doctrine of claim differentiation is "not a hard and fast rule of construction" and that its utility is diminished when comparing dependent claims where the limitation in dispute is not the only meaningful difference. *SunRace Roots Enter.*, 336 F. 3d at 1302.

(Appx290, 8:48-53.)

Thus, the Board's construction is wrong.[10] The Board's erroneous construction was the only reason for the Board's decision that claims 14 and 33 were not unpatentable over the prior art. (Appx88-90.) As explained above, Roseman discloses various ways in which a user's communication of content in a conference is censored. Under a correct interpretation of those claims, Facebook demonstrated by a preponderance of the evidence that they are obvious.

## CONCLUSION

For all of the foregoing reasons, Facebook respectfully requests that the Court reverse the Board's final written decisions and find all challenged claims unpatentable.

[10] While the "broadest reasonable construction" applies to the IPR2016-01157 proceeding, *see* 37 CFR § 42.100(b) (approved by *Cuozzo Speed Techs., LLC v. Lee*, ––– U.S. ––––, 136 S. Ct. 2131, 2144-45 (2016)), there is no basis for the construction under the *Phillips* standard either. *Phillips v. AWH Corp.*, 415 F. 3d 1303, 1313 (Fed. Cir. 2005) ("[T]he person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.").

Dated: May 21, 2018

COOLEY LLP

By: /s/ Heidi L. Keefe
Heidi L. Keefe

*Counsel for Appellant*
FACEBOOK, INC.

# ADDENDUM

# ADDENDUM TABLE OF CONTENTS

Trials@uspto.gov
571-272-7822

Paper No. 52
Entered: December 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FACEBOOK, INC.,
Petitioner,

v.

WINDY CITY INNOVATIONS, LLC,
Patent Owner.

Case IPR2016-01156[1]
Patent 8,458,245 B1

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

MCKONE, *Administrative Patent Judge*.

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

[1] Case IPR2017-00709 has been joined with this proceeding.

## I. INTRODUCTION

### *A. Background*

Facebook, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") seeking *inter partes* review of claims 1–15, 17, and 18 of U.S. Patent No. 8,458,245 B1 (Ex. 1001, "the '245 Patent"). Windy City Innovations, LLC ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp.").

Pursuant to 35 U.S.C. § 314, in our Institution Decision (Paper 7, "Dec."), we instituted this proceeding as to claims 1–15, 17, and 18.

Patent Owner filed a Patent Owner's Response (Paper 22, "PO Resp."), and Petitioner filed a Reply to the Patent Owner's Response (Paper 31, "Reply").

Petitioner relies on the Declarations of Tal Lavian, Ph.D. (Ex. 1002, "Lavian Decl."; Ex. 1021, "2nd Lavian Decl."). Patent Owner relies on the Declaration of Jaime G. Carbonell, Ph.D. (Ex. 2005, "Carbonell Decl.").

On January 17, 2017, Petitioner filed a petition seeking *inter partes* review of claims 19 and 22–25 of the '245 patent and sought to join that proceeding to this proceeding. IPR2017-00709, Paper 2 ("the '709 Pet."), Paper 3 (Mot. for Joinder). We instituted a trial in that proceeding and joined it to this proceeding. Paper 34 ("the '709 Dec."). Petitioner relies on the Declaration of Dr. Lavian in the '709 proceeding (IPR2017-00709, Ex. 1002 ("Lavian '709 Decl.").

As to the additional claims challenged in the '709 Petition, Patent Owner filed a Supplemental Patent Owner's Response (Paper 45, "Supp. PO Resp.") and Petitioner filed a Supplemental Reply (Paper 46, "Supp. Reply").

An oral argument was held on October 19, 2017 (Paper 51, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 1–15, 17–19, and 22–25. Based on the record before us, Petitioner has not proved, by a preponderance of the evidence, that any claim of the ’245 patent is unpatentable.

### *B. Related Matters*

The parties indicate that the ’245 patent has been asserted in *Windy City Innovations, LLC v. Microsoft Corp.*, Civ. A. No. 15-cv-00103-GM (W.D.N.C.) (transferred to 16-cv-1729 (N.D. Cal.)), and *Windy City Innovations, LLC v. Facebook, Inc.*, Civ. A. No. 15-cv-00102-GM (W.D.N.C.) (transferred to 16-cv-1730 (N.D. Cal.)). Pet. 1; Paper 4, 1. The ’245 patent also is the subject of *inter partes* review petitions in IPR2016-01141, Paper 4, 1, and IPR2017-00655, which was joined to IPR2016-01141. The ’245 patent was the subject of IPR2017-00669 (now terminated), which Microsoft Corp. filed and sought to join with this proceeding prior to settling with Patent Owner. Patents related to the ’245 patent are subjects of additional *inter partes* review petitions.

### *C. Asserted Prior Art References*

Petitioner relies on the following prior art:

U.S. Patent No. 6,608,636 B1, issued Aug. 19, 2003, filed May 13, 1992 (Ex. 1003, “Roseman”);

Published European Pat. App. No. 0 621 532 A1, published Oct. 26, 1994 (Ex. 1004, “Rissanen”);

Ronald J. Vetter, *Videoconferencing on the Internet*, IEEE COMPUTER SOCIETY 77–79 (Jan. 1995) (Ex. 1005, "Vetter");

MARY ANN PIKE ET AL., USING MOSAIC (1994) (Ex. 1006, "Pike");

U.S. Patent No. 5,226,176, issued July 6, 1993 (Ex. 1007, "Westaway"); and

TOM LICHTY, THE OFFICIAL AMERICA ONLINE FOR MACINTOSH MEMBERSHIP KIT & TOUR GUIDE (2nd ed. 1994) (Ex. 1008, "Lichty").

*D. The Instituted Grounds*

We instituted a trial on the following grounds of unpatentability. Dec. 30; '709 Dec. 6–7.

| References | Basis | Claims Challenged |
|---|---|---|
| Roseman, Rissanen, Vetter, Pike, and Westaway | § 103(a) | 1–5, 7, 9–14, 19, and 22–25 |
| Roseman, Rissanen, Vetter, Pike, Westaway, and Lichty | § 103(a) | 6, 8, 15, 17, and 18 |

*E. The '245 Patent*

The '245 patent describes an Internet "chat room." According to the '245 patent, it was known to link computers together to form chat rooms in which users communicated by text, graphics, and multimedia, giving the example of the Internet service provider "America On Line." Ex. 1001, 1:40–46. The '245 patent acknowledges that chat rooms have been implemented on the Internet, albeit with "limited chat capability," but contends that the complex chat room communications capable with Internet service providers had not been developed on the Internet "at least in part because [the] Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications" and because "there is no particular control over the platform that would be encountered on the Internet." *Id.* at 1:47–54, 1:60–62.

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

FIG. 1

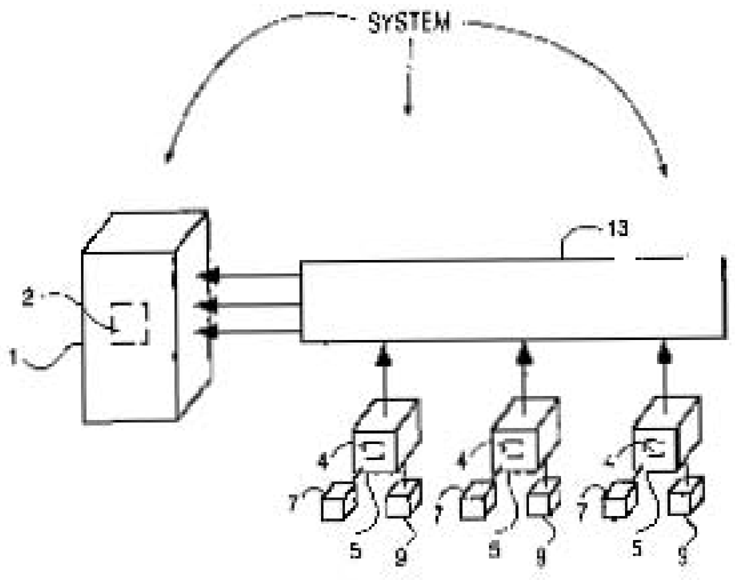


Figure 1 is a block diagram showing the components and data flow of a computerized human communication arbitrating and distributing system. *Id.* at 4:60–64. The system includes a controller computer (shown as 1 in Figure 1 but described as 3 in the written description) in communication with several participator computers 5 (e.g., IBM-compatible personal computers) over connection 13 (e.g., an Internet connection or a World Wide Web connection). *Id.* at 4:65–5:17.

The controller computer runs under the control of controller software 2, and the software arbitrates, in accordance with predefined rules (including user identities), which participator computers 5 can interact in a group through the controller computer, and directs real-time data to the members of the group. *Id.* at 5:19–25. The software uses "identity tokens," or pieces of information associated with user identity, in the arbitration. *Id.* at 8:6–9. The tokens are stored in memory 11 in a control computer database along with personal information about the users. *Id.* at 8:9–14.

The arbitration can be used to control a user's ability to join or leave a group of participator computers, to moderate communications involving the group, and to see other users in the group. *Id.* at 8:21–32. Arbitration using tokens also can be used to perform censorship:

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs [Uniform Resource Locators]—quantity, type, and subject.

*Id.* at 8:36–44.

According to the specification, "[t]he present invention comprehends communicating all electrically communicable multimedia information as Message 8, by such means as pointers, for example, URLs. URLs can point to pre-stored audio and video communications, which the Controller

Computer 3 can fetch and communicate to the Participator Computers 5." *Id.* at 5:36–41.

The '245 patent also describes a participator computer that can locate an agent for presenting a communication that the participator computer, on its own, cannot present. *See id.* at 7:34–43. Figure 6, reproduced below, illustrates an example:

FIG. 6

PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM

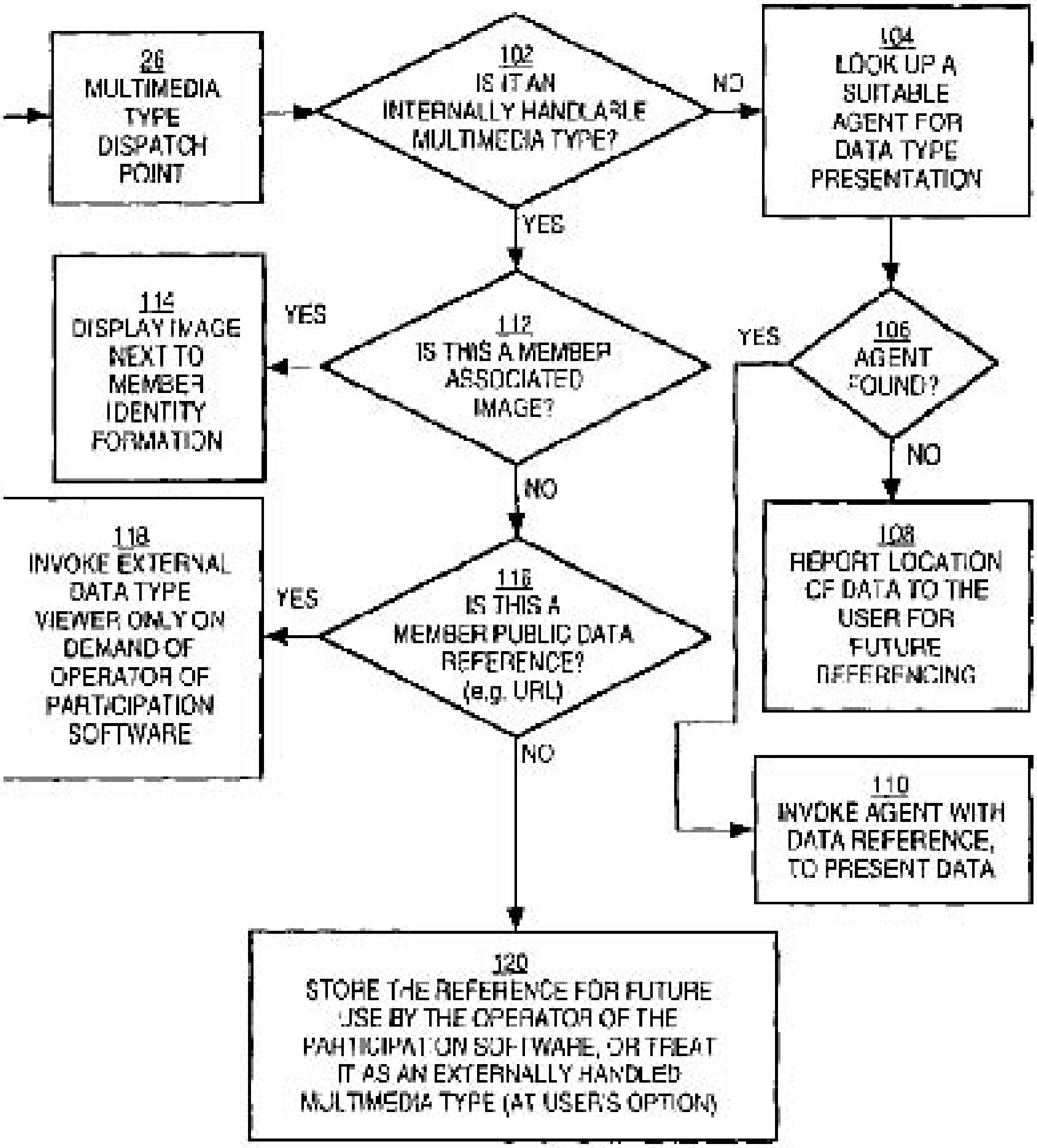

26
MULTIMEDIA TYPE DISPATCH POINT
102
IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104
LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114
DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112
IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106
AGENT FOUND?
NO
NO
118
INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116
IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
108
REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
NO
110
INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120
STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

Figure 6 is a flow diagram of participator software for out-of-band multimedia handling. *Id.* at 2:64–65, 7:34–45. When the software identifies a type of multimedia (step 26), the software determines whether it is an internally handlable multimedia type (step 102). *Id.* at 7:35–38. If not, the software looks up a suitable agent for presentation of that data type (step 104) and, if a suitable agent is found (step 106), the agent is invoked with a data reference (e.g., URL) to present the data (step 110). *Id.* at 7:38–43.

Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A computer apparatus distributing a communication over an Internet network, the apparatus including:
>
> a controller computer system adapted to communicate responsive to a respective authenticated user identity corresponding respectively to each of a plurality of participator computers,
>
> each said participator computer communicatively connected to said Internet network, each said participator computer programmed to enable the communication, the communication including at least one of a pre-stored sound, video, graphic, and multimedia,
>
> 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 the participator computers which are otherwise independent of each other;
>
> wherein
>
> one said authenticated user identity is used to communicate a pointer-triggered private message from a first of said participator computers to said controller computer and from said controller computer to a second of said participator computers that invokes said pointer-triggered private message to fetch and receive the communication from a computer other than said first or said second said

> participator computers in real time over the Internet network
>
> such that the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication, and otherwise presenting the communication independent of the first of the independent participator computers and the computer.

## II. ANALYSIS

### *A. Claim Construction*

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–45 (2016). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

#### *1. Constructions in the Institution Decision*

In the Institution Decision, we preliminarily construed the following terms (Dec. 6–9):

| **Claim Term** | **Preliminary Construction** |
|---|---|
| “token” | “piece of information associated with user identity” |
| “censored” | “controlled with respect to what is said in a group” |

Patent Owner adopts our construction of “token” (which Petitioner initially proposed), PO Resp. 8, and challenges our construction of “censored,” *id.* at 12–13. Petitioner accepts our construction of “censored” and presents arguments in favor of that construction. Reply 3. The parties also dispute the meaning of “database,” PO Resp. 8–12; Reply 3–6. Nevertheless, we determine that construction of these terms is not necessary to resolve the dispute in this proceeding. *See Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (“[O]nly those terms need be construed that are in controversy, and only to the extent necessary to resolve the controversy.”).

### *B. Asserted Grounds of Unpatentability*

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

In an obviousness analysis, some reason must be shown as to why a person of ordinary skill would have combined or modified the prior art to achieve the patented invention. *See Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008). A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the "interrelated teachings of multiple patents"; "any need or problem known in the field of endeavor at the time of invention and addressed by the patent"; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

### *1. Level of Ordinary Skill*

Neither party proposes a level of ordinary skill in the art. Nevertheless, both parties' experts testify to similar levels of skill. Specifically, Dr. Lavian testifies that a skilled artisan "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." Ex. 1002 ¶ 14. For his part, Dr. Carbonell testifies that a skilled artisan "would have had a bachelor's degree in

[2] The record does not include arguments or evidence regarding objective indicia of nonobviousness.

computer science (or a related field) and at least one year of work experience in programming in computer communication methods" and notes that his "opinions herein would not change even if the person having ordinary skill in the art were to be found to have the level of skill proposed by Dr. Lavian." Ex. 2005 ¶ 18. We adopt Dr. Lavian's proposal, as it is consistent with the level of skill reflected in the prior art of record. Nevertheless, we discern no material difference between his proposal and that of Dr. Carbonell. Thus, our findings and conclusions would be the same under either proposal.

### *2. Scope and Content of the Prior Art*

Petitioner contends that the challenged claims would have been obvious over Roseman, alone or in combination with Rissanen, Vetter, Pike, Westaway, and Lichty. Pet. 7–8; '709 Pet. 6.

#### *a. Overview of Roseman*

Roseman describes a system for multimedia conferencing, in which parties are linked by both video and audio media. Ex. 1003, Abstract. In Roseman, a conference is represented visually as a common virtual conference table, in which each participant can place a document onto the table electronically, manipulate and write on the document, write on a virtual notepad, and move a pointer to draw other users' attention. *Id.* at 2:38–45, 7:55–8:37. Participants can see the events as they occur. *Id.* at 2:46–47. Figure 9, reproduced below, illustrates an example conference room:

FIG. 9

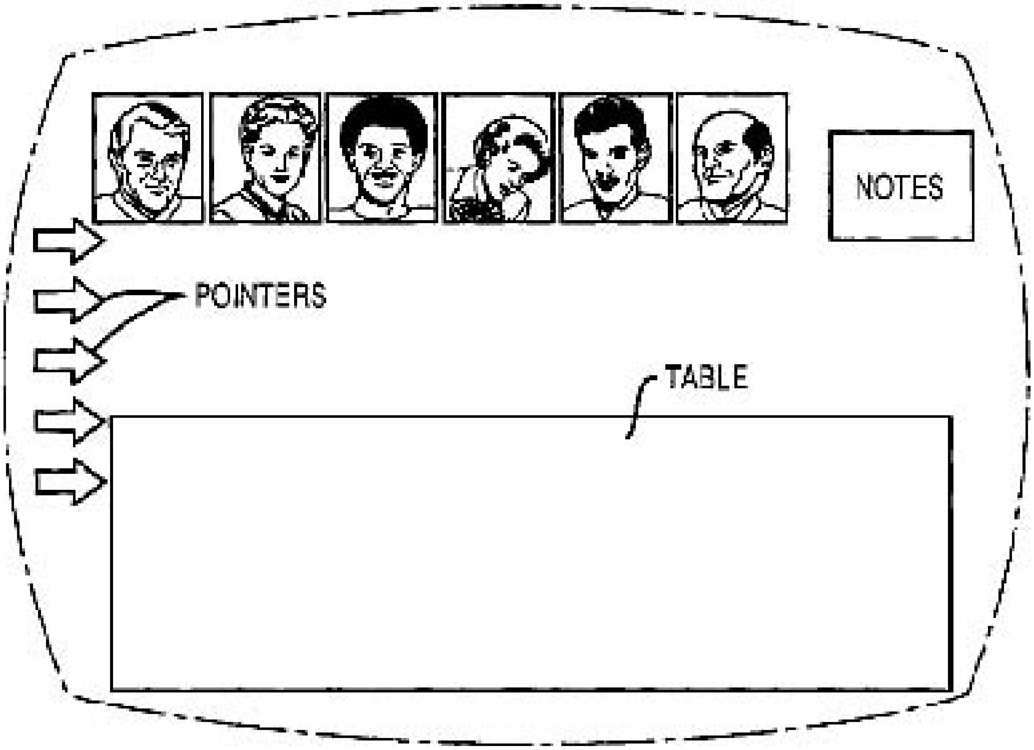


Figure 9 is a picture of a video screen that is generated by a host computer and distributed to all participants in a conference. *Id.* at 2:16–18.

The parties operate their own local computers (which include video cameras and speaker-type telephones) and, when a conference is established, connect to a host computer via commercially available local area networks (“LANs”) and wide area networks (“WANs”). *Id.* at 1:34–41. In the conference, the host computer generates a common video screen (e.g., Figure 9, reproduced above) displayed at each of the local computers, and the parties send information, such as drawings, to be displayed on the common screen. *Id.* at 1:42–46. The telephones and video cameras allow the parties to see and speak with each other. *Id.* at 1:47–49.

Roseman includes a pseudo code appendix that details how its features are implemented. *Id.* at 12:66–13:2. According to the pseudo code, a participant interacts with the conference table, for example, by dragging an icon onto the table, which causes a data file to be transmitted to the host. *Id.* at 14:53–55. The host then transmits the icon to the table of each participant. *Id.* at 14:56–57. If another participant activates the icon, the host sends the open file to the tables of all participants. *Id.* at 14:58–61. If the participant drags the icon from the table to his own screen and activates the icon on his screen, the data file is presented to the participant. *Id.* at 14:62–66.

Roseman describes additional features, such as a party's ability to "whisper" to another party without being heard by others in the conference room, and the ability to "pass notes" by dragging a note to the picture of another party, while the other parties are unaware of the note. *Id.* at 9:16–31. Each room may also have "doors" to committee rooms or child-rooms. A child-room is created in the same way as a parent room and is dependent upon the parent room for access and existence. *Id.* at 10:18–23.

A meeting requester creates a conference by selecting the participants, the attributes of the virtual conference room (e.g., virtual equipment and room décor), and the rules of the conference (e.g., whether the requester has absolute control over voice and message interaction of the parties). *Id.* at 3:22–56. According to Roseman, "[t]he conference room itself is actually a combination of stored data and computer programs," the stored data can include conference proceedings, and "both the conference room and the proceedings of the conference have persistence in time." *Id.* at 12:16–25.

The meeting requester specifies a level for each invitation and compiles an invitation list. *Id.* at 9:34–36. Invitations include "keys" specifying the level, e.g., whether the invitation is for the invitee only or can be passed to a delegate or to anyone. *Id.* at 9:35–48. For example, "Level 1 keys may not be passed to any other person and may not be copied" while "Level 2 keys may be passed to exactly one other person and may not be copied." *Id.* at 9:42–45. According to Roseman, "[t]he meeting room 'knows' about each key and its invitation level. Persons with improper keys are not admitted to the room." *Id.* at 9:49–51. A key is distributed electronically as an object attached to the invitation. *Id.* at 9:54–55. To attend a meeting, a party walks a virtual "hallway" to the meeting room and opens the meeting room door by dropping the key onto a virtual "door lock." *Id.* at 10:30–32, 10:61–65. Moreover, the host "can automatically prevent filibustering" by "monitor[ing] the speech of each person, and plac[ing] a limit on the total time allowed to each person." *Id.* at 12:29–38.

### *b. Overview of Rissanen*

Rissanen describes a system and method for validation of spoken passwords. Ex. 1004, 2:17–21. Rissanen's Background of the Invention discusses systems in which "business computer systems are arranged to initially record and store passwords assigned to users," a user is prompted for entry of a password, 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." *Id.* at 1:21–28. In Rissanen's proposed solution, "[u]sers 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." *Id.* at 2:26–29.

Petitioner makes clear that "[a]lthough Rissanen also describes using spoken voice passwords, this Petition cites it for its more pedestrian teachings relating to database storage of passwords of any form." Pet. 12.

### *c. Overview of Vetter*

Vetter is an IEEE Computer Society Magazine article discussing available tools for conducting teleconferencing over the Internet. According to Vetter, "[v]ideoconferences are becoming increasingly frequent on the Internet and are generating much research interest." Ex. 1005, 77. Vetter states that "the emerging multicast backbone (or MBone) can efficiently send traffic from a single source over the network to multiple recipients," and, "[a]t 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." *Id.* Vetter concludes that "[t]he 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." *Id.*

Vetter also describes challenges that faced implementation of audio, graphic, and video tools on the Internet, including "disturbing feedback when the microphones at multiple sites were left 'open' during a discussion," taking too much time to broadcast a simple graphic image to multiple participants when using "Whiteboard tools" (collaborative software tools that support a shared desktop whiteboard among a group of distributed users on the Internet), and use of video during a classroom presentation that

caused the workstations in the classroom lab to lock up. *Id.* at 78–79. Vetter also notes that the physical distance between two points on the Internet can be different from the electronic distance between those points. *Id.* at 79.

Vetter discusses in particular a CU-SeeMe platform from Cornell University that supported video and audio conferencing over the Internet, and a CU-SeeMe Reflector that allowed multiparty conferencing with CU-SeeMe. *Id.* at 78.

### *d. Overview of Pike*

Pike is a reference and guide book for using the Web browser Mosaic. Ex. 1006, 2. Petitioner cites to Pike's discussion of URLs and hyperlinks. According to Pike, URLs were developed as a standard way of referencing items on the World Wide Web. *Id.* at 38. "A *URL* is a complete description of an item, containing the location of the item that you want to retrieve. 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 also describes adding auxiliary software to Mosaic to allow Mosaic to handle documents it otherwise would not be able to handle. *Id.* at 55. For example, a user "may want to obtain additional software to allow Mosaic to handle things such as pictures, sounds, and animations (movies)" and could find such additional software at an anonymous FTP site identified in Pike. *Id.* at 55–56. According to Pike, "[a]fter you have a viewer installed and Mosaic knows where to find it and what type of files it displays, you can load files of that type and Mosaic automatically starts the viewer to display them." *Id.* at 96.

### *e. Overview of Westaway*

Westaway is directed to "methods and apparatus for automatically loading missing system software without terminating current processing operations being executed by the data processing device in a data processing system." Ex. 1007, 1:10–16. Specifically, Westaway describes a system including "a plurality of data processing devices ('agents')" coupled to a network. *Id.* at 1:18–20. "System software resources," such as a disk drive or optical storage device coupled to the network, provide system software to agents on the network. *Id.* at 1:20–24. "In the event an agent requires certain software for execution, and the software is not available on the agent's local hard disk drive or internal memory, then it [is] accessed from one of the system software resources such as a disk drive, tape drive or the like." *Id.* at 1:24–29.

### *f. Overview of Lichty*

Lichty is a book intended as a "tour guide" of America Online ("AOL"), an online email service, Internet gateway, and community. Ex. 1008, 1–3. Petitioner (Pet. 58–59) focuses on Lichty's description of AOL's real-time interactive "People Connection" feature. Ex. 1007, 251–78. People Connection includes chat rooms in which a user communicates with others by posting text messages to the other participants in a chat room. *Id.* at 252–55. Lichty describes, in particular, that a People Connection interface includes an "Ignore" button. *Id.* at 268–69. According to Lichty, "[i]f you wish to exclude a member's comments (or those of all the members in a 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." *Id.* at 269; *see also id.* at 510 (glossary definition of "Ignore—(1) Chat blinders; a way of blocking a member's chat from your view in a chat/conference room window. Ignore is most useful when the chat of another member becomes disruptive in the chat room.").

### *3. Claim 1, Differences Between the Claimed Subject Matter and the Prior Art, and Reasons to Modify or Combine*

For the reasons given below, we conclude that Petitioner has not shown that claim 1 would have been obvious over Roseman, Rissanen, Vetter, Pike, and Westaway.

Petitioner contends that Roseman teaches the majority of the limitations of claim 1, but cites the remaining references for the following, should we determine that Roseman lacks such a teaching:

> Rissanen for a teaching that tokens could have been stored in a database;
>
> Vetter for a teaching that Roseman's communications could have been over the Internet;
>
> Pike for a teaching of URLs; and
>
> Pike and Westaway teachings of external software applications used to view certain types of content.

Pet. 7–8.

Claim 1 recites "a controller computer system," including a "controller computer," that communicates with "each of a plurality of participator computers." Petitioner contends (Pet. 17) that Roseman describes a "host computer" that communicates with "local computers" that are used by the parties to a videoconference, the host computer overseeing the conference. Ex. 1003, 1:42–52; 3:14–19. With respect to the "Internet network" limitations, the Petition relies on combining the teachings of Roseman with Vetter. Pet. 17–19, 24. As Petitioner notes (*id.*), Vetter indicates explicitly that "[v]ideoconferences are becoming increasingly frequent on the Internet," and describes software that supports "video and audio conferencing over the Internet," including "multiparty conferencing." Ex. 1005, 77–78. Further, relying on Dr. Lavian's testimony, Petitioner asserts that a person of ordinary skill would have recognized Roseman's reference to connections via commercially available WANs to implicate the Internet. Pet. 17–18 (citing Ex. 1002 ¶ 51). According to Dr. Lavian, a person of ordinary skill in the art would have been motivated to combine the teachings of Roseman and Vetter, such that the videoconference communications described in Roseman occur over the Internet, based on the above disclosures of Vetter and Roseman, as well as the artisan's background knowledge regarding the Internet. Ex. 1002 ¶ 54.

As to "a respective authenticated user identity corresponding respectively to each of a plurality of participator computers," the Petition relies on Roseman's discussion of "keys" provided to invitees to a videoconference—for example, a "Level 1 key" that is restricted to a specific user only—which are used by the invitees to access the conference and enable communications among the users and the host computer. Pet. 21–23 (citing Ex. 1003, 9:34–55, 10:61–65, 11:10–17).

With respect to "a database which serves as a repository of tokens for other programs to access," as recited in claim 1, Petitioner cites to the combination of Roseman and Rissanen. Pet. 26–33. Petitioner contends that

Roseman's "keys" are blocks of data that are associated with users' identities and, thus, are tokens. *Id.* at 26–27. As explained above, Roseman describes that an invitor, in setting up a meeting, creates an invitation that includes a key that conforms to an invitation level. Ex. 1003, 9:34–48. A key "is an electronic object attached to the invitation." *Id.* at 9:54–55. The "level" of a key determines who can use it. For example, "Level 1 keys may not be passed to any other person and may not be copied." *Id.* at 9:42–44. According to Roseman, "[t]o 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." *Id.* at 10:61–64.

As to "a database which serves as a repository of tokens for other programs to access," as recited in claim 1, Petitioner argues that Roseman explains that each conference room "knows" about each key to that room, reasoning that Roseman, thus, teaches the host computer storing each key so users' keys can be recognized. Pet. 27–28 (citing Ex. 1003, 9:49–51; Ex. 1002 ¶ 68). Once a key is recognized and a user is granted access to a room, each of the participants in the room are notified of the user's entry, and data (e.g., the video signal of the user) is communicated to the participants. Ex. 1003, 10:61–65, 11:11–17. According to Petitioner, Roseman indicates that each virtual conference room provided by the host computer "is actually a combination of stored data and computer programs." Pet. 30 (quoting Ex. 1003, 12:16–18). Therefore, Petitioner asserts that Roseman teaches "other programs" (i.e., the conference rooms) accessing a central repository of tokens (i.e., keys), thereby affording information to each of the participator computers (i.e., communicating data to each participant in a conference).

Petitioner additionally argues that Rissanen teaches storing user authentication information, such as user identity information and passwords, in a database, and that such teaching would have been applicable to the keys of Roseman. Pet. 28–29. Petitioner argues that Roseman's keys are analogous to user identity and passwords. *Id.* Petitioner further argues that storing keys in a database is one of a finite number of known solutions for verifying whether a previously issued key matches to a key later presented by a user to access a conference room. Pet. 30 (citing Ex. 1002 ¶¶ 71–72).

As to "affording information to each of the participator computers," as recited in claim 1, Petitioner argues that Roseman describes allowing a user to communicate with others in the conference (e.g., by audio and video links, and by placing documents on a virtual table), upon that user being admitted via acceptance of a key. Pet. 31–32 (citing Ex. 1003, 8:1–4, 11:11–22).

Regarding participator computers that are "otherwise independent of each other," Petitioner argues that each of Roseman's local computers is independent of the others because the computers are located at different geographic locations and only become part of a virtual conference when connected to the host computer. Pet. 32–33 (citing Ex. 1003, 3:14–19).

The Petition identifies Roseman's description of conference participants placing a document or file onto the virtual conference table as an example of "communicat[ing] a pointer-triggered private message from a first of said participator computers to said controller computer and from said controller computer to a second of said participator computers," as recited in claim 1. Pet. 24–26, 34. Roseman describes a procedure where a participant in a conference can "drag-and-drop" a file from the participant's computer onto the table in the virtual conference room. Ex. 1003, 8:1–13, Figs. 10, 11. According to Roseman, the file may be "of any suitable kind: data, text, or graphic." *Id.* at 8:1–4. Roseman indicates that the participant may do this by dragging an icon "represent[ing]" the file. Ex. 1003, 8:1–13. When any participant "activates" the icon on the table, the file associated with the icon is "presented" on the table by the host computer and sent to all participants. *Id.* at 14:58–61. Petitioner contends that this icon is a "pointer-triggered message" because the icon contains information that points to and is used to present an underlying document. Pet. 35.

Petitioner further argues that, to the extent that a "pointer" requires an Internet URL or the like, a skilled artisan would have consulted Pike for a teaching of basic Internet concepts, such as URLs. Pet. 36–39. According to Petitioner, "[t]his 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." *Id.* at 36–37. Petitioner argues that Pike's URL would "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." *Id.* at 37. Petitioner argues that this would have saved bandwidth "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." *Id.* at 38. Thus, Petitioner argues that Roseman's icon causes the second participator computer to fetch and receive the underlying content by virtue of the host fetching and receiving the content and forwarding it to the second participator computer. *Id.* at 41.

The parties dispute whether the prior art teaches

> such that the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication,

as recited in claim 1. PO Resp. 36–38; Reply 22–23. Petitioner concedes that "Roseman does not appear to contemplate the scenario in which the second participant computer ***internally determines that it <u>cannot</u> present the communication***." Pet. 43. According to Petitioner, however the combination of Roseman, Pike, and Westaway teaches these limitations. *Id.* at 42–50.

Specifically, Petitioner contends that Pike "discloses the '**determining**' and '**obtaining**' steps" of claim 1. *Id.* at 44. Petitioner argues that Pike "explains that there may be occasions when a user receives information over the Internet but his or her computer lacks the software needed to view it." *Id.* at 43 (citing Ex. 1006, 55–56). Here, Pike notes that, while the Mosaic Web browser displays normal Web documents, it might not handle things like pictures, sounds, and movies. Ex. 1006, 55. In those instances, Pike explains, a user could obtain additional software to handle such things at an anonymous FTP site, using an address Pike specifies. *Id.* at 55–56. As Petitioner notes, Pike explains that once a user has installed an external viewer in Mosaic, Mosaic knows where to find the viewer and automatically invokes it to display files supported by the viewer. Pet. 44

(citing Ex. 1006, 96). According to Petitioner, this functionality teaches that a computer with Mosaic must internally determine that it cannot display a file because "if it cannot read the file using Mosaic, and it cannot locate an appropriate viewer application, it cannot present the communication." *Id.* Here, Petitioner assumes that the claim language does not require the "obtaining" limitation to be performed automatically without user involvement—in other words, Petitioner argues that the "obtaining" limitation is satisfied by a user manually obtaining and installing an agent with an ability to present a communication after a participator computer internally determines that it cannot present the communication. *Id.* at 45.

Alternatively, if we determine that the claim language requires the "obtaining" limitation to be performed automatically, Petitioner contends that this is taught by Westaway. *Id*. Westaway explains in its Background of the Invention, that, in the event that a software data processing agent lacked certain software necessary to execute a file, the agent would attempt to access that software from a disk drive, tape drive, or the like. Ex. 1007, 1:24–29. Petitioner contends that this shows an agent automatically obtaining requisite software if there has been a determination that the system cannot execute a certain process. Pet. 47. Westaway's Background further explains that, when an executing process would attempt to use software that had not yet been loaded onto the system's software resources, the system would generate a "file not found" message instead of finding and loading the required programs without causing a termination of the executing process. Ex. 1007, 1:47–51, 1:64–2:2. Petitioner argues that this evidences an agent that internally determines whether or not it can present the file. Pet. 46. Petitioner notes that "[a]lthough Westaway does not expressly disclose that the software determined to be missing and then obtained can include software for 'present[ing] [] communication,' that was already disclosed by Pike, as explained previously, which expressly contemplates that additional software may be required to present certain types of communications." *Id.* at 47.

Petitioner contends that it would have been predictable to combine Roseman, Pike, and Westaway. *Id.* at 47–48. Petitioner argues that "it was routine that a user could receive a document from someone else but be unable to open or access it because the user lacked the correct software" and that this would have been particularly applicable to Roseman because its system allowed a participant to drag and drop an icon of a document onto a table of a virtual conference room. *Id.* at 48. Petitioner contends that the teachings of Pike and Westaway would have been applied because of the possibility that a meeting participant would place a document on the table that other participants would not have the correct software to view. *Id.* at 49. In those instances, Petitioner argues, the skilled artisan would have followed the teachings of Pike and Westaway to obtain an external viewer software to handle files not supported by the participant's already-installed software. *Id.*

In response, Patent Owner argues that the '245 patent only describes these limitations in the context of participator software invoking an external data type viewer on demand of the operator of the participator software. PO Resp. 34–36 (citing Ex. 1001, 7:34–55). This is consistent with the language of claim 1, which recites "the *second of said participator computers* internally determines whether or not the second of the participator computers can present the communication" and "if it is determined that the *second of the participator computers* can not present the communication then obtaining an agent with an ability to present the communication." Patent Owner argues that "Petitioner does not identify any software on the users' computers that could qualify as participator software" and contends that Roseman actually teaches the contrary and describes "that all graphics are generated on the host computer." *Id.* at 36 (citing Ex. 1003, 1:43–46, 14:48–50).

In the passages cited by Patent Owner, Roseman describes a host receiving communications from participant computers and generating a common video screen, which it sends to all of the participator computers:

> 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.

Ex. 1003, 1:43–46. Other disclosure in Roseman confirms that its system operates in this manner. *Id.* at 7:30–34 ("[T]he host 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.").

The portions of Roseman cited by Petitioner (Pet. 42–43) also support Patent Owner's explanation of Roseman's system. For example, in its description of placing documents on a conference table, Roseman states that "[e]ach 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." Ex. 1003, 8:1–4. Roseman's pseudo code, which both parties cite (PO Resp. 36; Pet. 42–43), makes clear that documents are received by the host and communicated to all of the participants as a common display:

```
IF PARTICIPANT DRAGS ICON TO THE TABLE ON HIS SCREEN
    ICON (DATA FILE) TRANSMITTED TO HOST
    HOST TRANSMITS ICON (DATA FILE) TO TABLE OF EACH PARTICIPANT
IF ANY PARTICIPANT ACTIVATES ICON ON TABLE
    DATA FILE PRESENTED ON TABLE BY HOST
    HOST SENDS OPEN FILE TO ALL PARTICIPANTS TABLES
```

Ex. 1003, 14:53–62.

The disclosure in Roseman cited by both Petitioner and Patent Owner describes that the software that processes and renders images operates on Roseman's host. Indeed, Petitioner admits that "Roseman does not appear to contemplate the scenario in which the second participant computer ***internally determines that it cannot present the communication***." Pet. 43. Thus, Petitioner must show that this feature is taught elsewhere and that a skilled artisan would have had reason to combine that teaching with Roseman.

We are not persuaded that Pike provides that teaching. Petitioner relies on a description in Pike that a user could manually seek and install software to add to Mosaic. Pet. 43–44. Petitioner, however, does not explain why a skilled artisan would have incorporated this feature into Roseman's local computers (participator computers) in light of Roseman's system, which processes images at the host, not the local computers. The most logical reading of Roseman is that its local computers already have software sufficient to render the common image that the host provides to them. Thus, Petitioner's argument that Pike and Westaway would have been applied because of the possibility that a meeting participant would place a document on the table that other participants would not have the correct software to view (Pet. 49) is not applicable to Roseman. Petitioner has not explained why, in the case where the *host* is unable to present a communication received from a local computer as part of its common image, a local computer would make an internal determination to that effect, or why users at the local computers would seek out software to present the communication.

Petitioner's arguments with respect to Westaway suffer from the same deficiencies. Although Petitioner cites to Westaway for a teaching of a program determining that it cannot present a communication and obtaining software that can (Pet. 45–47), Petitioner does not explain persuasively why a skilled artisan would have applied these teachings to Roseman such that Roseman's local computers would have implemented the functionality.

Petitioner simply states, without persuasive reasoning or evidence, that "[i]t would have been obvious to adapt the teachings of Pike and Westaway to Roseman, predictably resulting in the videoconferencing system of Roseman in which participant local computers determine whether or not they can present a particular communication." Pet. 48. Petitioner cites only to Dr. Lavian, who merely repeats Petitioner's argument, nearly verbatim, without citation to the basis for his testimony. *Id.* (citing Ex. 1002 ¶ 101). Thus, Dr. Lavian's testimony does not add materially to Petitioner's unpersuasive attorney argument. Moreover, Petitioner's position on this limitation is inconsistent with its arguments as to the "pointer-triggered private message" limitation, in which Petitioner argues for a system in which "a person of ordinary skill in the art [would] 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 [a] second meeting participant computer over the Internet" (i.e., Petitioner concedes it is the host in Roseman that fetches the requested content, not the local computers). *Id.* at 37.

At most, Petitioner's contentions establish that a skilled artisan applying Pike's and Westaway's teachings to Roseman's system would have modified Roseman's host to seek out appropriate software to process communications it otherwise could not present. Petitioner has not shown that a skilled artisan would have further modified Roseman's system to move this processing from the host to each individual local computer and has not provided any persuasive reason to make such a modification.

Therefore, we find that Petitioner has not shown that Roseman, Pike, and Westaway teach

> such that the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication,

as recited in claim 1. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claim 1 would have been obvious over Roseman, Rissanen, Vetter, Pike, and Westaway.

#### *4. Claims 7 and 19*

Independent claims 7 and 19 are apparatus claims similar in most respects to claim 1. In particular, claim 7 recites

> the second of the participator computers determines internally whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication;

and claim 19 recites

> the second participator computer internally determines whether or not the second participator computer can present the pre-stored data, if it is determined that the second participator computer can not present the pre-stored data then obtaining an agent with an ability to present the pre-stored data.

Petitioner contends that these limitations are taught by Roseman, Pike, and Westaway for the same reasons, detailed above, Petitioner gives for the corresponding limitation of claim 1,

> such that the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication.

Pet. 55; ’709 Pet. 48–55 (substantially copying Pet. 42–49).

For the reasons given above, Petitioner has not shown that Roseman, Pike, and Westaway teach this limitation of claim 1. For the same reasons, Petitioner has not shown that Roseman, Pike and Westaway teach the corresponding limitations of claims 7 and 19. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claims 7 and 19 would have been obvious over Roseman, Rissanen, Vetter, Pike, and Westaway.

### *5. Claims 6 and 8*

Claims 6 and 8 depend from claims 1 and 7, respectively, and add "wherein the computer system further determines that the message is not censored."

Petitioner argues that this limitation would have been obvious over Roseman and Lichty. Pet. 57–60. Nevertheless, Petitioner's evidence and argument for this limitation do not overcome the deficiencies noted above for claims 1 and 7. Thus, Petitioner has not demonstrated, by a preponderance of the evidence, that claims 6 and 8 would have been obvious over Roseman, Rissanen, Vetter, Pike, Westaway, and Lichty.

### *6. Remaining Challenged Dependent Claims*

We have analyzed Petitioner's evidence and argument for claims 2–5, 9–15, 17, 18, 22–25. Pet. 50, 55–57, 61–63; '709 Pet. 56–58. Petitioner's evidence and argument for the additional limitations of these dependent claims do not overcome the deficiencies noted above for claims 1, 7, and 19. Thus, Petitioner has not demonstrated, by a preponderance of the evidence, that claims 2–5, 9–14, and 22–25 would have been obvious over Roseman, Rissanen, Vetter, Pike, and Westaway, or that claims 15, 17, and 18 would have been obvious over Roseman, Rissanen, Vetter, Pike, Westaway, and Lichty.

## III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner filed a paper styled "Motion to Exclude Evidence," seeking to exclude certain portions of the 2nd Lavian Declaration that it argues exceeds the proper scope of a reply. Paper 38, 1. In particular, Patent Owner seeks to exclude portions of paragraphs 54 and 74 of the 2nd Lavian Declaration. *Id.* at 2–4. Petitioner opposes this motion on the ground that it is not directed to the admissibility of evidence and, therefore, is procedurally improper. Paper 41, 2. We do not consider paragraphs 54 and 74. Moreover, even if we were to consider the evidence Patent Owner seeks to exclude, Petitioner still has not shown, by a preponderance of the evidence, that any claim of the '245 patent is unpatentable. Accordingly, we dismiss Patent Owner's Motion to Exclude as moot.

## III. CONCLUSION

Petitioner has not proved by a preponderance of the evidence that claims 1–15, 17–19, and 22–25 are unpatentable.

## IV. ORDER

For the reasons given, it is:

ORDERED, that Petitioner has not shown, by a preponderance of the evidence, that claims 1–15, 17–19, and 22–25 are unpatentable;

FURTHER ORDERED, that Patent Owner's Motion to Exclude is dismissed as moot; and

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

PETITIONER:

Heidi Keefe
Phillip E. Morton
Andrew C. Mace
COOLEY LLP
hkeefe@cooley.com
pmorton@cooley.com
amace@cooley.com

PATENT OWNER:

Peter Lambrianakos
Vincent Rubino
BROWN RUDNICK LLP
plambrianakos@brownrudnick.com
vrubino@brownrudnick.com

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

Paper 47
Entered: December 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FACEBOOK, INC.,
Petitioner,

v.

WINDY CITY INNOVATIONS, LLC,
Patent Owner.

Case IPR2016-01157
Patent 8,407,356 B1

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

MCKONE, *Administrative Patent Judge*.

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

## I. INTRODUCTION

### *A. Background*

Facebook, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") to institute an *inter partes* review of claims 1–9, 12, 14–28, 31, and 33–37 ("the challenged claims") of U.S. Patent No. 8,407,356 B1 (Ex. 1001, "the '356 Patent"). Windy City Innovations, LLC ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp.").

Pursuant to 35 U.S.C. § 314, in our Institution Decision (Paper 7, "Dec."), we instituted this proceeding as to claims 1–9, 12, 14–28, 31, and 33–37.

Patent Owner filed a Patent Owner's Response (Paper 22, "PO Resp."), and Petitioner filed a Reply to the Patent Owner's Response (Paper 31, "Reply").

Petitioner relies on the Declarations of Tal Lavian, Ph.D. (Ex. 1002, "Lavian Decl."; Ex. 1021, "2nd Lavian Decl."). Patent Owner relies on the Declaration of Jaime G. Carbonell, Ph.D. (Ex. 2005, "Carbonell Decl.").

An oral argument was held on October 19, 2017 (Paper 46, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 1–9, 12, 14–28, 31, and 33–37. Based on the record before us, Petitioner has proved, by a preponderance of the evidence, that claims 1–9, 12, 15–28, 31, and 34–37 of the '356 patent are unpatentable, but has not proved that claims 14 and 33 are unpatentable.

### *B. Related Matters*

The parties indicate that the ’356 patent has been asserted in *Windy City Innovations, LLC v. Microsoft Corp.*, Civ. A. No. 15-cv-00103-GM (W.D.N.C.) (transferred to 16-cv-1729 (N.D. Cal.)), and *Windy City Innovations, LLC v. Facebook, Inc.*, Civ. A. No. 15-cv-00102-GM (W.D.N.C.) (transferred to 16-cv-1730 (N.D. Cal.)). Pet. 1; Paper 4, 1. The ’356 patent was the subject of *inter partes* review petitions in IPR2016–01067. Paper 4, 1. The ’356 patent also was the subject of IPR2017-00624, which Microsoft Corp. filed and sought to join with this proceeding prior to settling with Patent Owner. Patents related to the ’356 patent are subjects of additional *inter partes* review petitions.

### *C. Asserted Prior Art References*

Petitioner relies on the following prior art:

U.S. Patent No. 6,608,636 B1, issued Aug. 19, 2003, filed May 13, 1992 (Ex. 1003, “Roseman”);

Published European Pat. App. No. 0 621 532 A1, published Oct. 26, 1994 (Ex. 1004, “Rissanen”);

Ronald J. Vetter, *Videoconferencing on the Internet*, IEEE COMPUTER SOCIETY 77–79 (Jan. 1995) (Ex. 1005, “Vetter”);

MARY ANN PIKE ET AL., USING MOSAIC (1994) (Ex. 1006, “Pike”); and

James Gosling, *Java Intermediate Bytecodes*, ACM SIGPLAN WORKSHOP ON INTERMEDIATE REPRESENTATIONS (IR ’95), VOL. 30, NO. 3 ACM SIGPLAN NOTICES 111–18 (Mar. 1995) (Ex. 1007, “Gosling”).

*D. The Instituted Grounds*

We instituted a trial on the following grounds of unpatentability (Dec. 27):

| References | Basis | Claims Challenged |
|---|---|---|
| Roseman, Rissanen, and Vetter | § 103(a) | 1–5, 8, 9, 12, 14–16, 19–24, 27, 28, 31, 33–35, and 37 |
| Roseman, Rissanen, Vetter, and Pike | § 103(a) | 6, 7, 17, 26, and 36 |
| Roseman, Rissanen, Vetter, and Gosling | § 103(a) | 18 and 25 |

*E. The '356 Patent*

The '356 patent describes an Internet "chat room." According to the '356 patent, it was known to link computers together to form chat rooms in which users communicated by text, graphics, and multimedia, giving the example of the Internet service provider "America On Line." Ex. 1001, 1:46–52. The '356 patent acknowledges that chat rooms have been implemented on the Internet, albeit with "limited chat capability," but contends that the complex chat room communications capable with Internet service providers had not been developed on the Internet "at least in part because [the] Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications" and because "there is no particular control over the platform that would be encountered on the Internet." *Id.* at 1:54–56, 1:60–62.

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

FIG. 1

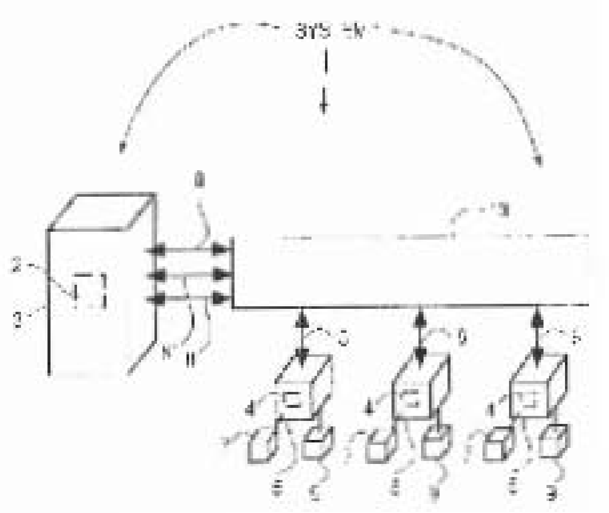


Figure 1 is a block diagram showing the components and data flow of a computerized human communication arbitrating and distributing system. *Id.* at 4:62–66. The system includes controller computer 3 in communication with several participator computers 5 (e.g., IBM-compatible personal computers) over connection 13 (e.g., an Internet connection or a World Wide Web connection). *Id.* at 4:67–5:20.

Controller computer 3 runs under the control of controller software 2, and the software arbitrates, in accordance with predefined rules (including user identities), which participator computers 5 can interact in a group through the controller computer, and directs real-time data to the members of the group. *Id.* at 5:21–27. The software uses “identity tokens,” or pieces of information associated with user identity, in the arbitration. *Id.* at 8:9–12.

The tokens are stored in a memory in a control computer database along with personal information about the users. *Id.* at 8:12–17.

The arbitration can be used to control a user's ability to join or leave a group of participator computers, to moderate communications involving the group, and to see other users in the group. *Id.* at 8:24–37. Arbitration using tokens also can be used to perform censorship:

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

*Id.* at 8:39–47.

According to the specification, "[t]he present invention comprehends communicating all electrically communicable multimedia information as Message 8, by such means as pointers, for example, URLs. URLs can point to pre-stored audio and video communications, which the Controller Computer 3 can fetch and communicate to the Participator Computers 5." *Id.* at 5:38–43.

Figure 2, reproduced below, represents an overview of the communications described in the '356 patent.

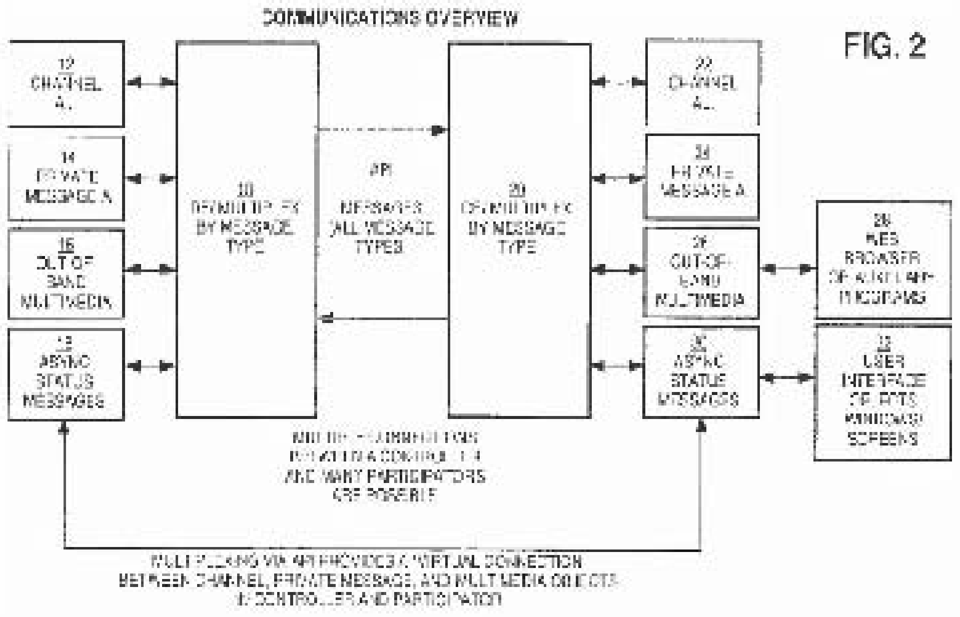

COMMUNICATIONS OVERVIEW
12 CHANNEL A
14 PRIVATE MESSAGE A
16 OUT OF BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DEMULTIPLEX BY MESSAGE TYPE
API
MESSAGES (ALL MESSAGE TYPES)
20 DEMULTIPLEX BY MESSAGE TYPE
22 CHANNEL A
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILIARY PROGRAMS
32 USER INTERFACE OF PC'S WINDOWS SCREENS
MULTIPLE INTERCONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A VIRTUAL CONNECTION BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

FIG. 2

Figure 2 is a block diagram that provides a communications overview. *Id.* at 2:63–64. Blocks 10, 12, 14, 16, and 18 in Figure 2 illustrate operations under controller software 2, and Blocks 20, 22, 24, 26, and 30 illustrate operations under participator software 4. *Id.* at 5:45–54, 5:58–6:2. For example, Block 14 represents the handling of a private message. *Id.* at 5:50–51.

Block 10 and Block 20 illustrate software multiplexing and demultiplexing of API messages by message type on the controller computer and a participator computer, respectively. *Id.* at 5:46–48, 5:59–61.[1] Multiplexing and demultiplexing the API messages, according to the ’356

[1] The ’356 patent does not specifically state what the acronym “API” represents, but the parties essentially agree that API messages represent messages of different types as discussed further below. Ex. 1002 ¶ 33; Ex. 1010 ¶ 8 (Patent Owner’s declarant asserting during prosecution that the ’356 patent “specification . . . never uses the term ‘application program interface’”).

patent, creates a "virtual connection" between different functions on the controller computer (e.g., a private message) and participator computer such that each function does not need to handle its own connection separately. *See id.* at 6:3–9.

In particular, the '356 patent states "[d]e/multiplexing via API provides a 'virtual connection' between Channel, Private message, and Multimedia objects in the controller computer 3 and each participator computer 5." *Id.* at 6:3–5. In essence, the API multiplexing system routes messages together, and a demultiplexor at the participator computer separates them according to message type in accordance with a particular function associated with that message type. *See id.* at Fig. 2, 5:44–54, 6:3–5. As background prior art, the '356 patent states "corporations may link remote offices to have a conference by computer . . . . [with a] central computer . . . control[ling] the multiplexing of what appears as an electronic equivalent to a discussion involving many individuals," but "[m]ultiplexing in multimedia is more complex." *Id.* at 1:42–45.

Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method of communicating content among users using of [sic] a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method comprising:
>
> authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database;

> 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;
>
> running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers;
>
> providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers; and
>
> communicating real-time messages within the group of the interactively connected said participator computers.

## II. ANALYSIS

### *A. Claim Construction*

We interpret claim terms in an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–45 (2016). In applying a broadest reasonable construction, claim terms generally carry their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

### 1. *Constructions in the Institution Decision*

In the Institution Decision, we preliminarily construed the following terms (Dec. 7–9):

| **Claim Term** | **Preliminary Construction** |
|---|---|
| "token" | "piece of information associated with user identity" |
| "channel" | "group of participator computers in active communication" |
| "censorship" | "control of what is said in a group" |

Neither party challenges our construction of "channel," and we maintain that construction on the complete record. Patent Owner adopts our construction of "token" (which Petitioner initially proposed), PO Resp. 8, and challenges our construction of "censoring," *id.* at 13. Petitioner accepts our construction of "censoring" and presents arguments in favor of that construction. Reply 3. We maintain our construction of "token" on the complete record. We address the construction "censoring" below. The parties further dispute the meaning of "database," PO Resp. 8–12; Reply 3–7, and we construe that term below. We also construe "multiplexing and demultiplexing API messages by type" to resolve the parties' dispute with respect to this term.

### 2. *"censorship"*

Dependent claims 14 and 33 recite "censorship of the content"; dependent claims 15 and 34 recite "determines censorship." As noted above, we preliminarily construed "censorship" to mean "control of what is said in a group." Dec. 9–10. We further explained that Patent Owner had not shown that "censorship" should be construed to exclude controlling user access rights or censorship of users. *Id.* at 10. We based our construction on the description of that term in the specification. *Id.* Specifically, the specification of the '356 patent describes censorship as follows:

> Censorship, which *broadly encompasses control of what is said in a group*, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

Ex. 1001, 8:39–47 (emphasis added). Here, the specification describes "censorship" as "broadly encompass[ing] control of what is said in a group" and includes an example in which an action is taken on a user, rather than the data itself.

Patent Owner argues that censorship should be construed to mean "examine in order to suppress or delete anything considered objectionable." PO Resp. 13. According to Patent Owner, "[i]n order to control what is said in a group, it is necessary to first know what is said (or proposed to be said)." *Id.* Patent Owner argues that this is consistent with the meaning given to "censor" and "censorship" in dictionaries, including "to examine in order to suppress or delete anything considered objectionable" (Webster's Collegiate Dictionary (Ex. 2002)) and "[t]he action of preventing material that a party considers objectionable from circulating within a system of communication over which that party has some power" (Microsoft Press Computer Dictionary (Ex. 2003)).

We are not persuaded by Patent Owner's arguments. The claim language itself does not support a construction of "censorship" limited to analysis of the content of data and suppression based on that content. Claim 15, for example, recites only that "the controller computer *determines censorship*," and does not recite that censoring is based on any analysis of the content of the message to determine whether it is objectionable. To the extent Patent Owner's dictionary definitions suggest a narrower meaning, extrinsic evidence such as dictionary definitions "may be used only to help the court come to the proper understanding of the claims; it may not be used to vary or contradict the claim language." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1584 (Fed. Cir. 1996); *accord Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005) (en banc) ("[W]hile extrinsic evidence can shed useful light on the relevant art, we have explained that it is less significant than the intrinsic record in determining the legally operative meaning of claim language." (internal citations and quotation marks omitted)).

On the complete record, in accordance with the specification's definition, "censorship" means "control of what is said in a group." "Censorship," by itself, is not limited to examining data to determine whether it is objectionable.

As noted above, claims 14 and 33 recite "determin[es/ing] censorship of the content." Here, the broad term "censorship" is modified by the term "of the content." This is consistent with the example in the specification, cited above, that "[c]ensorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject." Ex. 1001, 8:45–47. In this example, the censorship is based on the characteristics of the data itself, including determining what type of data it is (e.g., text or video) and does not simply involve blocking all communications from or to a particular user. Moreover, claims 2 and 20 depend from claims 1 and 19, respectively, and recite "wherein the communicating content includes communicating at least one of sound, video, pointer and multimedia content." This further shows that content refers to the type of data, so that censorship of content is directed to censoring content based on characteristics such as the type of data. Thus, "determining censorship of the content" is narrower than censorship generally, and means "determining whether to communicate content based on characteristics of the content."

### 3. *"database"*

Neither party proposed construing "database" prior to institution. Nevertheless, in related proceedings, for similar claims of related patents, we construed "database" to mean "a collection of logically related data." *See, e.g.*, Case IPR2016-01158, Paper 7, 9–10 (for claims of U.S. Patent No. 8,473,552 B1); Case IPR2016-01159, Paper 7, 9–10 (for claims of U.S. Patent No. 8,694,657 B1). Patent Owner challenges our preliminary construction of "database" in those proceedings and echoes its arguments in this proceeding. Specifically, Patent Owner contends that "a database should be construed as 'a collection of logically related data which is stored with persistence and associated tools for interacting with the data such as a DBMS.'" PO Resp. 12. In essence, Patent Owner urges a construction that differs from our preliminary construction in related matters in two regards: (1) Patent Owner contends that a database is a collection of logically related data "which is stored with persistence"; and (2) Patent Owner contends that a database includes "associated tools for interacting with the data such as a DBMS." PO Resp. 12.

Patent Owner's primary argument in favor of construing "database" to require these limitations is that it filed, in a related application before the Patent Office, an information disclosure statement (IDS) that supports its construction. *Id.* at 9–10 (citing Ex. 2008). The IDS was submitted to the Patent Office in pending application 14/246,965 on January 1, 2017, after Petitioner filed the Petition and shortly after we instituted this proceeding and preliminarily rejected Patent Owner's claim construction arguments in related proceedings. In the IDS, Patent Owner argued, *inter alia*, that "attention is respectfully drawn to the defendants' contentions[2] of invalidity in view of the database and 'other programs' limitations that are common to all claims" and that "[b]ecause the database affords information to other programs and computers, it must store the data, such as the tokens, with persistence, such that tools can interact with the data such as a DBMS when providing the data to the participator computers of the authenticated users." Ex. 2008, 2. Patent Owner argues that we must accept its construction pursuant to *Verizon Services Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1306 (Fed. Cir. 2007), which held that, in some circumstances, a statement made by a patentee in the prosecution history of a related application can operate as a disclaimer, even if the disclaimer occurred after the patent-in-suit had issued. PO Resp. 10.

[2] This appears to be a reference to invalidity contentions filed in a related district court proceeding.

Although we doubt that the Federal Circuit intended that an IDS in a related application should be a vehicle for overturning a disadvantageous claim construction in an adversarial proceeding,[3] we need not reach that issue. As the Federal Circuit also held, "[t]o operate as a disclaimer, the statement in the prosecution history must be clear and unambiguous, and constitute a clear disavowal of claim scope." *Verizon*, 503 F.3d at 1306. That is not the case here. The statements in Patent Owner's IDS are not in response to any rejection by the Examiner, do not accompany any amendments, and are not directed to any particular claims, other than a general statement that the statements apply to "all claims."[4] Ex. 2008, 2.

[3] *See Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1270 (Fed. Cir. 1986) ("A citation may be made at 'any time' either during prosecution or, as here, after the patent has issued. If made during prosecution, it is clear that the statements may be considered for claim interpretation purposes, just as any other document submitted during prosecution. If submitted after issuance, the answer, again, is it may be considered. To say that it *may* be considered is not to say what *weight* statements in the Citation are to be accorded. For example, a Citation filed during litigation might very well contain merely self-serving statements which likely would be accorded no more weight than testimony of an interested witness or argument of counsel. Issues of evidentiary weight are resolved on the circumstances of each case."); *Phillips*, 415 F.3d at 1317 ("Like the specification, *the prosecution history provides evidence of how the PTO and the inventor understood the patent*. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes." (emphasis added)).

[4] Adding to the ambiguity, it is not clear whether the IDS's reference to "all claims" refers to the claims in the pending application or the claims discussed in the defendants' contentions of invalidity to which the sentence is directed.

*See Phillips*, 415 F.3d at 1317 ("Like the specification, *the prosecution history provides evidence of how <u>the PTO and the inventor</u> understood the patent*. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes." (emphasis added)).

Although Patent Owner argues that the IDS "supports the construction that a database is limited" in the manner that it argues, Patent Owner does not contend that the IDS constitutes a disclaimer of any subject matter. PO Resp. 9–10. We find that the IDS does not contain a "'clear and unmistakable' disclaimer that would have been evident to one skilled in the art." *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1064 (Fed. Cir. 2016). Therefore, we are not persuaded that we should apply prosecution history disclaimer to limit the scope of the term "database."

Patent Owner also cites to the testimony of Dr. Carbonell that "[t]wo hallmarks of a database are (1) persistence of the data, and (2) interactivity with the data via a database management system (DBMS)." *Id.* (citing Ex. 2005 ¶ 33). In support, Patent Owner and Dr. Carbonell cite to the Macmillan Encyclopedia of Computers (Ex. 2004). PO Resp. 10–11; Carbonell Decl. ¶ 33. In the portion included in Exhibit 2004, The Macmillan Encyclopedia states that "[a] database system is a collection of related records stored in a manner that makes the storage and retrieval of the data very efficient. The four well-known data models for databases are the hierarchical, network, relational, and object-oriented models." Ex. 2004, 230. This definition does not require persistence and Patent Owner does not explain why persistence should be inferred from this definition. Dr. Lavian, in turn, cites to a 1991 textbook, which defines "database" as "a collection of interrelated data," a definition that does not require "persistence." Ex. 1021 ¶ 12 (quoting Ex. 1017 ("Korth"), 5). Moreover, we observe that Patent Owner provides no boundaries for "stored with persistence" to meaningfully limit the term. For example, all data accessed and stored by a program while the program is executing has some level of "persistence."

As to a DBMS, Macmillan explains:

> A database management system (DBMS) is a software package. Its main functions are (1) to provide the facility to set up the database, (2) to retrieve and store source data (actual data in the database), (3) to retrieve and store the data about the structure of the database (data dictionary), (4) to provide the facilities to enforce security rules, (5) to back up the database, and (6) to control the concurrent transactions so that one user's environment is protected from others.

Ex. 2004, 231. Patent Owner characterizes the DBMS as "another criteria of a database" that provides interactive querying capability not present in "[s]tandard storage" in temporary or permanent memory. PO Resp. 11. Dr. Carbonell repeats Patent Owner's arguments without citation to evidence. Ex. 2005 ¶¶ 33–36. Nevertheless, we read Macmillan to describe a DBMS as software that works with a database, rather than a part of a database or a component that necessarily accompanies a database. Dr. Carbonell's testimony, which does not identify its bases, adds little to Macmillan. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Patent Owner also argues that the disclosure of the '356 patent imposes "persistence" and DBMS limitations on the claimed database because it describes the database as storing security information such as tokens for other programs to access. PO Resp. 12. Patent Owner does not provide a citation to the ’356 patent in support of its argument. Nevertheless, Patent Owner argues, again without citation, that “[o]ne of ordinary skill in the art would have expected that this type of security feature would persist in a location other than in program memory so that other user programs could access the information.” *Id.* Finally, Patent Owner argues that the ’356 patent describes tokens stored in hierarchies, which, according to Patent Owner, “are typical of database storage organization, and natural schema when storing and managing access to diverse information.” *Id.* None of these arguments supports reading persistence or a DBMS into the term “database.” We note also that the other claim language, “serves as a repository of tokens for other programs to access,” is a requirement we evaluate separately and do not read into the term “database.”

The specification describes a database consistently with the Macmillan and Korth definitions, explaining that tokens are “pieces of information associated with user identity,” that tokens are “stored in memory 11 in a control computer database, along with personal information about the user,” and that “[i]n the database, the storage of tokens can be by user, group, and content.” Ex. 1001, 8:9–21. The specification does not require a DBMS (or similar software) or impose a persistence requirement.

On the complete record, we construe database to mean “a collection of logically related data.” This is the construction most consistent with both the intrinsic evidence and dictionary definitions. However, we note that Petitioner contends, and we find, that the prior art shows a database with persistence and associated tools for interacting with the stored data, as explained below.

### 4. *"multiplexing and demultiplexing API messages by type"*

Claim 1 recites "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type." Petitioner contends that the Background of the Invention section of the '356 patent describes "multiplexing" as transporting messages from different messaging technologies (e.g., email, conferencing, and chat messages) using a shared communications pathway. Pet. 8–9 (citing Ex. 1001, 1:34–52). Petitioner further points to Figure 2 (reproduced above) and its corresponding description, as supporting this framework. *Id.* at 11–12 (citing Ex. 1001, 5:45–48). Petitioner further argues that "'demultiplexing' would be understood as the reverse of multiplexing, i.e. separating an individual message from the combined signal carried by the communications pathway to deliver it to the intended recipient." Pet. 9.

Describing Figure 2, as it pertains to the controller computer, the specification explains:

> Beginning with the Controller Computer Software 2, reference is made to Block 10, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block 10 links to Block 12, which is illustrative of channel A . . . . Block 10 also links to Block 14, which illustrates handling private message A. Block 10 also links to Block 16, illustrative of handling out-of-band media. Block 10 additionally links to Block 18, which illustrates asynchronous status messages.

Ex. 1001, 5:45–54 (ellipses in original). As Petitioner points out (Pet. 12), the specification further describes demultiplexing by message type:

> From a message that is demultiplexed by message type, there are six possibilities: ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVE CHANNEL, AND MODMSG. ERROR MESSAGE is communicated to block 76, where the error message is displayed to the transcript in the transcript area of Block 80. MESSAGE is communicated to Block 78 where the message is immediately added to the transcript in transcript area 78. . . .

*Id.* at 7:4–24. We agree that the specification describes multiplexing as combining and transporting different types of messages over the same connection and demultiplexing as separating an individual message from the combined signal carried by the communications pathway to deliver it to a recipient based on the type of the message.

From the description in the specification, Petitioner concludes that "'demultiplexing' simply refers to routing a received API message to the correct software functionality based on the type of message." Pet. 14 (citing Ex. 1001, 7:11–12, 7:30–32). As explained above, the specification supports this conclusion, with the understanding that demultiplexing includes separating the received API messages from a combined signal.

As to "multiplexing," however, Petitioner proposes a construction inconsistent with its characterization of the specification, detailed above. Specifically, Petitioner argues that "'multiplexing' simply involves communicating an 'API message' to the appropriate software based on the type of the message." Pet. 13. Despite arguing (correctly) that demultiplexing is essentially the reverse of multiplexing, Petitioner proposes constructions of multiplexing and demultiplexing that are nearly identical in substance, rather than one being the reverse of the other. Although Patent Owner does not propose a construction of this term, Patent Owner does observe that Petitioner uses the term "multiplexing" in a way that is the same as demultiplexing. PO Resp. 31–32. Under its construction of "multiplexing," Petitioner concludes that "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type," should be construed to mean "providing software functionality on the controller computer for sending and receiving messages of different types and communicating each message to software functionality based on the message type." *Id.* at 15. Petitioner's combined construction does not account for two operations, with one being the reverse of the other.

Petitioner finds support for its construction of "multiplexing" in the specification's description of Figure 3 (Ex. 1001, 6:12–15, 25–40). Specifically, Petitioner argues that the specification describes Block 10, labeled "MULTIPLEXING OF MESSAGE TYPE," as evaluating a type of message and routing the message to an appropriate software functionality. Pet. 13. Petitioner mischaracterizes Figure 3. Figure 3 is a dependency diagram showing the relationships among various functions in a system, not a flow chart showing the actual flow of data through the system. Ex. 1001, 6:10–12. Thus, Figure 3 does not show a multiplexing block or module splitting data from a common connection and distributing it to multiple other modules according to data type (which would be demultiplexing). As explained above, Figure 2 shows multiplexing as combining multiple messages of different types for transmission rather than splitting a transmission apart and routing individual messages to appropriate software functionality.

In light of the specification, "multiplexing . . . API messages by type" means "combining and transporting different types of messages over the same connection" and "demultiplexing API messages by type" means "routing received API messages to the correct software functionalities based on the types of messages."

### *B. Asserted Grounds of Unpatentability*

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are "such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains." We resolve the question of obviousness on the basis of underlying factual determinations, including: (1) the scope and content of the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of nonobviousness, i.e., secondary considerations.[5] *See Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

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

[5] The record does not include arguments or evidence regarding objective indicia of nonobviousness.

the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

### *1. Level of Ordinary Skill*

Neither party proposes a level of ordinary skill in the art. Nevertheless, both parties' experts testify to similar levels of skill. Specifically, Dr. Lavian testifies that a skilled artisan "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." Ex. 1002 ¶ 13. For his part, Dr. Carbonell testifies that a skilled artisan "would have had a bachelor's degree in computer science (or a related field) and at least one year of work experience in programming in computer communication methods" and notes that his "opinions herein would not change even if the person having ordinary skill in the art were to be found to have the level of skill proposed by Dr. Lavian." Ex. 2005 ¶ 18. We adopt Dr. Lavian's proposal, as it is consistent with the level of skill reflected in the prior art of record. Nevertheless, we discern no material difference between his proposal and that of Dr. Carbonell. Thus, our findings and conclusions would be the same under either proposal.

### *2. Scope and Content of the Prior Art*

Petitioner contends that the challenged claims would have been obvious over Roseman, alone or in combination with Rissanen, Vetter, Pike, and Gosling. Pet. 16.

#### *a. Overview of Roseman*

Roseman describes a system for multimedia conferencing, in which parties are linked by both video and audio media. Ex. 1003, Abstract. In Roseman, a conference is represented visually as a common virtual conference table, in which each participant can place a document onto the table electronically, manipulate and write on the document, write on a virtual notepad, and move a pointer to draw other users' attention. *Id.* at 2:38–45, 7:55–8:37. Participants can see the events as they occur. *Id.* at 2:46–47. Figure 9, reproduced below, illustrates an example conference room:

FIG. 9

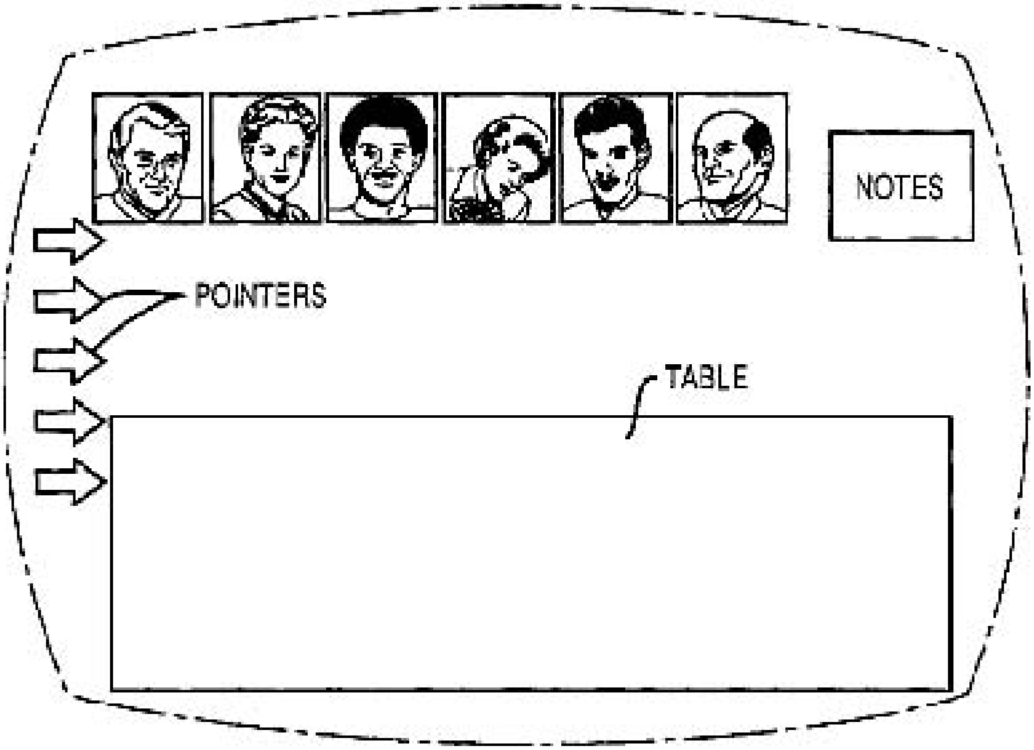


Figure 9 is a picture of a video screen that is generated by a host computer and distributed to all participants in a conference. *Id.* at 2:16–18.

The parties operate their own local computers (which include video cameras and speaker-type telephones) and, when a conference is established, connect to a host computer via commercially available local area networks (“LANs”) and wide area networks (“WANs”). *Id.* at 1:34–41. In the conference, the host computer generates a common video screen (e.g., Figure 9, reproduced above) displayed at each of the local computers, and the parties send information, such as drawings, to be displayed on the common screen. *Id.* at 1:42–46. The telephones and video cameras allow the parties to see and speak with each other. *Id.* at 1:47–49.

Roseman includes a pseudo code appendix that details how its features are implemented. *Id.* at 12:66–13:2. According to the pseudo code, a participant interacts with the conference table, for example, by dragging an icon onto the table, which causes a data file to be transmitted to the host. *Id.* at 14:53–55. The host then transmits the icon to the table of each participant. *Id.* at 14:56–57. If another participant activates the icon, the host sends the open file to the tables of all participants. *Id.* at 14:58–61. If the participant drags the icon from the table to his own screen and activates the icon on his screen, the data file is presented to the participant. *Id.* at 14:62–66.

Roseman describes additional features, such as a party's ability to "whisper" to another party without being heard by others in the conference room, and the ability to "pass notes" by dragging a note to the picture of another party, while the other parties are unaware of the note. *Id.* at 9:16–31. Each room may also have "doors" to committee rooms or child-rooms. A child-room is created in the same way as a parent room and is dependent upon the parent room for access and existence. *Id.* at 10:18–23.

A meeting requester creates a conference by selecting the participants, the attributes of the virtual conference room (e.g., virtual equipment and room décor), and the rules of the conference (e.g., whether the requester has absolute control over voice and message interaction of the parties). *Id.* at 3:22–56. According to Roseman, "[t]he conference room itself is actually a combination of stored data and computer programs," the stored data can include conference proceedings, and "both the conference room and the proceedings of the conference have persistence in time." *Id.* at 12:16–25.

The meeting requester specifies a level for each invitation and compiles an invitation list. *Id.* at 9:34–36. Invitations include "keys" specifying the level, e.g., whether the invitation is for the invitee only or can be passed to a delegate or to anyone. *Id.* at 9:35–48. For example, "Level 1 keys may not be passed to any other person and may not be copied" while "Level 2 keys may be passed to exactly one other person and may not be copied." *Id.* at 9:42–45. According to Roseman, "[t]he meeting room 'knows' about each key and its invitation level. Persons with improper keys are not admitted to the room." *Id.* at 9:49–51. A key is distributed electronically as an object attached to the invitation. *Id.* at 9:54–55. To attend a meeting, a party walks a virtual "hallway" to the meeting room and opens the meeting room door by dropping the key onto a virtual "door lock." *Id.* at 10:30–32, 10:61–65. Moreover, the host "can automatically prevent filibustering" by "monitor[ing] the speech of each person, and plac[ing] a limit on the total time allowed to each person." *Id.* at 12:29–38.

### *b. Overview of Rissanen*

Rissanen describes a system and method for validation of spoken passwords. Ex. 1004, 2:17–21. Rissanen's Background of the Invention discusses systems in which "business computer systems are arranged to initially record and store passwords assigned to users," a user is prompted for entry of a password, 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." *Id.* at 1:21–28. In Rissanen's proposed solution, "[u]sers 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." *Id.* at 2:26–29.

Petitioner makes clear that "[a]lthough Rissanen also describes using spoken voice passwords, this Petition cites it for its more pedestrian teachings relating to database storage of passwords of any form." Pet. 20.

### *c. Overview of Vetter*

Vetter is an IEEE Computer Society Magazine article discussing available tools for conducting teleconferencing over the Internet. According to Vetter, "[v]ideoconferences are becoming increasingly frequent on the Internet and are generating much research interest." Ex. 1005, 77. Vetter states that "the emerging multicast backbone (or MBone) can efficiently send traffic from a single source over the network to multiple recipients," and, "[a]t 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." *Id.* Vetter concludes that "[t]he 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." *Id.*

Vetter also describes challenges that faced implementation of audio, graphic, and video tools on the Internet, including "disturbing feedback when the microphones at multiple sites were left 'open' during a discussion," taking too much time to broadcast a simple graphic image to multiple participants when using "Whiteboard tools" (collaborative software tools that support a shared desktop whiteboard among a group of distributed users on the Internet), and use of video during a classroom presentation that

caused the workstations in the classroom lab to lock up. *Id.* at 78–79. Vetter also notes that the physical distance between two points on the Internet can be different from the electronic distance between those points. *Id.* at 79.

Vetter discusses in particular a CU-SeeMe platform from Cornell University that supported video and audio conferencing over the Internet, and a CU-SeeMe Reflector that allowed multiparty conferencing with CU-SeeMe. *Id.* at 78.

### *d. Overview of Pike*

Pike is a reference and guide book for using the Web browser Mosaic. Ex. 1006, 2. Petitioner cites to Pike's discussion of URLs and hyperlinks. According to Pike, URLs were developed as a standard way of referencing items on the World Wide Web. *Id.* at 38. "A *URL* is a complete description of an item, containing the location of the item that you want to retrieve. 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.*

### *e. Overview of Gosling*

Gosling is a paper describing various aspects of the Java programming language. Ex. 1007, 111. According to Gosling, programming in Java has the benefit of portability such that Java programs "can execute on any kind of CPU." *Id.* at 115.

### 3. *Claim 1, Differences Between the Claimed Subject Matter and the Prior Art, and Reasons to Modify or Combine*

Petitioner contends that Roseman teaches each limitation of claim 1, but cites the remaining references for the following, should we determine that Roseman lacks such a teaching:

> Rissanen for a teaching that tokens could have been stored in a database;
>
> Vetter for a teaching that Roseman's communications could have been over the Internet;
>
> Pike for a teaching of URLs; and
>
> Gosling for a teaching of a JAVA application.

Pet. 19–23.

#### a. *"A method of communicating content among users using of [sic] 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"*

Petitioner contends that Roseman's host computer is a controller computer. Pet. 24–25. Petitioner identifies Roseman's local computers as independent participator computers and argues that Roseman's various ways of communicating information (placing documents on a virtual table, shared notes, whisper conversations) are examples of affording information to those participator computers. Pet. 31–33. As detailed above, Roseman describes a system in which individual computers are connected to a central host computer via a combination of LANs and WANs. Ex. 1003, 3:14–19.

According to Roseman, "[t]he 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." *Id.* at 1:50–52. We find that Roseman's host computer is a "controller computer," that Roseman's local computers are "participator computers," and that Roseman's various ways of communicating information from the host to the local computers are examples of "affording information to each of a plurality of participator computers which are otherwise independent of each other," as recited in claim 1.[6]

The parties dispute whether Roseman describes "a database which serves as a repository of tokens for other programs to access." First, Petitioner contends that Roseman's "keys" are tokens. Pet. 25–26. As explained above, the parties agree that a "token" is "a piece of information associated with user identity." As also explained above, Roseman describes that an invitor, in setting up a meeting, creates an invitation that includes a key that conforms to an invitation level. Ex. 1003, 9:34–48. A key "is an electronic object attached to the invitation." *Id.* at 9:54–55. The "level" of a key determines who can use it. *Id.* at 9:34–41. For example, "Level 1 keys may not be passed to any other person and may not be copied." *Id.* at 9:42–44. According to Roseman, "[t]o 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." *Id.* at

[6] Patent Owner argues that "Petitioner does not address the issue that the **database** affords information to each of a plurality of computers." PO Resp. 21. Claim 1, however, does not recite that the database affords information to the plurality of computers.

10:61–64. Petitioner argues that this evidence shows that Roseman's keys are "pieces of information associated with a user identity," and thus, are "tokens." Pet. 26.

Patent Owner argues that Roseman's keys are not tokens because they are associated only with conference rooms, rather than user identities. PO Resp. 17. Patent Owner points to Roseman's Figure 8, which shows a key associated with "CONFERENCE ROOM 17L (DATE, TIME)." *Id.* In describing Figure 8, however, Roseman explains "the key is, essentially, a block of data, or a code," that can be used if the Invitee may send a delegate to give the Absentee-Invitee a "key," which enables access to the meeting. Ex. 1003, 6:54–61. "The Requester can leave the key in his local computer, in the form of an icon residing on the display, as shown in FIG. 8. Anyone entering the office can use the key." Ex. 1003, 6:60–63. In this example, the key can be used only with a particular user's computer. Figure 8 also shows the "key" icon contained within a "vault" icon. *Id.* at 6:64–65. In this example,

> a user must use a "combination" to the "vault" to obtain the "key." In this latter example, the [] "combination" (ie, a pass-code) is obtained from the Absentee-Invitee in some appropriate way. At conference time, the Delegate opens the "vault," obtains the "key," and enters the conference room, by using the key.

*Id.* at 6:65–7:3. Patent Owner argues that Roseman's keys are "transferable to anyone—like a key to a door lock." PO Resp. 17. Patent Owner contends that Roseman teaches away from keys being associated with a specific user through its description that "***[k]eys may be copied and redistributed, if permitted***, or sent to another individual, if permitted." *Id.* at 17–18 (quoting Ex. 1003, 9:55–57) (emphasis by Patent Owner).

Patent Owner's arguments are not persuasive. Roseman describes keys that are transferable (Level 2 and 3 keys) and keys that are not transferable (Level 1 keys). Ex. 1003, 9:42–48. Petitioner's contentions (Pet. 26) are directed to Level 1 keys, which "may not be passed to any other person and may not be copied." *Id.* at 9:43–44. We find that keys that may not be passed to any other person are keys associated with that person. Figure 8 of Roseman is consistent with this because it describes passing a key to an "Absentee-Invitee" when the Invitee sends a delegate, i.e., a Level 2 key.

As to Level 1 keys, Patent Owner argues that a key is merely an attachment to an invitation, which "offers the only suggestion of an association with specific invitee." PO Resp. 18. Dr. Carbonell testifies (without identifying a basis) that Roseman's system could prevent the transfer of a key using a "no-transfer or no-duplication policy of such a key to insure that [it] always stays in the possession of the first user," by making transferability an attribute of the key and having the system simply assume, without recording transfers, that a user in possession of a key is authorized to use it. Ex. 2005 ¶ 31. As Petitioner argues, however, the claim construction to which Patent Owner agreed does not require an association between a key and a user to be implemented in a certain way. Reply 15–16. Even if Dr. Carbonell is correct as to how Roseman's keys would be implemented, such a non-transferable key would still be associated with the person who is prevented from transferring it.

Petitioner further argues that Roseman discloses storing keys in "a database which serves as a repository of tokens," as recited in claim 1, because a meeting room that is accessed by a key "'knows' about each key and its invitation level." Pet. 27 (quoting Ex. 1003, 9:49–51). According to Petitioner, a copy of each key must be stored on the host computer for the meeting room to "know" about each key. *Id.* at 27. Petitioner argues that a skilled artisan would have understood the claimed database to be a stored collection of tokens. *Id.* at 27–28. Roseman does not expressly describe storing tokens in a database. Thus, we understand Petitioner to argue that tokens necessarily are stored in a database in light of Petitioner's cited disclosure—in other words, that a database is inherent in Roseman.

Patent Owner, relying on Dr. Carbonell's testimony, argues that a meeting room's knowledge of a key could be implemented using a hash function, which would not have required storage of the key in a database. PO Resp. 20–21 (citing Ex. 2005 ¶ 40). Petitioner characterizes Patent Owner's argument as "based on pure speculation and conjecture" and inconsistent with Roseman's disclosure. Reply 11–12. Nevertheless, we view both parties' respective theories of Roseman's implementation as speculation. Because Petitioner's position is speculative, it is insufficient to show that a database is inherent in Roseman.[7]

In the alternative, Petitioner argues that Rissanen teaches storing user authentication information, such as user identity information and passwords,

[7] Patent Owner also argues that Roseman does not suggest storing keys in a manner that is persistent and does not disclose tools such as a DBMS. PO Resp. 21–22. Roseman does teach that the data associated with its conference rooms are stored in a manner that is persistent, Ex. 1003, 12:16–28, and this at least suggests that keys also would be stored in such a manner. As to a DBMS, we explain above that the construction of "database" does not require this feature. Nevertheless, as explained below, Rissanen teaches a database even under Patent Owner's proposed construction.

in a database, and that such teaching would have been applicable to the keys of Roseman. Pet. 28–29. Petitioner argues that Roseman's keys are analogous to user identity and passwords. *Id.* According to Petitioner and its expert, Roseman's key verification step might not function properly if the keys are not stored in a database. *Id.* at 29 (citing Ex. 1002 ¶ 67). Petitioner further argues that storing keys in a database is one of a finite number of known solutions for verifying whether a previously issued key matches to a key later presented by a user to access a conference room. *Id.* at 29–30 (citing Ex. 1002 ¶¶ 67–68).

Patent Owner admits that "[Rissanen] does disclose a database," but argues that its database is used in a different type of system. PO Resp. 22. Thus, Patent Owner does not contest that Rissanen's database stores user identities and passwords in a persistent manner and is used in conjunction with tools such as a DBMS. For Petitioner, Dr. Lavian testifies that "Rissanen clearly discloses a relational database whose data is stored persistently and includes tools for interacting with the data such as a DBMS." Ex. 1021 ¶ 37. We find that Rissanen teaches a database that stores data with persistence and tools for interacting with the database.

Nevertheless, Patent Owner argues "[i]f one were going to combine Roseman and Rissenan in order to authenticate an individual (and not merely authenticate a key for a room) the necessary logic would be significantly more complicated." PO Resp. 23. Petitioner does not argue, however, that Rissanen's database would be bodily incorporated into Roseman's system. Rather, Petitioner argues that Rissanen teaches storing data "analogous to and serv[ing] the same purpose as" the keys in Roseman in a database. Pet. 28. *See In re Mouttet,* 686 F.3d 1322, 1332–32 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements. . . . Rather, the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art.”). Given that Roseman describes using keys to access conference rooms that have persistence, we agree with Petitioner that a database, described in Rissanen as storing similar information for a similar purpose, would be a straightforward and predictable choice for storing Roseman’s keys.

The parties also dispute whether Roseman and Rissanen teach that the database “serves as a repository of tokens *for other programs to access*, thereby affording information to each of a plurality of participator computers,” as recited in claim 1. Petitioner argues that other programs access the stored collection of tokens, including the various meeting or conference rooms maintained on the host computer. Pet. 30. Petitioner relies on disclosure in Roseman that a meeting room is accessible from a virtual hallway with doors to other meeting rooms. *Id.* (citing Ex. 1003, 9:63–65). According to Petitioner, “[e]ach meeting room . . . 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.” *Id.*

Patent Owner argues that “Petitioner does not identify any programs that could access a database of tokens and receive information, other than the singular conference calling software running on the host computer of Roseman.” PO Resp. 24–25. According to Patent Owner, “to the extent that there are multiple conference rooms in existence, that is because the

Roseman system has instantiated the same conference room program with different parameters as there is no suggestion that there is different software associated with each conference room." *Id.* Patent Owner does not explain why "other programs" require different software rather than different instantiations of the same software, or point to evidence supporting this view. We are not persuaded that the claims should be limited in this way. Nevertheless, as Petitioner points out (Reply 17–18), Roseman characterizes its conference rooms as collections of different programs (Ex. 1003, 12:16–18) and makes clear that different conference rooms will have different attributes (different virtual equipment, different tools, different appearances, etc.) (*id.* at 3:42–50, 10:9–12). We find that Roseman at least suggests different conference rooms with different programs, even under Patent Owner's view. These programs determine whether a participant can join a meeting room based on evaluations of keys that, in light of Rissanen, would have been stored in a database. Thus, we find that Roseman and Rissanen teach "a database which serves as a repository of tokens for other programs to access," as recited in claim 1.

#### *b. "authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database"*

As explained above, Roseman discusses a user validation system based on "keys" provided to invitees to a virtual conference—for example, a "Level 1 key" that is restricted to a specific user only—which are used by the invitees to access the conference and enable communications between and among the users and the host computer. *Id.* at 9:34–55, 10:61–65, 11:10–17. We find that this teaches authenticating users according to permissions retrieved from the repository of tokens.

### c. *"affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity"*

### *"affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity"*

As explained above, Roseman describes admitting participants into a conference room when the participants present keys. Ex. 1003, 10:61–65. We find that this teaches "an authenticated first user identity" and "an authenticated second user identity." Additionally, Roseman describes various ways of affording information to local computers of users admitted to the conference room, including as follows:

> 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.

*Id.* at 11:18–26. *See also* Pet. 36–37. We find that these examples in Roseman teach "affording some of the information to a [first/second] of the participator computers . . ., responsive to an authenticated [first/second] user identity," as recited in claim 1.

The parties dispute whether the prior art teaches affording information "via the Internet Network," as recited in claim 1. As explained above, Roseman describes communicating between a host and local computers via commercially available LANs and WANs. Ex. 1003, 1:37–41, 3:14–19. Petitioner contends that a skilled artisan would have understood the Internet to be an example of the commercially available WAN described in Roseman. Pet. 37; Ex. 1002 ¶ 83. According to Dr. Lavian, "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." Ex. 1002 ¶ 86; *see also* Ex. 2006 (Lavian Dep.), 104:12–105:23 ("Q So Roseman could have been implemented in that 1994 to '96 time frame with ATM technology? A If I'm looking at the specification of Roseman and what specifically Roseman disclose, it disclose as using a -- local computers become connected to host computer via commercially available Local Area Networks and Wide Area Networks. When you're talking about Local Area Networks and Wide Area Networks, this is the Internet. That's different name to Internet. Q So you're saying that Roseman by itself teaches the Internet? A Roseman by itself reference to remote computers commercially available, commercially available that said Internet. Local Area Networks, definitely part of the Internet. Wide Area Networks, different name to the Internet. It's actually the Internet itself. . . .").

Petitioner further argues that Vetter teaches using the Internet to facilitate the same types of computer-based conferencing functions as described in Roseman. Pet. 37–38. Petitioner contends that Vetter itself identifies a reason to combine the teachings of Roseman and Vetter, namely "[v]ideoconferences are becoming <u>increasingly frequent</u> on the Internet" and the CU-SeeMe videoconferencing tool described in Vetter "is also becoming very popular." *Id.* at 39 (quoting Ex. 1005, 77 (emphases by Petitioner)).

Patent Owner argues that Vetter does not state that Internet videoconferencing would have been ubiquitous at the time of the invention; rather, Patent Owner argues, the Internet was beginning to support video conferencing. PO Resp. 26. According to Patent Owner, "while communication over the Internet maybe obvious today, the mid-1990's were still the early formative years of the Internet, and one of ordinary skill in the art would not necessarily have looked to the Internet to improve systems such as Roseman." *Id.* at 27. Patent Owner further argues that Vetter describes a system for point-to-point and point-to-mulitpoint communications without the use of a centralized server structure, database, or tokens. *Id.*

We are persuaded by Petitioner. Roseman expressly states that its local computers and host communicate via a commercially available WAN. We credit Dr. Lavian's testimony that, to the extent that this is not an express reference to the Internet, the most suitable and obvious commercially available WAN would have been the Internet. We also find that Vetter suggests using the Internet for purposes similar to those of Roseman. Vetter describes an example in which features such as audio, video, and virtual whiteboard tools are used to conference over the Internet. Ex. 1005, 77–78. Thus, to the extent Roseman does not expressly suggest using the Internet, Vetter includes an express suggestion to update a system such as Roseman using modern electronic components, such as the Internet, to gain the commonly understood benefits of such adaptation. *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.,* 485 F.3d 1157, 1162 (Fed. Cir. 2007);

*cf.*, *Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1326–27 (Fed. Cir. 2008) ("The record in this case demonstrates that adapting existing electronic processes to incorporate modern internet and web browser technology was similarly commonplace at the time the '099 patent application was filed."). Vetter reinforces our finding that the Internet would have been the most suitable commercially available WAN for use in Roseman's system. Patent Owner's argument that Vetter does not describe a system with a controller computer, database, or tokens is unpersuasive as it merely attacks Vetter individually without considering the combination proposed by Petitioner. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.").

In sum, we find that Roseman and Vetter teach affording information to first and second participator computers "via the Internet network," as recited in claim 1.

### *d. "running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers"*

With regard to the limitation, "controller software . . . to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers," the Petition relies on teachings in Roseman about the functions of the host software on the host computer. Pet. 40–44. For example, Roseman describes applying rules to govern which conference participants can communicate interactively, and how the participants may communicate, such as a "talking queue" permitting only one participant to speak at a time, permitting only one participant at a time to utilize the pencil tool, and private communication features where only select participants may exchange private communications. Ex. 1003, 3:52–56, 9:16–31, 11:38–46, Fig. 19.

As to "in accordance with predefined rules," Petitioner (Pet. 41) argues that Roseman discloses that a person setting up a conference can determine aspects of the meeting, such as: "What rules govern the conduct of the meeting? Does the Requester have absolute control of the voice and message interaction among the participants? Or Is the meeting a brainstorming free-for-all, where numerous people can speak at once?" Ex. 1003, 3:52–54. As to a specific example, Petitioner points to Roseman's "pencil" tool, through which a participant can write a message in a conference room using the pencil tool, and other participants are disabled from doing so while the first participant has the pencil. Pet. 42 (citing Ex. 1003, Fig. 19). Petitioner also cites to Roseman's "Whisper Mode" for private voice conversations and "note-passing" for private textual conversations as examples of predefined rules that govern how users conduct real-time communications. *Id.* at 42–43 (citing Ex. 1003, 9:16–31, 15:12–15, Fig. 17C). We agree with Petitioner that these are examples of "predefined rules" that "direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers." Thus, we find that Roseman teaches this limitation. We note that Patent Owner does not contest that Roseman teaches this limitation.

### *e. "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers"*

Claim 1 recites "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type." For the recited "API," Petitioner identifies a series of software functions for which Roseman provides pseudo-code, including transmitting data files to conference participants, transmitting private notes between participants, and enabling (and disabling) the pencil tool. Pet. 44–47 (citing Ex. 1003, 12:66–13:2, Figs. 16A, 17C, 19). According to Petitioner, this API multiplexes and demultiplexes API messages by type, as recited in claim 1, because "the host computer receives a type of message and routes the message to the appropriate software functionality to handle that message type." *Id.* at 45–47. According to Petitioner,

> Roseman discloses software functionality that transmits and processes particular types of messages, such as placing a document on the table (*causing the document to be sent to each participant*), using the pencil (*causing the participant's actions to be sent to each participant*), sending a private message (*causing the message to be sent only to the intended recipient*), and other messaging functions. Messages corresponding to these commands are multiplexed because the host computer processes each message using the software functionality described above – using the message type to determine the appropriate software.

*Id.* at 46–47 (emphasis added). Petitioner argues that '356 patent's "description mirrors what the 'host computer' in Roseman does." *Id.* at 47.

In response, Patent Owner argues that "none of Petitioner's evidence indicates the presence of both multiplexing and demultiplexing *on the* *controller computer*." PO Resp. 31. According to Patent Owner, any multiplexing identified by Petitioner would occur only in the context of the participator software. *Id.* As to Petitioner's contention that messages corresponding to Roseman's, icon, note, and pencil features "are multiplexed because the host computer processes each message using the software functionality described above – using the message type to determine the appropriate software," Pet. 45–47, Patent Owner argues that "using the message type to determine the appropriate software is actually demultiplexing," PO Resp. 31–32.

In reply, Petitioner notes that Patent Owner, in a related proceeding (IPR2016-01067), proposed construing "multiplexing" to mean "collecting messages from different objects/code and sending the messages over a common channel to the participators," a construction similar to our construction in Section II.A.4 above ("combining and transporting different types of messages over the same connection"). Pet. 22–23 (citing IPR2016-02067, Paper 26, 31). Petitioner contends that it showed, in the Petition, multiplexing in Roseman under Patent Owner's construction. *Id.* at 23. We agree with Petitioner. As explained above, Roseman describes a host receiving icon, note, and pencil messages from the local computers over the Internet (a common communication channel), routing those messages to the appropriate software to handle the messages (demultiplexing), and further sending those messages to each of the participants (in the case of icons and pencil messages) or to only an identified participant (in the case of notes) over the Internet. Ex. 1003, 8:1–5, 9:26–31, 14:53–67, 15:10–13, 15:20–27. We find that, to send these messages of different types to the participants over the same Internet connection (in the combination that includes Vetter's teachings), the messages would be combined. Therefore, we find Roseman teaches multiplexing as construed ("combining and transporting different types of messages over the same connection").

Patent Owner further argues that Roseman's description of a "whisper mode" teaches away from multiplexing because a whisper mode audio communication is invoked in a separate voice connection that is not shared with the data connection. PO Resp. 32. Even if this is the case, Patent Owner does not explain how it undermines the other examples cited by Petitioner, including icons, notes, and pencil messages, which we find are multiplexed and carried over the same connection.

Claim 1 also recites "creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers." Petitioner asserts that Roseman's description of the virtual conference room provided by the host computer, within which the various software functions are made available, teaches the recited "virtual connection." Pet. 47. Petitioner contends that the host software providing a virtual conference room that connects a group of participants is an example of creating a virtual connection between channels in the controller computer and the participator computers. *Id.* at 48. As explained in Section II.A.1 above, "channel" means "a group of participator computers in active communication." Petitioner further argues that Roseman's child rooms are additional examples of channels. Pet. 48 (citing Ex. 1003, 10:18–25).

As discussed above, Roseman also describes private communications features within the virtual conference rooms, including note-passing, which Petitioner maps to the recited "private messages." *Id.* at 48 (citing Ex. 1003, 2:49–50). Petitioner contends that this teaches providing a virtual connection between private messages in the controller computer and the participator computers. *Id.* Finally, Roseman describes "multi-media conferencing" where audio and video are exchanged between participants in a virtual conference room, as well as the sharing of documents and files (including text and graphics). *Id.* at 48–49 (citing Ex. 1003, Abstract, 2:38–45, 7:65–67, 8:1–4, 11:11–13). Petitioner argues that this teaches providing a virtual connection between multimedia objects in the controller computer and the participator computers. *Id.* at 49.

Patent Owner argues that claim 1 "explicitly requires a connection to be established between corresponding objects in the controller and participator computers, necessitating the existence of the claimed objects within the participator computers," and that "Roseman does not disclose any software on the users' computers that could qualify as corresponding participator software that includes the claimed channel objects, private messaging objects, or multimedia objects." PO Resp. 29. Patent Owner argues that Roseman describes generating images on the host computer and sending that same display to each of the local computers, rather than opening files on the local computers. *Id.* at 29–30 (citing Ex. 1003, 8:1–4, 8:11–13).

Petitioner argues that "[t]he claims do not under their broadest reasonable construction exclude a communications system in which the controller computer provides information to participator computers in the form of graphical representations." Reply 21. According to Petitioner, Patent Owner's expert admitted that an "object" in the context of the challenged claims is simply an item of information. *Id.* (citing Ex. 1016, 111:20–112:14).[8] Consistent with Petitioner's argument, Dr. Carbonell testified that "objects" means "items of information," for example, "[i]t can be a figure, it can be a video clip, it can be audio." Ex. 1016, 111:20–112:3. Petitioner argues that Roseman's rendering of a conference room constitutes an "object." Reply 21.

We agree with Petitioner that the claims do not require corresponding software at a participator computer for demultiplexing messages such that an object (item of information) multiplexed at the host and sent to the participator computer is demultiplexed to separate out that object, which is how Patent Owner construes this claim limitation. On one hand, the '356 patent Specification describes demultiplexing and multiplexing on both participator and controller computers to create the disclosed virtual connection between channel, message, and multimedia objects: "De/multiplexing via API provides a 'virtual connection' between Channel, Private Message, and Multimedia objects in the controller computer 3 and each participator computer 5." Ex. 1001, 6:3–5. On the other hand, the caption at the bottom of Figure 2 implies that merely multiplexing API messages creates a "virtual" connection. *See id.* at Fig. 2 ("MULTIPLEXING VIA API PROVIDES A 'VIRTUAL CONNECTION BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR.").

The claims, however, in essence define a "virtual" connection as one created by multiplexing and demultiplexing messages by type on the

[8] Petitioner cites to Exhibit 1014, which we assume is a typographical error. Dr. Carbonell's deposition is Exhibit 1016.

controller computer. For example, claim 1 recites "providing an API *on the controller computer*, the API multiplexing and demultiplexing API messages by type, *creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers*."

Although the '356 patent presents different generic or functional descriptions about what it means by a "virtual" connection, the disclosure reveals that a virtual connection is not "a separate connection between each object," which is "[a]n alternate connection" to a "virtual connection." Ex. 1001, 6:3–9. In view of the '356 patent specification, a "virtual" connection "between channels" means that the controller computer connects participators to the same "channel" via the controller computer—meaning that users in a group on that "channel" can chat or teleconference. Roseman's description of placing documents on a virtual conference table, causing the document to be sent to each participant as part of a common rendering, teaches a virtual connection between channels. Pet. 48.

In similar fashion, a "virtual" connection for the claimed "private message" and "multimedia object" simply means a connection through the controller computer and between different users exists so that participators on a "channel" each may see a "private message" and a "multimedia object" (e.g., via a download or URL connection) sent by another participator user. *See* Ex. 1001, Fig. 2, 5:38–43 (describing multimedia as sent by URL links), 5:44–6:9 (discussing private messages, channels, multimedia objects, and virtual connections).

By way of example, the specification describes in general terms how participator computer Block 20, which "is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types," "links to Block 24, which illustrates handling private message A," and "also links to Block 26, illustrative of handling out-of-band media." Ex. 1001, 5:58–68 (emphases added). These illustrations using different "Blocks" simply describe in functional software terms connecting users on "channels" (so that users can chat and/or send messages) and transferring private messages and multimedia objects between users via the controller computer. *Id.* at 5:43–67. Another feature of a "virtual" connection implied by Figures 1 and 2 is that no direct connection between users exists, rather, an indirect connection routed through the controller computer exists. Ex. 1001, Figs. 1, 2.

We find that Roseman's description of sending notes to an identified participant, and no one else, is a teaching of a connection through the host (controller computer) and between different local computers (participator computers) that allows participators on a "channel" to see a "private message."

Patent Owner also argues that Roseman describes initiating separate data and voice connections when the "whisper mode" is used, rather than a shared connection. PO Resp. 30. This is similar to Patent Owner's argument, discussed above, that Roseman's whisper mode teaches away from claim 1. Once again, Patent Owner does not explain why Roseman's description of one particular type of communication (whisper mode) undermines Petitioner's evidence as to Roseman's other examples of communications, such as note passing and multi-media conferencing.

In sum, we find that Roseman and Vetter teach "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers," as recited in claim 1.

### *f. "communicating real-time messages within the group of the interactively connected said participator computers"*

Petitioner identifies Roseman's teachings of real-time communications in the form of sharing documents, writing/drawing on shared documents, and using a virtual pointer to indicate parts of shared documents. Pet. 50–51 (citing Ex. 1003, 2:38–47, 7:54–8:5, 8:41–46, 12:26–28). Petitioner contends that communications in one of Roseman's conference rooms, such as placing documents on a table, drawing on a document, and moving a pointer, take place in real time because they are communicated to participants as the underlying events occur. *Id.* For example, Roseman explains:

> 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 [] preceding three events as they occur.

Ex. 1003, 2:38–47. We find that these are specific examples in Roseman of real-time communications sent and received by the participator computers in a group.

Thus, we find that Roseman teaches this limitation of claim 1. We note that Patent Owner does not contest that Roseman teaches this limitation.

In sum, we find that Roseman, Rissanen, and Vetter teach each limitation of claim 1.

### *4. Remaining Challenged Independent Claims*

Claim 19 recites an apparatus configured to perform functions that track the steps of claim 1, except that claim 19 does not recite functions corresponding to "affording some of the information to a [first/second] of the participator computers via the Internet network, responsive to an authenticated [first/second] user identity." Claim 37 is substantively the same as claim 19, except that, where claim 19 recites "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," claim 37 recites "affording information to each of a plurality of independent participator computers which are otherwise independent of each other, *via the Internet network* communicating with the participator computers." Petitioner compares the limitations of claims 1 and 19 side-by-side and argues that claim 19 is taught by Roseman, Rissanen, and Vetter for the same reasons as given for claim 1. Pet. 55–57. Petitioner further compares the limitations of claims 19 and 37 side-by-side and argues that claim 37 is unpatentable for the same reasons as given for claims 1 and 19.

Patent Owner argues claims 19 and 37 along with claim 1. For the reasons given for claim 1, Roseman, Rissanen, and Vetter teach each limitation of claims 19 and 37.

### 1. *Claims 2–5, 8, 9, 12, 16, 20–24, 27, 28, 31, 35*

Claims 2–5 depend, directly or indirectly, from claim 1, and recite that the communication content includes communicating at least one, two, three, or four of "sound, video, graphic, pointer, and multimedia content." Claims 20–24 depend, directly or indirectly, from claim 19 and include similar limitations. Petitioner points to examples in Roseman of communicating sound and video (Ex. 1003, 11:11–16 ("Audio and video connections")), graphic content (*id.* at 8:1–4 ("[e]ach Invitee can transmit a file (of any suitable kind: data, text or graphic) to the host")), and multi-media (*id.* at Abstract ("'multi-media' conferencing")). Pet. 51–52, 57. Patent Owner does not present separate arguments for these claims. Based on Petitioner's evidence, we find that Roseman teaches the additional limitations of claims 2–5 and 20–24.

Claims 8, 9, and 12 depend from claim 1. Claim 8 recites "wherein the API includes API messages"; claim 9 recites "wherein communications among the controller computer and the participator computers are mediated via API messages"; and claim 12 recites "wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages." Claims 27, 28, and 31 depend from claim 19 and recite similar limitations. Petitioner contends that these claims do not add materially to claim 1 and are unpatentable for the same reasons as given for the limitation of claim 1, "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers." Pet. 53, 57–58. Patent Owner does not present separate argument for these claims. We agree with Petitioner that Roseman and Vetter teach the additional limitations for the same reasons as given for claim 1, "providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers."

Claim 16 depends from claim 1 and adds "wherein the communicating is conducted over the network, including the Internet." Claim 35 depends from claim 19 and recites a similar limitation. We find that this limitation is taught by Roseman and Vetter for the same reasons given above for claim 1, the limitation "affording some of the information to a first of the participator computers *via the Internet network*."

### *2. Claims 14, 15, 33, 34 ("censorship" claims)*

Claims 15 and 34 depend from claims 1 and 19, respectively, and add "the controller computer determines censorship." Claims 14 and 33 also depend from claims 1 and 19, respectively, and add a more narrow "determining censorship of the content" and "the computer system determines censorship of the content," respectively. Petitioner presents the same arguments and evidence for both of these sets of claims, without distinguishing between them. Pet. 54, 58.

Petitioner points to Roseman's description of measures that can be taken to prevent participants from speaking. *Id.* at 54 (citing Ex. 1003, 11:40–46, 12:29–45). For example, Roseman's host can act as a moderator, such that

> While one participant is speaking, the host can monitor the audio input of the other participants. The host looks for instances when the speaker refuses to stop talking when the other participants speak. When the host finds such instances, the host issues a message to all participants stating that a filibuster appears to be occurring, and requests a vote as to whether to allow the filibuster to continue.

Ex. 1003, 12:39–45. Petitioner argues that this "mirror[s] the examples of 'censorship' in the written description of the '356 patent." Pet. 54 (citing Ex. 1001, 8:41–46)

As to claims 15 and 34, we agree with Petitioner. These claims simply recite that the controller computer "determines censorship." As explained in Section II.A.2 above, censorship is "control of what is said in a group." Roseman's host preventing participants from speaking is a form of control over what is said in a group. This is similar to the '356 patent's example in which "[c]ensorship can control . . . access to system 1 by identity of the user." Ex. 1001, 8:41–42. Thus, we find that Roseman teaches the additional limitations of claims 15 and 34.

As to claims 14 and 33, however, Petitioner has not explained persuasively why preventing a user from speaking constitutes "censorship of the *content*." As explained in Section II.A.2 above, censorship of the content means "determining whether to communicate content based on characteristics of the content." This aligns with the '356 patent's example in which "[c]ensorship also can use the tokens for real time control of data (asci, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject." Ex. 1001, 8:45–47. When Roseman's host acts as a moderator, it prevents a user from speaking without regard to characteristics of the content. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claims 14 and 33 would have been obvious over Roseman, Rissanen, and Vetter.

### *3. Claims 6, 7, 17, 26, 36 ("pointer" claims)*

As noted above, claim 2 recites "wherein the communicating content includes communicating at least one of sound, video, graphic, pointer, and multimedia content." Claim 6 depends from claim 2 and recites "wherein said at least one comprises at least five." In our analysis of claim 5, above, we find that Roseman teaches examples of four of these, sound video, graphic, and multimedia, leaving "pointer" unaccounted for. Claim 7 depends from claim 1 and recites "wherein the communicating content includes communicating a pointer that allows the content to be produced on demand." Claim 26 depends from claim 19 and adds a similar limitation. Petitioner cites Roseman and Pike for examples of pointers. Pet. 60–64.

For example, as noted above, Roseman describes a user placing an icon onto the table of a virtual conference room and the host sending the icon to the table of each conference participant. If the icon is clicked by a participant, the host presents the file to all of the participants. Ex. 1003, 14:53–62. Petitioner contends that the icon is a pointer because it points to, or references, an underlying document. Pet. 60–61. We agree, and find that Roseman teaches communicating content by communicating a pointer that allows content to be produced on demand.

Petitioner further cites to Pike "in the event it is later argued or determined that 'pointer' requires an Internet URL or something functionally similar." *Id.* at 61. Although we do not determine that claims 6, 7, and 26 require a URL, claim 17 depends from claim 1 and recites "wherein the communicating content includes communicating content invoked with a URL." Claim 36 depends from claim 19 and includes a similar recitation. Thus, we evaluate whether Roseman, Vetter, and Pike teach communicating content invoked with a URL.

As Petitioner argues (Pet. 61–62), Pike explains that a URL "is a complete description of an item, including the location of the item that you want to retrieve," and can be used to locate and retrieve documents from another computer. Ex. 1006, 36–39. Dr. Lavian testifies that incorporating Pike's URLs into Roseman's system (communicating via the Internet, per Vetter's teaching) "would have predictably resulted in the virtual conferencing system of Roseman in which the clickable icons used to access content (such as documents and notes) included a URL that identified the location of content on the host computer." Ex. 1002 ¶ 121. On this evidence, we find that Roseman, Vetter, and Pike teach communicating content invoked with a URL.

We note that Patent Owner does not present separate arguments for these claims. On the complete record, we find that Roseman, Vetter, and Pike teach the additional limitations of claims 6, 7, 17, 26, and 36.

### *4. Claims 18, 25 ("JAVA" claims)*

Claim 18 depends from claim 1 and recites "wherein the controller software comprises a JAVA$^{TM}$ application." Claim 25 depends from claim

19 and adds a similar limitation. Petitioner cites to Gosling as providing evidence that Java was a known programming language that could be used to build application software. Pet. 64 (citing Lavian Decl. ¶ 131). Petitioner argues that Gosling provides a reason to use Java in Roseman's application, namely, "[o]ne of the obvious benefits of using a bytecode like Java's is that compiled programs are portable: so long as the interpreter is present, programs can execute on any kind of CPU." *Id.* (citing Ex. 1007, 115). Dr. Lavian testifies that "[b]y using Java for the host computer software in Roseman, the developer would be freed from the burden of having to rewrite or change the application in the event of a change in the type of CPU or computer architecture for the server computer." Lavian Decl. ¶ 132. On the complete record, we find that a skilled artisan would have had reason to implement Roseman's system using Java, namely, to create programs that are portable and that can be executed on many kinds of computers without having to be rewritten. Thus, Roseman and Gosling teach the additional limitations of claims 18 and 25.

### 5. *Conclusion of Obviousness*

As explained above, Roseman, Rissanen, and Vetter teach each limitation of claims 1–5, 8, 9, 12, 15, 16, 19–24, 27, 28, 31, 34, 35, and 37; Roseman, Rissanen, Vetter, and Pike teach each limitation of claims 6, 7, 17, 26, and 36; and Roseman, Rissanen, Vetter, and Gosling teach each limitation of claims 18 and 25. Petitioner has introduced persuasive evidence that a skilled artisan would have had reasons to combine the teachings of Roseman, Rissanen, Vetter, Pike, and Gosling. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness.

In sum, upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence, that claims 1–5, 8, 9, 12, 15, 16, 19–24, 27, 28, 31, 34, 35, and 37 would have been obvious over Roseman, Rissanen, and Vetter; that claims 6, 7, 17, 26, and 36 would have been obvious over Roseman, Rissanen, Vetter, and Pike; and that claims 18 and 25 would have been obvious over Roseman, Rissanen, Vetter, and Gosling.

As explained above, Petitioner has not proved by a preponderance of the evidence that claims 14 and 33 would have been obvious over Roseman, Rissanen, and Vetter.

## III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner filed a paper styled a "Motion to Exclude Evidence," seeking to exclude certain portions of the 2nd Lavian Declaration that it argues exceeds the proper scope of a reply. Paper 37, 1. Specifically, Patent Owner moves to exclude portions of paragraphs 54, 74, and 75 of the 2nd Lavian Declaration. *Id.* at 2–4.

Petitioner opposes this motion on the ground that it is not directed to the admissibility of evidence and, therefore, is procedurally improper. Paper 39, 2. Patent Owner contends that arguments that exceed the scope of a reply are irrelevant, prejudicial, confusing, or misleading under Federal Rules of Evidence 401, 402, and 403. Paper 41, 1–2. As Petitioner points out, however, the Board repeatedly has denied, as improper, motions to exclude that merely argue that evidence is outside the proper scope of a reply. Paper 39, 2–3. Despite its invocation of Rules 401, 402, and 403, we agree that Patent Owner's Motion to Exclude is nothing more than an argument that Petitioner's Reply exceeds its proper scope. Accordingly, we deny Patent Owner's Motion.

Nevertheless, we have considered Patent Owner's argument with respect to those portions of Petitioner's Reply that are relied upon, and determine they do not belatedly raise new issues or present evidence that should have been presented in the Petition. In any case, we do not rely on paragraphs 54, 74, and 75 of the 2nd Lavian Declaration.

## III. CONCLUSION

Petitioner has established by a preponderance of the evidence that claims 1–9, 12, 15–28, 31, and 34–37 are unpatentable, but has not proved that claims 14 and 33 are unpatentable.

## IV. ORDER

For the reasons given, it is:

ORDERED, based on a preponderance of the evidence, that claims 1–9, 12, 15–28, 31, and 34–37 are unpatentable; and

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

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

PATENT OWNER:

Peter Lambrianakos
plambrianakos@brownrudnick.com

Vincent Rubino
vrubino@brownrudnick.com

Trials@uspto.gov Paper No. 47
571-272-7822 Entered: December 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

FACEBOOK, INC.,
Petitioner,

v.

WINDY CITY INNOVATIONS, LLC,
Patent Owner.

---

Case IPR2016-01158
Patent 8,473,552 B1

---

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

MCKONE, *Administrative Patent Judge*.

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

## I. INTRODUCTION

### *A. Background*

Facebook, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") to institute an *inter partes* review of claims 1–61 and 64 of U.S. Patent No. 8,473,552 B1 (Ex. 1001, "the '552 patent"). Windy City Innovations, LLC ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp.").

Pursuant to 35 U.S.C. § 314, in our Institution Decision (Paper 7, "Dec."), we instituted this proceeding as to claims 1–59 and 64, but not claims 60 and 61.

Patent Owner filed a Patent Owner's Response (Paper 22, "PO Resp."), and Petitioner filed a Reply to the Patent Owner's Response (Paper 31, "Reply").

Petitioner relies on the Declarations of Tal Lavian, Ph.D. (Ex. 1002, "Lavian Decl."; Ex. 1021, "2nd Lavian Decl."). Patent Owner relies on the Declaration of Jaime G. Carbonell, Ph.D. (Ex. 2005, "Carbonell Decl.").

An oral argument was held on October 19, 2017 (Paper 46, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 1–59 and 64. Based on the record before us, Petitioner has proved, by a preponderance of the evidence, that claims 2, 3, 5, 7, 10–17, 59, and 64 of the '552 patent are unpatentable, but has not proved that claims 1, 4, 6, 8, 9, and 18–58 are unpatentable.

### *B. Related Matters*

The parties indicate that the '552 patent has been asserted in *Windy City Innovations, LLC v. Microsoft Corp.*, Civ. A. No. 15-cv-00103-GM

(W.D.N.C.) (transferred to 16-cv-1729 (N.D. Cal.)), and *Windy City Innovations, LLC v. Facebook, Inc.*, Civ. A. No. 15-cv-00102-GM (W.D.N.C.) (transferred to 16-cv-1730 (N.D. Cal.)). Pet. 1; Paper 4, 1. The ’552 patent was the subject of *inter partes* review petitions in IPR2016-01138, IPR2016-01137, IPR2016-01146, and IPR2016-01147. Paper 4, 1–2. The ’552 patent also was the subject of IPR2017-00603, which Microsoft Corp. filed and sought to join with this proceeding prior to settling with Patent Owner. Patents related to the ’552 patent are subjects of additional *inter partes* review petitions.

### *C. Asserted Prior Art References*

Petitioner relies on the following prior art:

U.S. Patent No. 6,608,636 B1, issued Aug. 19, 2003, filed May 13, 1992 (Ex. 1003, “Roseman”);

Published European Pat. App. No. 0 621 532 A1, published Oct. 26, 1994 (Ex. 1004, “Rissanen”);

Ronald J. Vetter, *Videoconferencing on the Internet*, IEEE COMPUTER SOCIETY 77–79 (Jan. 1995) (Ex. 1005, “Vetter”);

MARY ANN PIKE ET AL., USING MOSAIC (1994) (Ex. 1006, “Pike”);

TOM LICHTY, THE OFFICIAL AMERICA ONLINE FOR MACINTOSH MEMBERSHIP KIT & TOUR GUIDE (2nd ed. 1994) (Ex. 1007, “Lichty”).

### *D. The Instituted Ground*

We instituted a trial on the ground of unpatentability of claims 1–59 and 64 as obvious, under 35 U.S.C. § 103(a), over Roseman, Rissanen, Vetter, Pike, and Lichty. Dec. 37.

### *E. The ’552 Patent*

The ’552 patent describes an Internet “chat room.” According to the ’552 patent, it was known to link computers together to form chat rooms in which users communicated by text, graphics, and multimedia, giving the example of the Internet service provider “America On Line.” Ex. 1001, 1:40–46. The ’552 patent acknowledges that chat rooms have been implemented on the Internet, albeit with “limited chat capability,” but contends that the complex chat room communications capable with Internet service providers had not been developed on the Internet “at least in part because [the] Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications” and because “there is no particular control over the platform that would be encountered on the Internet.” *Id.* at 1:47–54, 1:60–62.

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

FIG. 1

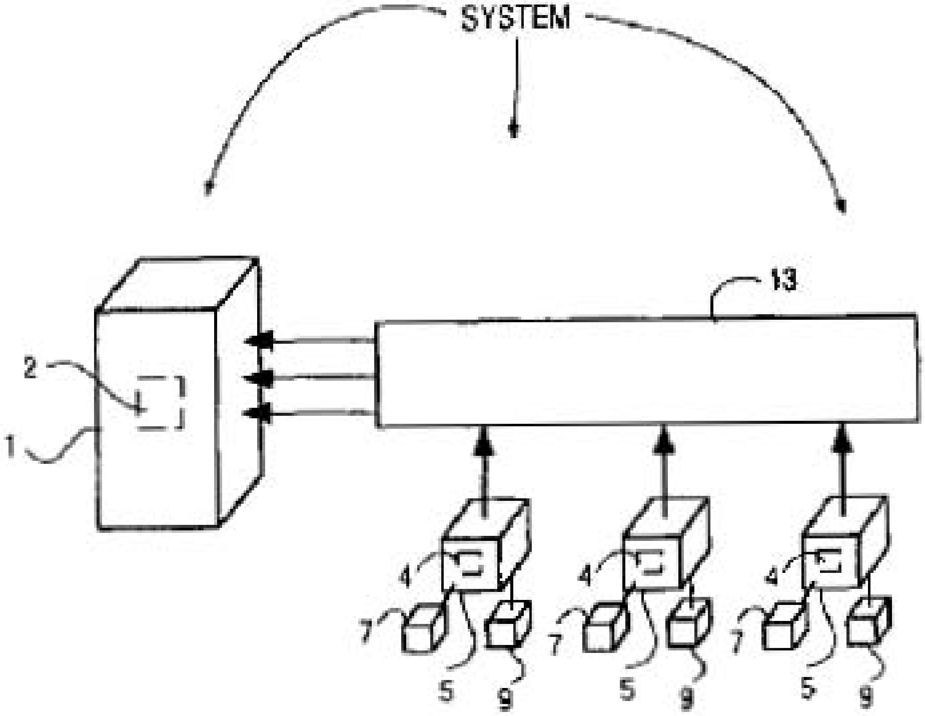


Figure 1 is a block diagram showing the components and data flow of a computerized human communication arbitrating and distributing system. *Id.* at 4:50–54. The system includes a controller computer (shown as 1 in Figure 1 but described as 3 in the written description) in communication with several participator computers 5 (e.g., IBM-compatible personal computers) over connection 13 (e.g., an Internet connection or a World Wide Web connection). *Id.* at 4:55–5:7.

The controller computer runs under the control of controller software 2, and the software arbitrates, in accordance with predefined rules (including user identities), which participator computers 5 can interact in a group through the controller computer, and directs real-time data to the members of the group. *Id.* at 5:8–14. The software uses "identity tokens," or pieces of information associated with user identity, in the arbitration. *Id.* at 7:61–64. The tokens are stored in memory 11 in a control computer database along with personal information about the users. *Id.* at 7:64–8:2.

The arbitration can be used to control a user's ability to join or leave a group of participator computers, to moderate communications involving the group, and to see other users in the group. *Id.* at 8:8–20. Arbitration using tokens also can be used to perform censorship:

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs [Uniform Resource Locators]—quantity, type, and subject.

*Id.* at 8:24–32.

According to the specification, "[t]he present invention comprehends communicating all electrically communicable multimedia information as Message 8, by such means as pointers, for example, URLs. URLs can point to pre-stored audio and video communications, which the Controller Computer 3 can fetch and communicate to the Participator Computers 5." *Id.* at 5:25–30.

Claim 2, reproduced below (disputed terms in italics), is illustrative of the claimed subject matter:

> 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, 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, the method including:
>
> affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;
>
> affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity;
>
> 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*.

## II. ANALYSIS

### *A. Claim Construction*

#### *1. Constructions in the Institution Decision*

We interpret claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *Cuozzo Speed Techs., LLC v. Lee*, 136 S. Ct. 2131, 2144–45 (2016). In applying a broadest reasonable construction, claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

In the Institution Decision, we preliminarily construed the following terms (Dec. 7–15):

| **Claim Term** | **Preliminary Construction** |
|---|---|
| "token" | "piece of information associated with user identity" |
| "database" | "a collection of logically related data" |
| "censor" | "control what is said in a group" |
| "at least one of the user identities, individually, is censored from data" | refers to control of data received by the at least one of the user identities, individually, and is not limited to data suppressed based on the content of those data or by a moderator |
| "pointer" | "a link or reference to a file, data, or service" |

| **Claim Term** | **Preliminary Construction** |
|---|---|
| "a pointer-triggered message on demand" | "a message, where the content of the message is specified by a pointer and found on demand of the operator of the participator software" |

Patent Owner adopts our construction of "token" (which Petitioner initially proposed) PO Resp. 8, and challenges our constructions of "database" and "censor," *id.* at 8–13. Petitioner accepts our constructions of "database" and "censor" and presents arguments in favor of those constructions. Reply 1–7. We maintain our construction of "token" on the complete record. We address the constructions of "database" and "censor," below, as well as the construction of the related term "at least one of the user identities, individually, is censored from data." Neither party challenges our constructions of "pointer" and "a pointer-triggered message on demand," and we maintain those constructions on the complete record.

### 2. *"database"*

In the Petition, relying on Dr. Lavian's testimony, Petitioner argues that "[a] person of ordinary skill in the art would have understood the claimed 'database' under its broadest reasonable construction to simply refer to a stored collection of tokens. The patent does not require that the database be any particular type, such as relational." Pet. 19 (citing Ex. 1002 ¶ 56). Dr. Lavian, in turn, relies on the specification's description of tokens being "stored in memory 11 in a control computer database, along with personal information about the user, such as the user's age." Ex. 1002 ¶ 56 (citing Ex. 1001, 7:64–66).

Patent Owner urges a construction that is narrower in two regards: (1) Patent Owner contends that a database is a collection of logically-related data "which is stored with persistence"; and (2) Patent Owner contends that a database includes "associated tools for interacting with the data such as a DBMS." PO Resp. 12.

Patent Owner's primary argument in favor of construing "database" to require these limitations is that it filed, in a related application before the Patent Office, an information disclosure statement (IDS) that supports its construction. *Id.* at 9–10 (citing Ex. 2008). The IDS was submitted to the Patent Office in pending application 14/246,965 on January 1, 2017, after Petitioner filed the Petition and shortly after we instituted this proceeding and preliminarily rejected Patent Owner's claim construction arguments. In the IDS, Patent Owner argued, *inter alia*, that "attention is respectfully drawn to the defendants' contentions[1] of invalidity in view of the database and 'other programs' limitations that are common to all claims" and that "[b]ecause the database affords information to other programs and computers, it must store the data, such as the tokens, with persistence, such that tools can interact with the data such as a DBMS when providing the data to the participator computers of the authenticated users." Ex. 2008, 2. Patent Owner argues that we must accept its construction pursuant to *Verizon Services Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1306 (Fed. Cir. 2007), which held that, in some circumstances, a statement made by a patentee in the prosecution history of a related application can operate

[1] This appears to be a reference to invalidity contentions filed in a related district court proceeding.

as a disclaimer, even if the disclaimer occurred after the patent-in-suit had issued. PO Resp. 10.

Although we doubt that the Federal Circuit intended that an IDS in a related application should be a vehicle for overturning a disadvantageous claim construction in an adversarial proceeding,[2] we need not reach that issue. As the Federal Circuit also held, "[t]o operate as a disclaimer, the statement in the prosecution history must be clear and unambiguous, and constitute a clear disavowal of claim scope." *Verizon*, 503 F.3d at 1306. That is not the case here. The statements in Patent Owner's IDS are not in response to any rejection by the Examiner, do not accompany any

[2] *See Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1270 (Fed. Cir. 1986) ("A citation may be made at 'any time' either during prosecution or, as here, after the patent has issued. If made during prosecution, it is clear that the statements may be considered for claim interpretation purposes, just as any other document submitted during prosecution. If submitted after issuance, the answer, again, is it may be considered. To say that it *may* be considered is not to say what *weight* statements in the Citation are to be accorded. For example, a Citation filed during litigation might very well contain merely self-serving statements which likely would be accorded no more weight than testimony of an interested witness or argument of counsel. Issues of evidentiary weight are resolved on the circumstances of each case."); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1317 (Fed. Cir. 2005) (en banc) ("Like the specification, *the prosecution history provides evidence of how the PTO and the inventor understood the patent*. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes." (emphasis added)).

amendments, and are not directed to any particular claims, other than a general statement that the statements apply to "all claims."[3] Ex. 2008, 2.

Although Patent Owner argues that the IDS "supports the construction that a database is limited" in the manner that it argues, Patent Owner does not contend that the IDS constitutes a disclaimer of any subject matter. PO Resp. 10. We find that the IDS does not contain a "'clear and unmistakable' disclaimer that would have been evident to one skilled in the art." *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1064 (Fed. Cir. 2016). Therefore, we are not persuaded that we should apply prosecution history disclaimer to limit the scope of the term "database."

Patent Owner also cites to the testimony of Dr. Carbonell that "[t]wo hallmarks of a database are (1) persistence of the data, and (2) interactivity with the data via a database management system (DBMS)." *Id.* (quoting Ex. 2005 ¶ 33). As Petitioner points out (Reply 1–2), Dr. Carbonell's testimony on this point appears to be a copy of the testimony of Dr. Bajaj, who submitted a declaration in support of Patent Owner's Preliminary Response (*compare* Ex. 2005 ¶ 33, *with* Ex. 2001 ¶ 20), although Dr. Carbonell testified that he was unaware of Dr. Bajaj's declaration (Ex. 1016, 132:2–12). In any case, as Petitioner points out, Dr. Carbonell marshals the same evidence that did not persuade us at the institution stage without adding any additional evidence or even acknowledging our concerns with Dr. Bajaj's evidence. Reply 2 n.1.

[3] Adding to the ambiguity, it is not clear whether the IDS's reference to "all claims" refers to the claims in the pending application or the claims discussed in the defendants' contentions of invalidity to which the sentence is directed.

In particular, Patent Owner and Dr. Carbonell cite to the Macmillan Encyclopedia of Computers (Ex. 2004). PO Resp. 10–11; Carbonell Decl. ¶ 33. In the portion included in Exhibit 2004, The Macmillan Encyclopedia states that "[a] database system is a collection of related records stored in a manner that makes the storage and retrieval of the data very efficient. The four well-known data models for databases are the hierarchical, network, relational, and object-oriented models." Ex. 2004, 230. This definition does not require persistence and Patent Owner does not explain why persistence should be inferred from this definition. Moreover, as we observed in the Institution Decision, the Macmillan definition is consistent with the definition of "database" given by the IEEE Dictionary of Standards Terms. *See* IEEE 100 THE AUTHORITATIVE DICTIONARY OF IEEE STANDARDS TERMS 268 (7th ed. 2000) ("**database (DB)** . . . A collection of logically related data stored together in one or more computerized files.") (Ex. 3001). This definition also does not require persistence. Although this dictionary was published several years after the filing date of the '552 patent, Dr. Lavian testifies that the plain and ordinary meaning of "database" did not change during this time. Ex. 1021 ¶ 11. In support of this testimony, Dr. Lavian cites to a 1991 textbook, which defines "database" as "a collection of interrelated data," yet another definition that does not require "persistence." *See* Ex. 1017, 5. Moreover, we observe that Patent Owner provides no boundaries for "stored with persistence" to meaningfully limit the term. For example, all data accessed and stored by a program while the program is executing has some level of "persistence."

As to a DBMS, Macmillan explains:

> A database management system (DBMS) is a software package. Its main functions are (1) to provide the facility to set up the database, (2) to retrieve and store source data (actual data in the database), (3) to retrieve and store the data about the structure of the database (data dictionary), (4) to provide the facilities to enforce security rules, (5) to back up the database, and (6) to control the concurrent transactions so that one user's environment is protected from others.

Ex. 2004, 231. Patent Owner characterizes the DBMS as "another criteria of a database" that provides interactive querying capability not present in "[s]tandard storage" in temporary or permanent memory. PO Resp. 11. Dr. Carbonell repeats Patent Owner's arguments without citation to evidence and in testimony that largely copies that of Dr. Bajaj. Ex. 2005 ¶¶ 33–36; *see also* Ex. 2001 ¶¶ 20–23. Nevertheless, we read Macmillan to describe a DBMS as software that works with a database, rather than a part of a database or a component that necessarily accompanies a database. Dr. Carbonell's testimony, which does not identify its bases, adds little to Macmillan. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Patent Owner also argues that the disclosure of the '552 patent imposes "persistence" and DBMS limitations on the claimed database because it describes the database as storing security information such as tokens for other programs to access. PO Resp. 12. Patent Owner does not provide a citation to the '552 patent in support of its argument. Nevertheless, Patent Owner argues, again without citation, that "[o]ne of ordinary skill in the art would have expected that this type of security feature would persist in a location other than in program memory so that other user programs could access the information." *Id.* Finally, Patent Owner argues that the '552 patent describes tokens stored in hierarchies, which, according to Patent Owner, "are typical of database storage organization, and natural schema when storing and managing access to diverse information." *Id.* None of these arguments supports reading persistence or a DBMS into the term "database." We note also that the other claim language, "serves as a repository of tokens for other programs to access," is a requirement we evaluate separately and do not read into the term "database."

As noted in the Institution Decision (at 10), the specification describes a database consistently with the Macmillan and IEEE definitions, explaining that tokens are "pieces of information associated with user identity," that tokens are "stored in memory 11 in a control computer database, along with personal information about the user," and that "[i]n the database, the storage of tokens can be by user, group, and content." Ex. 1001, 7:61–8:5. The specification does not require a DBMS (or similar software) or impose a persistence requirement.

On the complete record, we maintain our construction of database, namely, "a collection of logically related data." This is the construction most consistent with both the intrinsic evidence and dictionary definitions. However, we note that Petitioner contends, and we find, that the prior art shows a database with persistence and associated tools for interacting with the stored data, as explained below.

### *3. "censor" / "at least one of the user identities, individually, is censored from data"*

Claim 2 recites "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 other challenged independent claims include similar recitations. As noted above, we preliminarily construed "censor" to mean "control what is said in a group" and explained that "at least one of the user identities, individually, is censored from data" refers to control of data received by the at least one of the user identities, individually, and is not limited to data suppressed based on the content of those data or by a moderator. Dec. 13.

We based our construction on the description of that term in the specification. *Id.* at 12. Specifically, the specification describes censorship as follows:

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. *Censorship can control of access* [sic] *to system 1 by identity of the user*, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

Ex. 1001, 8:24–32 (emphasis added). Here, the specification describes "censorship" as "broadly encompass[ing] control of what is said in a group" and includes an example in which an action is taken on a user, rather than the data itself.

Patent Owner argues that "censorship should be construed to be 'examine in order to suppress or delete anything considered objectionable.'" PO Resp. 13. According to Patent Owner, "[i]n order to control what is said in a group, it is necessary to first know what is said (or proposed to be said)." *Id.* Patent Owner argues that this is consistent with the meaning given to "censor" and "censorship" in dictionaries, including "to examine in order to suppress or delete anything considered objectionable" (Webster's Collegiate Dictionary (Ex. 2002)) and "[t]he action of preventing material that a party considers objectionable from circulating within a system of communication over which that party has some power" (Microsoft Press Computer Dictionary (Ex. 2003)).

We are not persuaded by Patent Owner's arguments, which essentially track those presented in the Preliminary Response (at 6–7). The claim language itself does not support a construction of "censor" limited to analysis of the content of data and suppression based on that content. Claim 2 recites "at least one of *the user identities, individually, is censored* from data." The claim language focuses on censoring a user identity and does not specify that such censoring is based on the content of the data. As explained above, the specification describes censorship as an action taken on a user, rather than the data itself. As explained in the Institution Decision (at 12–13), extrinsic evidence such as dictionary definitions "may be used only to help the court come to the proper understanding of the claims; it may not be used to vary or contradict the claim language." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1584 (Fed. Cir. 1996); *accord Phillips*, 415 F.3d at 1317 ("[W]hile extrinsic evidence can shed useful light on the relevant art, we have explained that it is less significant than the intrinsic record in determining the legally operative meaning of claim language.") (internal citations and quotation marks omitted).

On the complete record, in accordance with the specification's definition, "censor" means "control what is said in a group." In the context of claim 2, for example, "at least one of the user identities, individually, is censored from data" refers to control of data received by the at least one of the user identities, individually, and is not limited to data suppressed based on the content of those data or by a moderator. We apply the same definition of "censor" in interpreting similar language in the remaining challenged independent claims.

### *B. Asserted Grounds of Unpatentability*

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

[4] The record does not include arguments or evidence regarding objective indicia of nonobviousness.

In an obviousness analysis, some reason must be shown as to why a person of ordinary skill would have combined or modified the prior art to achieve the patented invention. *See Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008). A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the "interrelated teachings of multiple patents"; "any need or problem known in the field of endeavor at the time of invention and addressed by the patent"; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

### *1. Level of Ordinary Skill*

Relying on Dr. Lavian's testimony, Petitioner contends that a person of ordinary skill in the art "would have had at least a bachelor's degree in electrical engineering or computer science (or equivalent degree or experience) with practical experience or coursework in the design or development of systems for network-based communication between computer systems." Pet. 7–8 n.1 (citing Ex. 1002 ¶ 14). Patent Owner does not contest this statement in its Response. In his testimony, Dr. Carbonell proposes a similar level of skill, namely "a bachelor's degree in computer science (or a related field) and at least one year of work experience in programming in computer communication methods." Ex. 2005 ¶ 18. Dr. Carbonell states that his opinions would not change under a determination that Dr. Lavian's opinion regarding the level of ordinary skill is correct. *Id.* On the complete record, we adopt Petitioner's statement of the level of ordinary skill, although we note that Dr. Carbonell's statement of the level of skill is not materially different.

### *2. Scope and Content of the Prior Art*

Petitioner contends that the challenged claims would have been obvious over Roseman, alone or in combination with Rissanen, Vetter, Pike, and Lichty. Pet. 7–8.

#### *a. Overview of Roseman*

Roseman describes a system for multimedia conferencing, in which parties are linked by both video and audio media. Ex. 1003, Abstract. In Roseman, a conference is represented visually as a common virtual conference table, in which each participant can place a document onto the table electronically, manipulate and write on the document, write on a virtual notepad, and move a pointer to draw other users' attention. *Id.* at 2:38–45, 7:55–8:37. Participants can see the events as they occur. *Id.* at 2:46–47. Figure 9, reproduced below, illustrates an example conference room:

FIG. 9

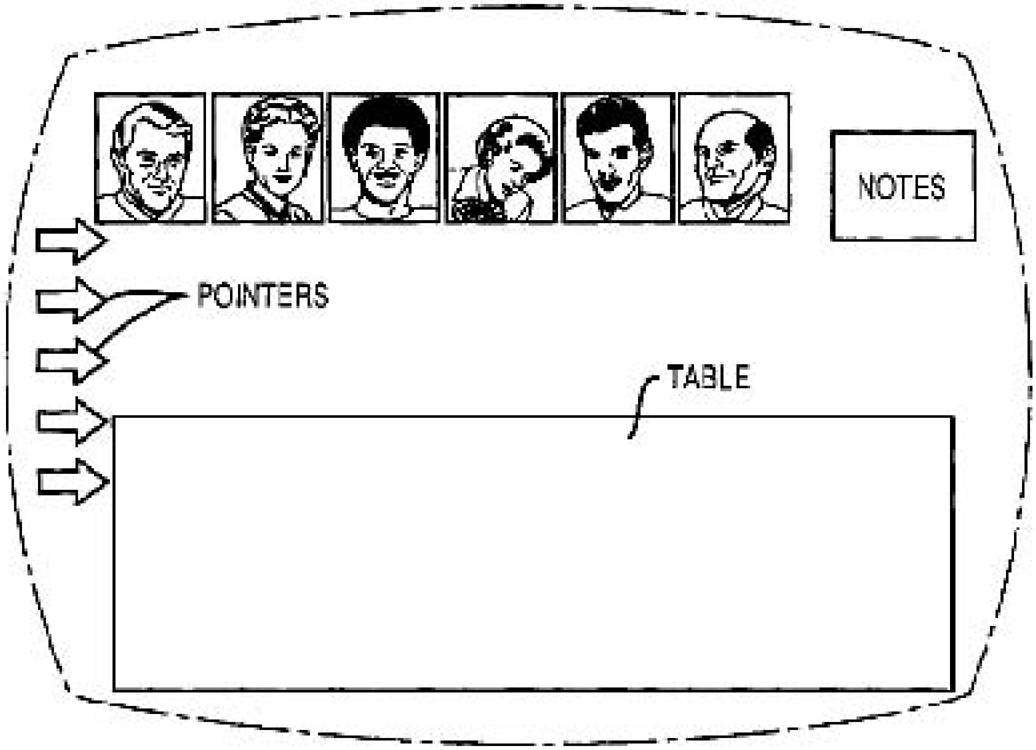


Figure 9 is a picture of a video screen that is generated by a host computer and distributed to all participants in a conference. *Id.* at 2:16–18.

The parties operate their own local computers (which include video cameras and speaker-type telephones) and, when a conference is established, connect to a host computer via commercially available local area networks (“LANs”) and wide area networks (“WANs”). *Id.* at 1:34–41. In the conference, the host computer generates a common video screen (e.g., Figure 9, reproduced above) displayed at each of the local computers, and the parties send information, such as drawings, to be displayed on the common screen. *Id.* at 1:42–46. The telephones and video cameras allow the parties to see and speak with each other. *Id.* at 1:47–49.

Roseman includes a pseudo code appendix that details how its features are implemented. *Id.* at 12:66–13:2. According to the pseudo code, a participant interacts with the conference table, for example, by dragging an icon onto the table, which causes a data file to be transmitted to the host. *Id.* at 14:53–55. The host then transmits the icon to the table of each participant. *Id.* at 14:56–57. If another participant activates the icon, the host sends the open file to the tables of all participants. *Id.* at 14:58–61. If the participant drags the icon from the table to his own screen and activates the icon on his screen, the data file is presented to the participant. *Id.* at 14:62–66.

Roseman describes additional features, such as a party's ability to "whisper" to another party without being heard by others in the conference room, and the ability to "pass notes" by dragging a note to the picture of another party, while the other parties are unaware of the note. *Id.* at 9:16–31. Each room may also have "doors" to committee rooms or child-rooms. A child-room is created in the same way as a parent room and is dependent upon the parent room for access and existence. *Id.* at 10:18–23.

A meeting requester creates a conference by selecting the participants, the attributes of the virtual conference room (e.g., virtual equipment and room décor), and the rules of the conference (e.g., whether the requester has absolute control over voice and message interaction of the parties). *Id.* at 3:22–56. According to Roseman, "[t]he conference room itself is actually a combination of stored data and computer programs," the stored data can include conference proceedings, and "both the conference room and the proceedings of the conference have persistence in time." *Id.* at 12:16–25.

The meeting requester specifies a level for each invitation and compiles an invitation list. *Id.* at 9:34–36. Invitations include "keys" specifying the level, e.g., whether the invitation is for the invitee only or can be passed to a delegate or to anyone. *Id.* at 9:35–48. For example, "Level 1 keys may not be passed to any other person and may not be copied" while "Level 2 keys may be passed to exactly one other person and may not be copied." *Id.* at 9:42–45. According to Roseman, "[t]he meeting room 'knows' about each key and its invitation level. Persons with improper keys are not admitted to the room." *Id.* at 9:49–51. A key is distributed electronically as an object attached to the invitation. *Id.* at 9:54–55. To attend a meeting, a party walks a virtual "hallway" to the meeting room and opens the meeting room door by dropping the key onto a virtual "door lock." *Id.* at 10:30–32, 10:61–65. Moreover, the host "can automatically prevent filibustering" by "monitor[ing] the speech of each person, and plac[ing] a limit on the total time allowed to each person." *Id.* at 12:29–38.

### *b. Overview of Rissanen*

Rissanen describes a system and method for validation of spoken passwords. Ex. 1004, 2:17–21. Rissanen's Background of the Invention discusses systems in which "business computer systems are arranged to initially record and store passwords assigned to users," a user is prompted for entry of a password, 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." *Id.* at 1:21–28. In Rissanen's proposed solution, "[u]sers 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.” *Id.* at 2:26–29.

Petitioner makes clear that “[a]lthough Rissanen also describes using spoken voice passwords, this Petition cites it for its more pedestrian teachings relating to database storage of passwords of any form.” Pet. 12.

### *c. Overview of Vetter*

Vetter is an IEEE Computer Society Magazine article discussing available tools for conducting teleconferencing over the Internet. According to Vetter, “[v]ideoconferences are becoming increasingly frequent on the Internet and are generating much research interest.” Ex. 1005, 77. Vetter states that “the emerging multicast backbone (or MBone) can efficiently send traffic from a single source over the network to multiple recipients,” and, “[a]t 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.” *Id.* Vetter concludes that “[t]he 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.” *Id.*

Vetter also describes challenges that faced implementation of audio, graphic, and video tools on the Internet, including “disturbing feedback when the microphones at multiple sites were left ‘open’ during a discussion,” taking too much time to broadcast a simple graphic image to multiple participants when using “Whiteboard tools” (collaborative software tools that support a shared desktop whiteboard among a group of distributed users on the Internet), and use of video during a classroom presentation that

caused the workstations in the classroom lab to lock up. *Id.* at 78–79. Vetter also notes that the physical distance between two points on the Internet can be different from the electronic distance between those points. *Id.* at 79.

Vetter discusses in particular a CU-SeeMe platform from Cornell University that supported video and audio conferencing over the Internet, and a CU-SeeMe Reflector that allowed multiparty conferencing with CU-SeeMe. *Id.* at 78.

### *d. Overview of Pike*

Pike is a reference and guide book for using the Web browser Mosaic. Ex. 1006, 2. Petitioner cites to Pike's discussion of URLs and hyperlinks. According to Pike, URLs were developed as a standard way of referencing items on the World Wide Web. *Id.* at 38. "A *URL* is a complete description of an item, containing the location of the item that you want to retrieve. 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.*

### *e. Overview of Lichty*

Lichty is a book intended as a "tour guide" of America Online ("AOL"), an online email service, Internet gateway, and community. Ex. 1007, 1–3. Petitioner (Pet. 34) focuses on Lichty's description of AOL's real-time interactive "People Connection" feature. Ex. 1007, 251–78. People Connection includes chat rooms in which a user communicates with others by posting text messages to the other participants in a chat room. *Id.* at 252–55. Lichty describes, in particular, that a People Connection interface includes an "Ignore" button. *Id.* at 268–69. According to Lichty, "[i]f you wish to exclude a member's comments (or those of all the members in a 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." *Id.* at 269; *see also id.* at 510 (glossary definition of "Ignore—(1) Chat blinders; a way of blocking a member's chat from your view in a chat/conference room window. Ignore is most useful when the chat of another member becomes disruptive in the chat room.").

### *3. Claim 2, Differences Between the Claimed Subject Matter and the Prior Art, and Reasons to Modify or Combine*

Petitioner contends that Roseman teaches each limitation of claim 2, but cites the remaining references for the following, should we determine that Roseman lacks such a teaching:

Rissanen for a teaching that tokens could have been stored in a database;

Vetter for a teaching that Roseman's communications could have been over the Internet;

Pike for a teaching of URLs; and

Lichty for a teaching of content filtering, in particular an "ignore" feature, which Petitioner equates to "censoring."

Pet. 7–8.

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

Petitioner contends that Roseman's host computer is a controller computer. Pet. 16. Petitioner identifies Roseman's local computers as independent participator computers and argues that Roseman's various ways of communicating information (placing documents on a virtual table, shared notes, whisper conversations) are examples of affording information to those participator computers. Pet. 26–27. As detailed above, Roseman describes a system in which individual computers are connected to a central host computer via a combination of LANs and WANs. Ex. 1003, 3:14–19. According to Roseman, "[t]he 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." *Id.* at 1:50–52. We find that Roseman's host computer is a "controller computer," that Roseman's local computers are "participator computers," and that Roseman's various ways of communicating information from the host to the local computers are examples of "affording information to each of a plurality of participator computers which are otherwise independent of each other," as recited in claim 2.[5]

[5] Patent Owner argues that "Petitioner does not address the issue that the **database** affords information to each of a plurality of computers." PO Resp. 21. Claim 2, however, does not recite that the database affords information to the plurality of computers.

The parties dispute whether Roseman describes "a database which serves as a repository of tokens for other programs to access." First, Petitioner contends that Roseman's "keys" are tokens. Pet. 17–18. As explained above, the parties agree that a "token" is "a piece of information associated with user identity." As also explained above, Roseman describes that an invitor, in setting up a meeting, creates an invitation that includes a key that conforms to an invitation level. Ex. 1003, 9:34–48. A key "is an electronic object attached to the invitation." *Id.* at 9:54–55. The "level" of a key determines who can use it. For example, "Level 1 keys may not be passed to any other person and may not be copied." *Id.* at 9:42–44. According to Roseman, "[t]o 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." *Id.* at 10:61–64. Petitioner argues that this evidence shows that Roseman's keys are "pieces of information associated with a user identity," and thus, are "tokens." Pet. 18.

Patent Owner argues that Roseman's keys are not tokens because they are associated only with conference rooms, rather than user identities. PO Resp. 19. Patent Owner points to Roseman's Figure 8, which shows a key associated with "CONFERENCE ROOM 17L (DATE, TIME)." *Id.* In describing Figure 8, however, Roseman explains "the key is, essentially, a block of data, or a code," that can be used if the Invitee may send a delegate, to give the Absentee-Invitee a "key," which enables access to the meeting. Ex. 1003, 6:54–61. "The Requester can leave the key in his local computer, in the form of an icon residing on the display, as shown in FIG. 8. Anyone entering the office can use the key." Ex. 1003, 6:60–63. In this example, the key can be used only with a particular user's computer. Figure 8 also shows the "key" icon contained within a "vault" icon. *Id.* at 6:64–65. In this example,

> a user must use a "combination" to the "vault" to obtain the "key." In this latter example, the [] "combination" (ie, a pass-code) is obtained from the Absentee-Invitee in some appropriate way. At conference time, the Delegate opens the "vault," obtains the "key," and enters the conference room, by using the key.

*Id.* at 6:65–7:3. Patent Owner argues that Roseman's keys are "transferable to anyone—like a key to a door lock." PO Resp. 19. Patent Owner contends that Roseman teaches away from keys being associated with a specific user through its description that "***[k]eys may be copied and redistributed, if permitted***, or sent to another individual, if permitted." PO Resp., 19–20 (quoting Ex. 1003, 9:55–57) (emphasis by Patent Owner).

Patent Owner's arguments are not persuasive. Roseman describes keys that are transferable (Level 2 and 3 keys) and keys that are not transferable (Level 1 keys). Ex. 1003, 9:42–48. Petitioner's contentions (Pet. 18) are directed to Level 1 keys, which "may not be passed to any other person and may not be copied." *Id.* at 9:43–44. We find that keys that may not be passed to any other person are keys associated with that person. Figure 8 of Roseman is consistent with this because it describes passing a key to an "Absentee-Invitee" when the Invitee sends a delegate, i.e., a Level 2 key.

As to Level 1 keys, Patent Owner argues that a key is merely an attachment to an invitation, which "offers the only suggestion of an association with specific invitee." PO Resp. 20. Dr. Carbonell testifies (without identifying a basis) that Roseman's system could prevent the transfer of a key using a "no-transfer or no-duplication policy of such a key to insure that [it] always stays in the possession of the first user," by making transferability an attribute of the key and having the system simply assume, without recording transfers, that a user in possession of a key is authorized to use it. Ex. 2005 ¶ 31. As Petitioner argues, however, the claim construction to which Patent Owner agreed does not require an association between a key and a user to be implemented in a certain way. Reply 15–16. Even if Dr. Carbonell is correct as to how Roseman's keys would be implemented, such a non-transferable key would still be associated with the person who is prevented from transferring it.

Petitioner further argues that Roseman discloses storing keys in "a database which serves as a repository of tokens," as recited in claim 2, because a meeting room that is accessed by a key "'knows' about each key and its invitation level." Pet. 18–19 (quoting Ex. 1003, 9:49–51). According to Petitioner, a copy of each key must be stored on the host computer for the meeting room to "know" about each key. *Id.* at 19. Petitioner argues that a skilled artisan would have understood a database to be a stored collection of tokens. *Id.* Roseman does not expressly describe storing tokens in a database. Thus, we understand Petitioner to argue that tokens necessarily are stored in a database in light of Petitioner's cited disclosure—in other words, that a database is inherent in Roseman.

Patent Owner, relying on Dr. Carbonell's testimony, argues that a meeting room's knowledge of a key could be implemented using a hash function, which would not have required storage of the key in a database. PO Resp. 21–22 (citing Ex. 2005 ¶ 40). Petitioner characterizes Patent Owner's argument as "based on pure speculation and conjecture" and inconsistent with Roseman's disclosure. Reply 10–12. Nevertheless, we view both parties' respective theories of Roseman's implementation as speculation. Because Petitioner's position is speculative, it is insufficient to show that a database is inherent in Roseman.[6]

In the alternative, Petitioner argues that Rissanen teaches storing user authentication information, such as user identity information and passwords, in a database, and that such teaching would have been applicable to the keys of Roseman. Pet. 20–21. Petitioner argues that Roseman's keys are analogous to user identity and passwords. *Id.* at 20. According to Petitioner and its expert, Roseman's key verification step might not function properly if the keys are not stored in a database. *Id.* at 21 (citing Ex. 1002 ¶ 58). Petitioner further argues that storing keys in a database is one of a finite number of known solutions for verifying whether a previously issued key matches to a key later presented by a user to access a conference room. *Id.* at 21–22 (citing Ex. 1002 ¶¶ 58–59).

Patent Owner admits that "[Rissanen] does disclose a database," but argues that its database is used in a different type of system. PO Resp. 23. Thus, Patent Owner does not contest that Rissanen's database stores user identities and passwords in a persistent manner and is used in conjunction

[6] Patent Owner also argues that Roseman does not suggest storing keys in a manner that is persistent and does not disclose tools such as a DBMS. PO Resp. 22–23. Roseman does teach that the data associated with its conference rooms are stored in a manner that is persistent, Ex. 1003, 12:16–28, and this at least suggests that keys also would be stored in such a manner. As to a DBMS, we explain above that the construction of "database" does not require this feature. Nevertheless, as explained below, Rissanen teaches a database even under Patent Owner's proposed construction.

with tools such as a DBMS. For Petitioner, Dr. Lavian testifies that "Rissanen clearly discloses a relational database whose data is stored persistently and includes tools for interacting with the data such as a DBMS." Ex. 1021 ¶ 37. We find that Rissanen teaches a database that stores data with persistence and tools for interacting with the database.

Nevertheless, Patent Owner argues "[i]f one were going to combine Roseman and Rissenan in order to authenticate an individual (and not merely authenticate a key for a room) the necessary logic would be significantly more complicated." PO Resp. 23. Petitioner does not argue, however, that Rissanen's database would be bodily incorporated into Roseman's system. Rather, Petitioner argues that Rissanen teaches storing data "analogous to and serv[ing] the same purpose as" the keys in Roseman in a database. Pet. 20. *See In re Mouttet*, 686 F.3d 1322, 1332–33 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements. . . . Rather, the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art."). Given that Roseman describes using keys to access conference rooms that have persistence, we agree with Petitioner that a database, described in Rissanen as storing similar information for a similar purpose, would be a straightforward and predictable choice for storing Roseman's keys.

The parties also dispute whether Roseman and Rissanen teach that the database "serves as a repository of tokens *for other programs to access*, thereby affording information to each of a plurality of participator computers," as recited in claim 2. Petitioner argues that other programs access the stored collection of tokens, including the various meeting or conference rooms maintained on the host computer. Pet. 22. Petitioner relies on disclosure in Roseman that a meeting room is accessible from a virtual hallway with doors to other meeting rooms. *Id.* (citing Ex. 1003, 9:63–65). According to Petitioner, "[e]ach meeting room . . . 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." *Id.*

Patent Owner argues that "Petitioner does not identify any programs that could access a database of tokens and receive information, other than the singular conference calling software running on the host computer of Roseman." PO Resp. 25. According to Patent Owner, "to the extent that there are multiple conference rooms programs [sic] in existence, that is because the Roseman system has instantiated the same conference room program with different parameters as there is no suggestion that there is different software associated with each conference room." *Id.* Patent Owner does not explain why "other programs" require different software rather than different instantiations of the same software, or point to evidence supporting this view. We are not persuaded that the claims should be limited in this way. Nevertheless, as Petitioner points out (Reply 18), Roseman characterizes its conference rooms as collections of different programs (Ex. 1003, 12:16–18) and makes clear that different conference rooms will have different attributes (different virtual equipment, different tools, different appearances, etc.) (*id.* at 3:42–50, 10:9–12). We find that Roseman at least suggests different conference rooms with different programs, even under Patent Owner's view. These programs determine whether a participant can join a meeting room based on evaluations of keys that, in light of Rissanen, would have been stored in a database. Thus, we find that Roseman and Rissanen teach "a database which serves as a repository of tokens for other programs to access," as recited in claim 2.

The parties also dispute whether Roseman and Vetter teach "communicating via an Internet network," as recited in claim 2. As explained above, Roseman describes communicating between a host and local computers via commercially available LANs and WANs. Ex. 1003, 1:37–41, 3:14–19. Petitioner contends that a skilled artisan would have understood the Internet to be an example of the commercially available WAN described in Roseman. Pet. 23, 25; Ex. 1002 ¶¶ 65–66. According to Dr. Lavian, "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." Ex. 1002 ¶ 65; *see also* Ex. 2006 (Lavian Dep.), 104:12–105:23 ("Q So Roseman could have been implemented in that 1994 to '96 time frame with ATM technology? A If I'm looking at the specification of Roseman and what specifically Roseman disclose, it disclose as using a -- local computers become connected to host computer via commercially available Local Area Networks and Wide Area Networks. When you're talking about Local Area Networks and Wide Area Networks, this is the Internet. That's different name to Internet. Q So you're saying that Roseman by itself teaches the Internet? A Roseman by itself reference to remote computers commercially available, commercially available that said Internet. Local Area Networks, definitely part of the Internet. Wide Area Networks, different name to the Internet. It's actually the Internet itself. . . .").

Petitioner further argues that Vetter teaches using the Internet to facilitate the same types of computer-based conferencing functions as described in Roseman. Pet. 23–24. Petitioner contends that Vetter itself identifies a reason to combine the teachings of Roseman and Vetter, namely "[v]ideoconferences are becoming <u>increasingly frequent</u> on the Internet" and the CU-SeeMe videoconferencing tool described in Vetter "is also becoming <u>very popular</u>." *Id.* at 25 (quoting Ex. 1005, 77 (emphases by Petitioner)).

Patent Owner argues that Vetter does not state that Internet videoconferencing would have been ubiquitous at the time of the invention; rather, Patent Owner argues, the Internet was beginning to support video conferencing. PO Resp. 26–27. Patent Owner further argues that Vetter discusses difficulties in applying videoconferencing on the Internet, including feedback when participants leave their microphones on, degraded performance when broadcasting simple graphic images, workstations that locked up in a classroom when video streams overwhelmed a network, and counter-intuitive paths that data can take when travelling from one site to another. *Id.* at 27–28 (citing Ex. 1005, 78–79). Dr. Carbonell testifies (without citation) that video traffic on the Internet would experience unpredictable delay that would interfere with re-assembling video streams at the receiving end in real time. Ex. 2005 ¶ 59. Dr. Carbonell testifies (again without citation to evidence) that one would not experience these problems on a private WAN because such a network would be of a more predictable configuration. *Id.* ¶ 61.

Patent Owner also points to a half-page article in a technical magazine by Robert Metcalfe, founder of 3Com, "[p]redicting the Internet's catastrophic collapse" at the end of 1995 due to reasons such as low user measurements, telecom company monopolies, and security and capacity concerns. PO Resp. 28–29 (quoting Ex. 2009). We agree with Petitioner, however, that "the incorrect prediction of a single individual would not have discouraged (and did not discourage) the industry from using the Internet." Reply 8. Patent Owner offers no persuasive evidence that Dr. Metcalfe's views were shared widely, or at all, by skilled artisans in 1995. Indeed, the article itself suggests the contrary. Ex. 2009 ("Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth.").

Citing Dr. Metcalfe's article, Dr. Carbonell testifies that other technologies such as Integrated Services Digital Network (ISDN) and Asynchronous Transfer Mode (ATM) would have been better suited than the Internet to handle video conferencing in the mid-1990's. Ex. 2005 ¶ 60. As explained above, Patent Owner has not explained persuasively why Dr. Metcalfe's magazine article is representative of the views of a skilled artisan. The article itself does not state that there were, or identify evidence of, technologies better suited than the Internet to handle videoconferencing. Ex. 2009. Thus, we are not persuaded that the Internet would have been an inferior technology for videoconferencing in 1995. Moreover, claim 2 on its face is not limited to videoconferencing. In any case, the Federal Circuit has explained that "just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes." *Mouttet*, 686 F.3d at 1334.

Roseman expressly states that its local computers and host communicate via a commercially available WAN. We credit Dr. Lavian's testimony that, to the extent that this is not an express reference to the Internet, the most suitable and obvious commercially available WAN would have been the Internet. We also find that Vetter suggests using the Internet for purposes similar to those of Roseman. Vetter describes an example in which features such as audio, video, and virtual whiteboard tools are used to conference over the Internet. Ex. 1005, 77–78. Thus, to the extent Roseman does not expressly suggest using the Internet, Vetter includes an express suggestion to update a system such as Roseman using modern electronic components, such as the Internet, to gain the commonly understood benefits of such adaptation. *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007); *cf., Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1326–27 (Fed. Cir. 2008) ("The record in this case demonstrates that adapting existing electronic processes to incorporate modern internet and web browser technology was similarly commonplace at the time the '099 patent application was filed."). Vetter reinforces our finding that the Internet would have been the most suitable commercially available WAN for use in Roseman's system.

To be sure, Vetter discusses challenges encountered in implementing videoconferencing on the Internet, but Vetter also teaches that existing tools can be tailored to specific applications on the Internet "so that their limitations can be *promptly recognized and corrected*." Ex. 1005, 79 (emphasis added). The Federal Circuit has recognized that "a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v.*

*Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006). We find that addressing the challenges discussed in Vetter would have been well within the skill of an ordinarily skilled artisan, an engineer experienced in computer networking. Thus, we find that Roseman, Rissanen, and Vetter teach "[a] method of communicating via an Internet network" as recited in claim 2.

In sum, we find that the combination of Roseman, Rissanen, and Vetter teaches "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," as recited in claim 2.

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

In the Institution Decision, we determined that the claim language "the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives" refers to separate software platforms implementing user interfaces on two different participator computers, with both providing access to the control computer. Dec. 27. This is the reading most consistent with the '552 patent's description. Ex. 1001, 2:35–41 ("Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message."), 4:43–49 ("[T]he appendix includes code for two different embodiments: a Tellnet embodiment and a JAVA embodiment. . . . While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled."), 5:15–19 ("The Participator Computers 5 are each running and under the control of Participator Software 4, which directs each of the Participator Computers 5 to handle a user Interface 6 permitting one said user to send a multimedia information Message 8 to the Controller Computer 3 . . . .").

Petitioner argues that Roseman describes its local computers as using a Windows operating system, but notes that other environments are within the level of skill in the art. Pet. 28 (citing Ex. 1003, 12:1–5, 12:9–10). Dr. Lavian testifies that it was well-known to provide software products for multiple computing platforms, such as Windows and Macintosh because it was more commercially attractive and would increase the number of users who could use the software. Ex. 1002 ¶ 73. Petitioner argues that it would have been obvious to provide alternatives for local computer software that would operate on Windows and Macintosh platforms. Pet. 28.

Patent Owner argues that "Roseman does not indicate how a second alternative would be able to communicate with the host computer to receive the common image or to interact with it" and that "Roseman's disclosure of the 'Windows Context' is not an affirmative teaching of another client software alternative." PO Resp. 35. Petitioner, however, does not argue that Roseman expressly teaches two client software alternatives. Rather, Petitioner argues that Roseman describes one software alternative, for the Windows platform, and expressly teaches that software for other platforms would have been within the level of skill in the art. Pet. 28; Reply 22 ("The Petition explained that the claimed two client software alternatives were obvious, among other reasons, because it would have been obvious to adapt the participator software in Roseman to run on multiple computing platforms, such as Windows and Macintosh.").

Patent Owner argues that Roseman does not "indicate how any of its client software could be modified so as to make [a] second software alternative." PO Resp. 35. According to Patent Owner, Dr. Lavian admitted in deposition that it is not always possible to make the same software programs for different operating systems. *Id.* at 36 (citing Ex. 2006, 157:6–158:11). Although it might not be possible to adapt every software program to work on every operating system, Roseman itself suggests adapting its software to different environments beyond Windows. Ex. 1003, 12:1–10. Thus, Patent Owner's argument is not persuasive.[7]

Patent Owner also argues that Windows and Macintosh are not client software, but instead are operating systems. PO Resp. 35–36. Petitioner, however, does not argue that Windows and Macintosh are the two software alternatives. Rather, Petitioner argues that Roseman describes a client software alternative that would work with the Windows operating system and suggests that another client software alternative working with the Macintosh operating system would have been within the level of skill in the art. Pet. 28; Reply 22–23 ("But the Petitioner did not point to Windows and

[7] Patent Owner also argues that a Telnet-based solution for Roseman would not work without graphical user interface (GUI) support. PO Resp. 35. This is inapposite, as Petitioner does not argue that Roseman would have been modified to accommodate a Telnet-based solution.

Macintosh *themselves* as the two client software alternatives, but rather, to versions of the participator software in Roseman adapted to run on those platforms."). Thus, Patent Owner's argument is not persuasive.

Patent Owner further contends that a skilled artisan would not have used two separate software alternatives to implement Roseman's client software with Windows and Macintosh platforms because the skilled artisan would have used Java instead. PO Resp. 36–37. According to Patent Owner, "Java and byte-code are cross-platform solutions that can run on both Windows and Macintosh." *Id.* at 36. Dr. Carbonell testifies that "one of ordinary skill in the art who was motivated to provide software that could work across different platforms and operating systems would have been motivated to utilize a single platform independent software implementation, such as a Java implementation and would not have been motivated to provide additional alternatives to that cross-platform software." Ex. 2005 ¶ 74.

Petitioner argues that the claim language does not exclude platform-specific embodiments and that the '552 patent specifically describes such embodiments as within the scope of the invention. Reply 23–24 (citing Ex. 1001, 4:46–49 ("While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled."). We agree with Petitioner. As noted above, "just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes." *Mouttet*, 686 F.3d at 1334. Thus, even if Java would have been advantageous in some circumstances, we still find that platform-specific client software embodiments would have been an apt extension of Roseman's system.

In light of Roseman's description of client software for the Windows environment and its express teaching that the software for other environments is within the level of skill, Ex. 1003, 12:1–10, we are persuaded that Roseman at least suggests client software for other platforms that were common at the time, such as Macintosh. We credit Dr. Lavian's testimony that providing software for use with both Windows and Macintosh would have made Roseman's system more commercially attractive by increasing the number of users who could use the software. Ex. 1002 ¶ 73. *See also KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one."). Thus, we find that Roseman suggests "wherein the controller computer system is programmed to provide access to the controller computer system via any of two client software alternatives," as recited in claim 2.

c. *"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" and*

*"permitting at least the first user identity and the second user identity to form a group"*

Petitioner contends that Roseman's software running on a local computer, which (as explained above) can be a software implementation for a Windows platform and a Macintosh platform, allows user identities to be recognized by the host computer. Pet. 30–31. Petitioner argues that a group of local computers is formed when a user of a local computer in Roseman drags other participants into a child-room. *Id.* at 32. In another example, Petitioner argues that Roseman's description of creating a virtual conference room, involving identifying the participants of the conference room and requiring invited users to have appropriate keys, teaches permitting at least a first user identity and a second user identity to form a group. *Id.* at 39–40.

We agree with Petitioner. When Roseman's users, via software running on their respective local computers, access conference rooms using keys, Roseman's host computer recognizes the users and allows them to send and receive communications from each other. Ex. 1003, 3:22–56. Thus, we find that Roseman teaches these limitations of claim 2. We note that Patent Owner does not contest that Roseman teaches these limitations.

### *d. "wherein at least some of the communications are received in real time via the Internet network" and*

### *"permitting sending communications in real time, via the Internet network, among the participator computers corresponding to the user identities in the group"*

Petitioner contends that communications in one of Roseman's conference rooms, such as placing documents on a table, drawing on a document, and moving a pointer, take place in real time because they are communicated to participants as the underlying events occur. Pet. 32, 40. For example, Roseman explains:

> 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 [] preceding three events as they occur.

Ex. 1003, 2:38–47. We find that these are specific examples in Roseman of real-time communications sent and received by the participator computers in a group.

As explained in Section II.B.3.a above, Roseman and Vetter teach that such communications can be via an Internet network.

Thus, we find that Roseman and Vetter teach these limitations of claim 2. We note that Patent Owner does not contest that Roseman and Vetter teach these limitations.

*e. "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"*

Petitioner argues that this limitation would have been obvious over Roseman and Lichty. Pet. 34. In particular, Petitioner points to the "Ignore" button of Lichty's user interface. *Id.* Petitioner notes that Roseman already has a feature in which a host computer limits the amount of information another participant can send in a meeting room (a group). *Id.* at 35 (citing Ex. 1003, 12:29–45). Petitioner argues that both Roseman and Lichty state essentially the same reason for their respective features, namely solving the common problem of dealing with potentially unwanted communications from conference participants. *Id.*; *see also* Ex. 1003, 12:29–33; Ex. 1007, 510. Petitioner argues that Lichty's solution would be equally applicable to Roseman. Pet. 35.

Patent Owner, relying on its proposed claim construction, argues that claim 2 requires that the data itself is censored and that this is not shown in Roseman and Lichty. Specifically, Patent Owner argues that "Roseman's procedures are inconsistent with the meaning of censorship" because "Roseman does not disclose restrictions ***based on data*** or other types of content as the claim limitation requires." PO Resp. 38.[8] As explained in Section II.A.3 above, this limitation refers to control of data received by the at least one of the user identities, individually, and is not limited to data suppressed based on the content of those data or by a moderator. Thus, Patent Owner's argument is not persuasive.

As to Lichty, Patent Owner argues that it "does not explain how AOL works either at the user interface level or at the server level." PO Resp. 38. Patent Owner further argues that "Petitioner does not explain how Lichty teaches or discloses censoring whereby a determination as to whether to censor the information is made by the ***controller computer***" and that "Petitioner does not even suggest that Lichty teaches a controller computer." PO Resp. 40. According to Dr. Carbonell, "one would have understood that such ignore features were implemented locally on the user's computer as a filter, i.e. as a user-interface or presentation feature" and that "[o]ne of ordinary skill in the art would not have understood such features to be implemented at the server level." Ex. 2005 ¶ 27. In reply, Petitioner argues that where Lichty implemented the ignore feature is irrelevant because "[t]he Petition cited Lichty only for its disclosure of its censoring feature, and relied on the host in Roseman to carry out the features of the claim." Reply 20.

[8] Patent Owner also argues that "the claim limitation 'determines that the ***message*** is not censored' requires that the message itself is censored" and that "[t]here is no disclosure in either Roseman or Lichty of a system where data (*i.e.*, a message) is censored." PO Resp. 40. This language, however, is not part of any challenged claim. Thus, this argument is not persuasive.

We agree with Petitioner. As we explained in the Institution Decision (at 32), Roseman teaches a scheme in which a host (controller computer) determines whether a user identity should be prevented from sending data. Ex. 1003, 12:29–45. Specifically, Roseman describes a "moderator" feature in which a "host can automatically prevent filibustering, in several ways," including "[b]y plac[ing] a limit on the total time allowed to each person." *Id.* at 12:34–37. We find that this is an example of censoring performed at the controller computer. Petitioner cites Lichty to show that it was known to prevent a user identity from receiving data. Lichty explains why this feature is useful, including "[w]hen rooms become full and everyone is talking, it can be difficult to follow what's going on" and that "Ignore is most useful when the chat of another member becomes disruptive in the chat room." Ex. 1007, 269, 510. This closely tracks Roseman's reason for the moderator feature, namely, preserving free discussion that otherwise would be "defeated by an aggressive person who dominates the conference, and, in effect, maintains a 'filibuster.'" Ex. 1003, 12:29–33.

Patent Owner also argues that the '552 patent distinguishes AOL software. PO Resp. 39–40 (citing Ex. 1001, 1:41–44 ("Chat room communications . . . can involve graphics and certain multimedia capability, as exemplified by such Internet service providers as America On Line."), 1:45–56 ("On the Internet, 'chat room' communications analogous to America On Line have not been developed, at least in part because Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications. Further, unlike the an Internet service provider, which has control over both the hardware platform and the computer program running on the platform to create the 'chat room', there is no particular control over the platform that would be encountered on the Internet. Therefore, development of multiplexing technology for such an environment has been minimal.")). Our focus here is on the disclosure of Lichty, not the '552 patent's characterization of the system disclosed by Lichty. In any case, Petitioner relies on the combination of Lichty and Roseman, rather than Lichty alone, to show censoring a user identity from data. Thus, Patent Owner's argument is not persuasive. *See In re Merck & Co., Inc.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references.").

Patent Owner further argues that "Petitioner fails to address how the disclosure of Lichty's text-based user interface could predictably result in the virtual conferencing system of Roseman where at least one participant is censored from receiving audio data" and that "there is no teaching or suggestion provided by the Lichty reference that motivates any changes to a voice and/or video conferencing system." PO Resp. 41. We are not persuaded by this argument. Roseman teaches censoring senders in meetings that involve text, audio, and graphics. Ex. 1003, 12:26–45. Lichty is cited to show censoring from receiving data. In any case, given the level of skill in the art noted above, we are persuaded that the proposed combination would have been within that level of skill, including applying Lichty's teachings to other forms of data besides text, including audio, video, and pointers.

On the complete record, we find that Roseman and Lichty teach "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," as recited in claim 2.

#### *f. "affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity; affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity"*

As explained above, Roseman describes admitting participants into a conference room when the participants present keys. Ex. 1003, 10:61–65. We find that this teaches "an authenticated first user identity" and "an authenticated second user identity." Additionally, Roseman describes various ways of affording information to local computers of users admitted to the conference room, including as follows:

> 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.

*Id.* at 11:18–26. *See also* Pet. 36–38. As explained in Section II.B.3.a above, Roseman and Vetter teach that such communications can be via an Internet network.

Accordingly, we find that Roseman and Vetter teach these limitations of claim 2. We note that Patent Owner does not contest that Roseman and Vetter teach these limitations.

#### g. *"wherein at least some of the communications include messages comprising more than one data type"*

As noted by Petitioner, Roseman describes various forms of multimedia conferencing, including "multiple parties are linked by both video and audio media," Ex. 1003, Abstract, and "[e]ach 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," *id.* at 8:1–4. Pet. 40–41. On this record, we find that Roseman teaches "wherein at least some of the communications include messages comprising more than one data type." We note that Patent Owner does not contest that Roseman teaches this limitation.

#### h. *"at least some other of the communications include a pointer that produces a pointer-triggered message on demand"*

Petitioner refers to Roseman's description of a user placing a document, represented by an icon, onto a virtual conference table. Pet. 41–42. Petitioner contends that Roseman's icon "serves as a 'pointer' because it points to, or references, the underlying document." *Id.* at 42. According to Petitioner, the icon points to a file and, when the icon is invoked, the host computer causes the file to appear on the table of each participant. *Id.* Petitioner argues that this teaches a pointer that produces a pointer-triggered message on demand. *Id.*

Patent Owner argues that Petitioner "conflates what appears on a GUI and the steps performed by [Roseman's] host computer," that "[t]he icon in Roseman is not a message, it is merely an indication that there is accessible information and clicking on the icon is merely a request to the host computer to send the appropriate data file" and, "[a]ccordingly, the icon itself is not a message, nor a pointer-triggered message." PO Resp. 32. This misstates Petitioner's argument. As explained above, Petitioner contends that Roseman's icon is a pointer, not a pointer-triggered message. The pointer-triggered message is the message that is delivered after a user clicks on the icon.

As explained in Section II.A above, a "pointer" is "a link or reference to a file, data, or service" and a "pointer-triggered message" is "a message, where the content of the message is specified by a pointer and found on demand of the operator of the participator software." Under these constructions, Roseman's icon is a pointer, as it is a link to a file. Likewise, the message retrieved when Roseman's icon is selected is a "pointer-triggered message" because its contents are specified by the icon and are found on demand of a user at a remote computer.

Petitioner further argues that, to the extent that a "pointer" requires an Internet URL or the like, a skilled artisan would have consulted Pike for a teaching of basic Internet concepts, such as URLs. Pet. 42–43. Nevertheless, Patent Owner has not argued, and we do not find, that the claimed "pointer" is required to be a URL. Thus, we need not determine whether a skilled artisan would have sought out Pike's teachings of URLs.

On the complete record, we find that Roseman teaches "at least some other of the communications include a pointer that produces a pointer-triggered message on demand," as recited in claim 2.

In sum, we find that Roseman, Rissanen, Vetter, Pike, and Lichty teach each limitation of claim 2.

### *4. Remaining Challenged Independent Claims*

Petitioner also challenges independent claims 1, 10, 18, 50, 54, 58, 59, and 64. The additional independent claims have significant overlap with claim 2. For example, each of the additional independent claims recites a "database which serves as a repository of tokens," an "Internet network" (or "the Internet"), "two client software alternatives," and "at least one of the user identities, individually, is censored from data," discussed in detail above. Petitioner shows in claim charts where each of the additional independent claims overlaps with claim 2 and provides analysis for the portions of those claims that do not overlap with claim 2. Pet. 46–70. We agree with Petitioner's identification of overlap and find that the overlapping limitations of claims 1, 10, 18, 50, 54, 59, and 64 are taught by Roseman, Rissanen, Vetter, and Lichty for the reasons given for claim 2, above. We agree with Petitioner that claim 10 does not add any limitations not covered by our analysis of claim 2. Pet. 51–52

Petitioner essentially addresses claims 1, 18, 50, 54, 58 together, referring back to claims 1 and 2 for its analysis of claims 18, 50, 54, and 58. Pet. 54–57, 59–66. Claim 1 recites "storing each said user identity and a respective authorization to send multimedia 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." Petitioner argues that Roseman describes using stored keys, associated with user identities, for controlling admission to a particular conference. Pet. 48. Petitioner contends that "[e]ach 'key' [] relates to the identity of the participant and provides the permissions allowing access to the conference room." *Id.* (citing Ex. 1003, 9:34–55). The cited passage, however, only describes a key granting a user admission to a virtual conference room. It does not describe keys as determining what a user can do in a conference room once admitted. Ex. 1003, 9:34–55; *see also id.* at 10:61–65. Although Roseman's keys may be associated with a user identity in that a Level 1 key is given to a person and "may not be passed to any other person and may not be copied," Ex. 1003, 9:43–44, it does not follow that the key provides permissions for behavior within a conference room, such as authorization to send multimedia data.

Petitioner concludes, based on its citations to Roseman, that "Roseman discloses these limitations because a user identity that is not authorized to access a room cannot send multimedia data to conference participants." *Id.* at 49. It is true that a user denied access to a conference room would not be permitted to send multimedia data in that conference room, as Petitioner argues. Pet. 49. Petitioner, however, does not argue persuasively that a key that grants admission also includes an authorization to send multimedia data in that conference room. Roseman's key simply grants access to a conference room. We are not persuaded that such a key constitutes stored authorization to engage in certain activities once admitted to the conference room. Furthermore, Petitioner does not provide persuasive analysis that Roseman checks if the user identity is permitted to send multimedia data before allowing the corresponding participator computer to send such data. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claim 1 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike.

Claim 18 recites

> 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.

As to these limitations, although they differ somewhat from those of claim 1, Petitioner argues that "[t]he analysis for claim 1 as to these limitations accordingly applies to claim 18." As explained above, Petitioner's arguments are not persuasive for claim 1. As to claim 18, Petitioner does not include any additional argument as to why Roseman teaches "the computer system: stores, for a first of the user identities, a respective authorization associated with multimedia data communication." Furthermore, Petitioner does not include any analysis explaining how Roseman teaches "*based* on the respective authorization, cause the multimedia data to be presented" at a participator computer corresponding to a second user identity. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claim 18 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike.

Claim 50 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;

Claims 54 and 58 recite similar limitations. Petitioner does not explain how Roseman teaches associating with a user identity a respective authorization to communicate multimedia data. For example, Petitioner does not explain why simply showing that a user has access to a conference room is enough to show a respective authorization to communicate multimedia data associated with a user identity. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claims 50, 54, and 58 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike.

Claim 59 recites "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." Similarly, claim 64 recites "groups in which members distribute, via predefined rules, the messages in real time to the respective ones of the participator computers."

Petitioner (Pet. 65) argues that Roseman discloses that a person setting up a conference can determine aspects of the meeting, such as: "What rules govern the conduct of the meeting? Does the Requester have absolute control of the voice and message interaction among the participants? Or Is the meeting a brainstorming free-for-all, where numerous people can speak at once?" Ex. 1003, 3:52–54. As to a specific example, Petitioner points to Roseman's "pencil" tool, through which a participant can write a message in a conference room using the pencil tool, and other participants are disabled from doing so while the first participant has the pencil. Pet. 66 (citing Ex. 1003, Fig. 19). Petitioner also cites to Roseman's "Whisper Mode" for private voice conversations and "note-passing" for private textual conversations as examples of predefined rules that govern how users conduct real-time communications. *Id.* at 66–67 (citing Ex. 1003, 9:16–31, 15:12–15, Fig. 17C). We agree with Petitioner that these are examples of groups in which members distribute, in accordance with predefined rules, the user messages in real time. We find that Roseman teaches these limitations of claims 59 and 64. We note that Patent Owner does not present separate arguments for claims 59 and 64.

### 5. *Challenged Dependent Claims*

Claims 19–49 depend, directly or indirectly, from claim 18. Claims 51–53 depend, directly or indirectly, from claim 50. Claims 55–57 depend from claim 54. As explained above, Petitioner has not shown that claims 18, 50, and 54 would have been obvious. Petitioner's analysis of these dependent claims does not cure the deficiencies noted above for claims 18, 50, and 54. Accordingly, Petitioner has not shown, by a preponderance of the evidence, that claims 19–49, 51–53, and 55–57 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike.

Claims 3, 5, and 7 depend from claim 2 and add "wherein at least one of the messages includes data representing" sound, video, and both sound and video, respectively. Claims 11, 13, and 15 depend from claim 10 and recite "wherein at least one of the messages includes data representing" sound, video, and both sound and video, respectively. Petitioner has persuasively shown that the communications in Roseman's meetings can include sound, video, graphic, and multimedia. Pet. 71–72 (citing Ex. 1003, 1:42–46 (drawings), 3:40–41 (graphics), 7:35–38 (pictures of participants), 8:1–4 (graphics), 11:11–16 (audio and video), 12:34–45 (audio)). We find that Roseman teaches the additional limitations of claims 3, 5, 7, 11, 13, and 15.

Claims 4, 6, 8, and 9 depend, directly or indirectly, from claim 2 and 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." These limitations are substantially similar to those we found missing from claim 1, discussed above. Petitioner incorporates its analysis of claim 1 for this limitation.[9] For the reasons given for claim 1, Petitioner has not shown, by a preponderance of the evidence, that claims 4, 6, 8, and 9 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike.

Each of claims 12, 14, 16, and 17 depends indirectly from claim 10 and adds "the computer system is further programmed to provide access to a member-associated image." As Petitioner points out (Pet. 73), Roseman describes that "[a] small picture of each user is displayed in a meeting room to indicate presence." Ex. 1003, 11:11–14. We find that these are examples of member-associated images. Thus, we find that Roseman teaches the additional limitation of claims 12, 14, 16, and 17.

As to the challenged dependent claims, Patent Owner refers to its arguments for claim 2. PO Resp. 42. We note that Patent Owner does not present separate arguments for the challenged dependent claims.

[9] Petitioner cites to claim 10, but we read this as a typographical error. Claim 1, not claim 10, includes a recitation similar to that of claims 4, 6, 8, and 9.

### *6. Conclusion of Obviousness*

As explained above, Roseman, Rissanen, Vetter, and Lichty teach each limitation of claims 2, 3, 5, 7, 10–17, 59, and 64. Petitioner has introduced persuasive evidence that a skilled artisan would have had reasons to combine the teachings of Roseman, Rissanen, Vetter, and Lichty. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. In sum, upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence, that claims 2, 3, 5, 7, 10–17, 59, and 64 would have been obvious over Roseman, Rissanen, Vetter, and Lichty.

## III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner filed a paper styled "Motion to Exclude Evidence," seeking to exclude certain portions of the 2nd Lavian Declaration that it argues exceeds the proper scope of a reply. Paper 37, 1. Specifically, Patent Owner moves to exclude portions of paragraphs 54, 74, and 75 of the 2nd Lavian Declaration. *Id.* at 2–5.

Petitioner opposes this motion on the ground that it is not directed to the admissibility of evidence and, therefore, is procedurally improper. Paper 39, 2. Patent Owner contends that arguments that exceed the scope of a reply are irrelevant, prejudicial, confusing, or misleading under Federal Rules of Evidence 401, 402, and 403. Paper 41, 1–2. As Petitioner points out, however, the Board repeatedly has denied, as improper, motions to exclude that merely argue that evidence is outside the proper scope of a reply. Paper 39, 2–3. Despite its invocation of Rules 401, 402, and 403, we agree that Patent Owner's Motion to Exclude is nothing more than an argument that Petitioner's Reply exceeds its proper scope. Accordingly, we deny Patent Owner's Motion.

Nevertheless, we have considered Patent Owner's argument with respect to those portions of Petitioner's Reply that are relied upon in this decision, and determine they do not belatedly raise new issues or present evidence that should have been presented in the Petition. In any case, we do not rely on paragraphs 54, 74, and 75 of the 2nd Lavian Declaration.

## III. CONCLUSION

Petitioner has proved by a preponderance of the evidence that claims 2, 3, 5, 7, 10–17, 59, and 64 are unpatentable, but has not proved claims 1, 4, 6, 8, 9, and 18–58 are unpatentable.

## IV. ORDER

For the reasons given, it is:

ORDERED, based on a preponderance of the evidence, that claims 2, 3, 5, 7, 10–17, 59, and 64 are unpatentable; and

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

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

PATENT OWNER:

Peter Lambrianakos
plambrianakos@brownrudnick.com

Vincent Rubino
vrubino@brownrudnick.com

Trials@uspto.gov
571-272-7822

Paper No. 52
Entered: December 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FACEBOOK, INC.,
Petitioner,

v.

WINDY CITY INNOVATIONS, LLC,
Patent Owner.

Case IPR2016-01159[1]
Patent 8,694,657 B1

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

MCKONE, *Administrative Patent Judge*.

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

[1] Case No. IPR2017-00659 has been joined with this proceeding.

## I. INTRODUCTION

### *A. Background*

Facebook, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") to institute an *inter partes* review of claims 189, 334, 342, 348, 465, 580, 584, and 592 of U.S. Patent No. 8,694,657 B1 (Ex. 1001, "the '657 patent"). Windy City Innovations, LLC ("Patent Owner") filed a Preliminary Response (Paper 6, "Prelim. Resp.").

Pursuant to 35 U.S.C. § 314, in our Institution Decision (Paper 7, "Dec."), we instituted this proceeding as to claims 189, 334, 342, 348, 465, 580, 584, and 592.

Patent Owner filed a Patent Owner's Response (Paper 22, "PO Resp."), and Petitioner filed a Reply to the Patent Owner's Response (Paper 31, "Reply").

Petitioner relies on the Declarations of Tal Lavian, Ph.D. (Ex. 1002, "Lavian Decl."; Ex. 1021, "2nd Lavian Decl."). Patent Owner relies on the Declaration of Jaime G. Carbonell, Ph.D. (Ex. 2005, "Carbonell Decl.").

On January 12, 2017, Petitioner filed a petition seeking *inter partes* review of claims 203, 209, 215, 221, 477, 482, 487, and 492 of the '657 patent and sought to join that proceeding to this proceeding. IPR2017-00659, Paper 2 ("the '659 Pet."), Paper 3 (Mot. for Joinder). We instituted a trial in that proceeding for all challenged claims and joined it to this proceeding. Paper 34 (the "'659 Dec."). Petitioner relies on the Declaration of Dr. Lavian in the '659 proceeding (IPR2017-00659, Ex. 1002 ("Lavian '659 Decl.")).

As to the additional claims challenged in the '659 Petition, Patent Owner filed a Supplemental Patent Owner's Response (Paper 45, "Supp. PO

Resp.") and Petitioner filed a Supplemental Reply (Paper 46, "Supp. Reply").

An oral argument was held on October 19, 2017 (Paper 51, "Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a final written decision under 35 U.S.C. § 318(a) as to the patentability of claims 189, 203, 209, 215, 221, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592. Based on the record before us, Petitioner has proved, by a preponderance of the evidence, that claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 are unpatentable, but has not proved that claims 203, 209, 215, and 221 are unpatentable.

### *B. Related Matters*

The parties indicate that the '657 patent has been asserted in *Windy City Innovations, LLC v. Microsoft Corp.*, Civ. A. No. 15-cv-00103-GM (W.D.N.C.) (transferred to 16-cv-1729 (N.D. Cal.)), and *Windy City Innovations, LLC v. Facebook, Inc.*, Civ. A. No. 15-cv-00102-GM (W.D.N.C.) (transferred to 16-cv-1730 (N.D. Cal.)). Pet. 1; Paper 4, 1. The '657 patent is the subject of an *inter partes* review petition in IPR2016-01155. Paper 4, 1. IPR2017-00622, also challenging the '657 patent, has been joined to IPR2016-01155. The '657 patent also was the subject of IPR2017-00606 and IPR2017-00656, which Microsoft Corp. filed and sought to join with IPR2016-01155 and this proceeding, respectively, prior to settling with Patent Owner. Patents related to the '657 patent are subjects of additional *inter partes* review petitions.

### *C. Asserted Prior Art References*

Petitioner relies on the following prior art:

U.S. Patent No. 6,608,636 B1, issued Aug. 19, 2003, filed May 13, 1992 (Ex. 1003, "Roseman");

Published European Pat. App. No. 0 621 532 A1, published Oct. 26, 1994 (Ex. 1004, "Rissanen");

Ronald J. Vetter, *Videoconferencing on the Internet*, IEEE COMPUTER SOCIETY 77–79 (Jan. 1995) (Ex. 1005, "Vetter");

MARY ANN PIKE ET AL., USING MOSAIC (1994) (Ex. 1006, "Pike"); and

TOM LICHTY, THE OFFICIAL AMERICA ONLINE FOR MACINTOSH MEMBERSHIP KIT & TOUR GUIDE (2nd ed. 1994) (Ex. 1007, "Lichty").

### *D. The Instituted Ground*

We instituted a trial on the ground of unpatentability of claims 189, 203, 209, 215, 221, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 as obvious, under 35 U.S.C. § 103(a), over Roseman, Rissanen, Vetter, Pike, and Lichty. Dec. 36; '659 Dec. 15.

### *E. The '657 Patent*

The '657 patent describes an Internet "chat room." According to the '657 patent, it was known to link computers together to form chat rooms in which users communicated by text, graphics, and multimedia, giving the example of "America On Line." Ex. 1001, 1:33–37. The '657 patent acknowledges that chat rooms have been implemented on the Internet, albeit with "limited chat capability," but contends that the complex chat room communications capable with Internet service providers had not been developed on the Internet because "[t]he Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications" and because "there is no particular control over the platform that would be encountered on the Internet." *Id.* at 1:38–44, 1:50–52.

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

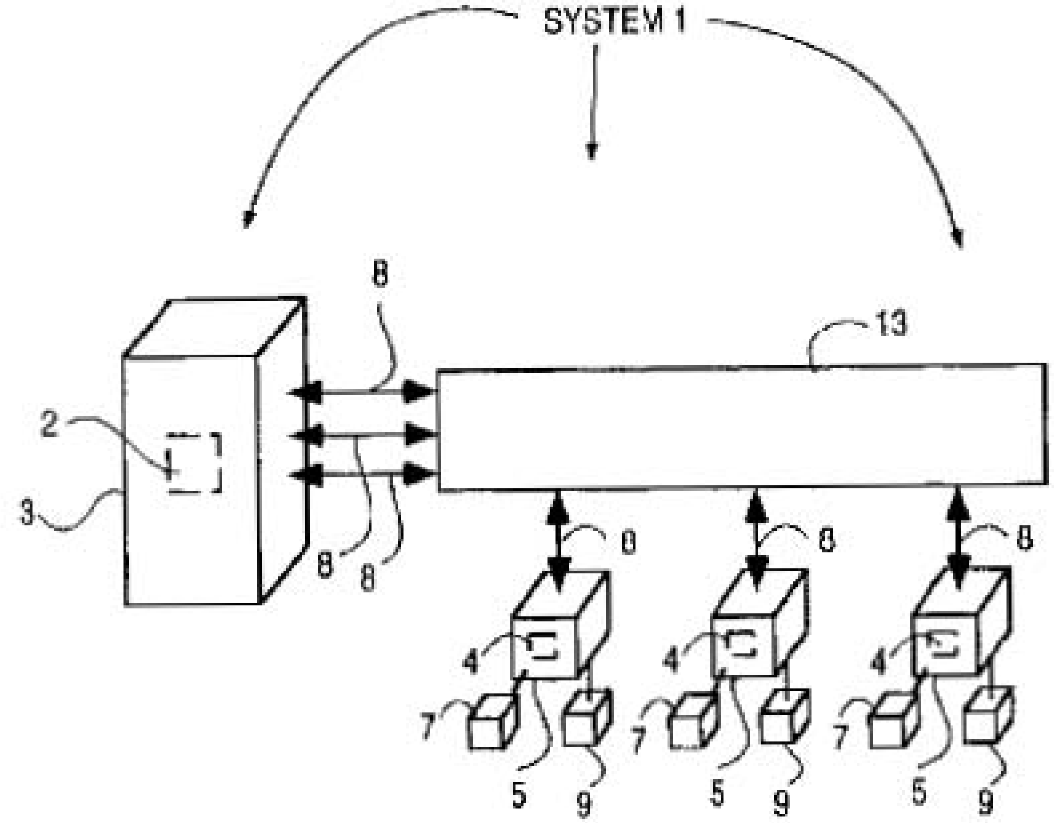


Figure 1 is a block diagram showing the components and data flow of a computerized human communication arbitrating and distributing system.

*Id.* at 4:36–40. The system includes controller computer 3 in communication with several participator computers 5 (e.g., IBM-compatible personal computers) over connection 13 (e.g., an Internet connection or a World Wide Web connection). *Id.* at 4:41–60.

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

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

> Censorship, which broadly encompasses control of what is said in a group, is also arbitrated by means of the tokens. Censorship can control of access [sic] to system 1 by identity of the user, which is associated with the user's tokens. By checking the tokens, a user's access can be controlled per group, as well as in giving group priority, moderation privileges, etc.
>
> Censorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject.

*Id.* at 8:11–19.

According to the specification, "[t]he present invention comprehends communicating all electrically communicable multimedia information as

Message 8, by such means as pointers, for example, URLs. URLs can point to pre-stored audio and video communications, which the Controller Computer 3 can fetch and communicate to the Participator Computers 5." *Id.* at 5:11–16.

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

> 189. A method of communicating via an Internet network by using a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method including:
>
> affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity;
>
> affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity; and
>
> determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications; and
>
> determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities; and
>
> if the user identities are able to form the group, forming the group and facilitating sending the communications that are not censored from the first participator computer to the second participator

computer, wherein the sending is in real time and via the Internet network, and wherein, for the communications which are received and which present an Internet URL, facilitating handling the Internet URL via the computer system so as to find content specified by the Internet URL and presenting the content at an output device of the second participator computer, and

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

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

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

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

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

> if the user identities are determined to be able to form the group, forms the group and facilitates sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer; and
>
> if the first user identity is censored from sending the data, does not facilitate sending the data that is censored from the first participator computer to the second participator computer.

## II. ANALYSIS

### *A. Claim Construction*

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

### *1. Constructions in the Institution Decision*

In the Institution Decision, we preliminarily construed the following terms (Dec. 7–13):

| **Claim Term** | **Preliminary Construction** |
|---|---|
| "token" | "piece of information associated with user identity" |
| "database" | "a collection of logically related data" |
| "censor" | "control what is said in a group" |
| "the first user identity is individually censored from sending data" | refers to control of data sent by the at least one of the user identities, individually, and is not limited to data suppressed based on the content of those data or by a moderator |

Patent Owner adopts our construction of "token" (which Petitioner initially proposed) PO Resp. 7–8, and challenges our construction of "database," *id.* at 8–12. Petitioner accepts our construction of "database" and presents arguments in favor of it. Reply 3–7. The parties do not address further our constructions of "censor" and "the first user identity is individually censored from sending data." We maintain our constructions of "token," "censor," and "the first user identity is individually censored from sending data" on the complete record. We address the construction of "database," below.[2]

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

### *2. "database"*

In the Petition, relying on Dr. Lavian's testimony, Petitioner argues that "[a] person of ordinary skill in the art would have understood the claimed 'database' to simply refer to a stored collection of tokens. The '657 patent does not require that the database be any particular type, such as relational." Pet. 18 (citing Ex. 1002 ¶ 50). Dr. Lavian, in turn, relies on the specification's description of tokens being "stored in memory in a control computer database, along with personal information about the user, such as the user's age." Ex. 1002 ¶ 50 (citing Ex. 1001, 7:52–54).

Patent Owner urges a construction that is narrower in two regards: (1) Patent Owner contends that a database is a collection of logically-related data "which is stored with persistence"; and (2) Patent Owner contends that a database includes "associated tools for interacting with the data such as a DBMS." PO Resp. 12.

Patent Owner's primary argument in favor of construing "database" to require these limitations is that it filed, in a related application before the Patent Office, an information disclosure statement (IDS) that supports its construction. *Id.* at 9–10 (citing Ex. 2008). The IDS was submitted to the Patent Office in pending application 14/246,965 on January 1, 2017, after Petitioner filed the Petition and shortly after we instituted this proceeding and preliminarily rejected Patent Owner's claim construction arguments. In the IDS, Patent Owner argued, *inter alia*, that "attention is respectfully drawn to the defendants' contentions[3] of invalidity in view of the database

[3] This appears to be a reference to invalidity contentions filed in a related district court proceeding.

and 'other programs' limitations that are common to all claims" and that "[b]ecause the database affords information to other programs and computers, it must store the data, such as the tokens, with persistence, such that tools can interact with the data such as a DBMS when providing the data to the participator computers of the authenticated users." Ex. 2008, 2. Patent Owner argues that we must accept its construction pursuant to *Verizon Services Corp. v. Vonage Holdings Corp.*, 503 F.3d 1295, 1306 (Fed. Cir. 2007), which held that, in some circumstances, a statement made by a patentee in the prosecution history of a related application can operate as a disclaimer, even if the disclaimer occurred after the patent-in-suit had issued. PO Resp. 9–10.

Although we doubt that the Federal Circuit intended that an IDS in a related application should be a vehicle for overturning a disadvantageous claim construction in an adversarial proceeding,[4] we need not reach that issue. As the Federal Circuit also held, "[t]o operate as a disclaimer, the statement in the prosecution history must be clear and unambiguous, and constitute a clear disavowal of claim scope." *Verizon*, 503 F.3d at 1306. That is not the case here. The statements in Patent Owner's IDS are not in response to any rejection by the Examiner, do not accompany any amendments, and are not directed to any particular claims, other than a general statement that the statements apply to "all claims."[5] Ex. 2008, 2.

Although Patent Owner argues that the IDS "supports the construction that a database is limited" in the manner that it argues, Patent Owner does

[4] *See Moleculon Research Corp. v. CBS, Inc.*, 793 F.2d 1261, 1270 (Fed. Cir. 1986) ("A citation may be made at 'any time' either during prosecution or, as here, after the patent has issued. If made during prosecution, it is clear that the statements may be considered for claim interpretation purposes, just as any other document submitted during prosecution. If submitted after issuance, the answer, again, is it may be considered. To say that it *may* be considered is not to say what *weight* statements in the Citation are to be accorded. For example, a Citation filed during litigation might very well contain merely self-serving statements which likely would be accorded no more weight than testimony of an interested witness or argument of counsel. Issues of evidentiary weight are resolved on the circumstances of each case."); *Phillips*, 415 F.3d at 1317 ("Like the specification, *the prosecution history provides evidence of how <u>the PTO and the inventor</u> understood the patent*. . . . Yet because the prosecution history represents an ongoing negotiation between the PTO and the applicant, rather than the final product of that negotiation, it often lacks the clarity of the specification and thus is less useful for claim construction purposes." (emphasis added)).

[5] Adding to the ambiguity, it is not clear whether the IDS's reference to "all claims" refers to the claims in the pending application or the claims discussed in the defendants' contentions of invalidity to which the sentence is directed.

not contend that the IDS constitutes a disclaimer of any subject matter. PO Resp. 9. We find that the IDS does not contain a "'clear and unmistakable' disclaimer that would have been evident to one skilled in the art." *Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1064 (Fed. Cir. 2016). Therefore, we are not persuaded that we should apply prosecution history disclaimer to limit the scope of the term "database."

Patent Owner also cites to the testimony of Dr. Carbonell that "[t]wo hallmarks of a database are (1) persistence of the data, and (2) interactivity with the data via a database management system (DBMS)." *Id.* at 10 (quoting Ex. 2005 ¶ 33). As Petitioner points out (Reply 1–2), Dr. Carbonell's testimony on this point appears to be a copy of the testimony of Dr. Bajaj, who submitted a declaration in support of Patent Owner's Preliminary Response (*compare* Ex. 2005 ¶ 33, *with* Ex. 2001 ¶ 20), although Dr. Carbonell testified that he was unaware of Dr. Bajaj's declaration (Ex. 1016, 132:2–12). In any case, as Petitioner points out, Dr. Carbonell marshals the same evidence that did not persuade us at the institution stage without adding any additional evidence or even acknowledging our concerns with Dr. Bajaj's evidence. Reply 2 n.1.

In particular, Patent Owner and Dr. Carbonell cite to the Macmillan Encyclopedia of Computers (Ex. 2004). PO Resp. 10–11; Carbonell Decl. ¶ 33. In the portion included in Exhibit 2004, The Macmillan Encyclopedia states that "[a] database system is a collection of related records stored in a manner that makes the storage and retrieval of the data very efficient. The four well-known data models for databases are the hierarchical, network, relational, and object-oriented models." Ex. 2004, 230. This definition does not require persistence and Patent Owner does not explain why persistence should be inferred from this definition. Moreover, as we observed in the Institution Decision, the Macmillan definition is consistent with the definition of "database" given by the IEEE Dictionary of Standards Terms. *See* IEEE 100 THE AUTHORITATIVE DICTIONARY OF IEEE STANDARDS TERMS 268 (7th ed. 2000) ("**database (DB)** . . . A collection of logically related data stored together in one or more computerized files.") (Ex. 3001). This definition also does not require persistence. Although this dictionary was published several years after the filing date of the '657 patent, Dr. Lavian testifies that the plain and ordinary meaning of "database" did not change during this time. Ex. 1021 ¶ 11. In support of this testimony, Dr. Lavian cites to a 1991 textbook, which defines "database" as "a collection of interrelated data," yet another definition that does not require "persistence." *See* Ex. 1017, 5. Moreover, we observe that Patent Owner provides no boundaries for "stored with persistence" to meaningfully limit the term. For example, all data accessed and stored by a program while the program is executing has some level of "persistence."

As to a DBMS, Macmillan explains:

> A database management system (DBMS) is a software package. Its main functions are (1) to provide the facility to set up the database, (2) to retrieve and store source data (actual data in the database), (3) to retrieve and store the data about the structure of the database (data dictionary), (4) to provide the facilities to enforce security rules, (5) to back up the database, and (6) to control the concurrent transactions so that one user's environment is protected from others.

Ex. 2004, 231. Patent Owner characterizes the DBMS as "another criteria of a database" that provides interactive querying capability not present in "[s]tandard storage" in temporary or permanent memory. PO Resp. 10–11.

Dr. Carbonell repeats Patent Owner's arguments without citation to evidence and in testimony that largely copies that of Dr. Bajaj. Ex. 2005 ¶¶ 33–36; *see also* Ex. 2001 ¶¶ 20–23. Nevertheless, we read Macmillan to describe a DBMS as software that works with a database, rather than a part of a database or a component that necessarily accompanies a database. Dr. Carbonell's testimony, which does not identify its bases, adds little to Macmillan. *See* 37 C.F.R. § 42.65(a) ("Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.").

Patent Owner also argues that the disclosure of the '657 patent imposes "persistence" and DBMS limitations on the claimed database because it describes the database as storing security information such as tokens for other programs to access. PO Resp. 12. Patent Owner does not provide a citation to the '657 patent in support of its argument. Nevertheless, Patent Owner argues, again without citation, that "[o]ne of ordinary skill in the art would have expected that this type of security feature would persist in a location other than in program memory so that other user programs could access the information." *Id.* Finally, Patent Owner argues that the '657 patent describes tokens stored in hierarchies, which, according to Patent Owner, "are typical of database storage organization, and natural schema when storing and managing access to diverse information." *Id.* None of these arguments supports reading persistence or a DBMS into the term "database." We note also that the other claim language, "serves as a repository of tokens for other programs to access," is a requirement we evaluate separately and do not read into the term "database."

As noted in the Institution Decision (at 10), the specification describes a database consistently with the Macmillan and IEEE definitions, explaining that tokens are "pieces of information associated with user identity," that tokens are "stored in memory in a control computer database, along with personal information about the user," and that "[i]n the database, the storage of tokens can be by user, group, and content." Ex. 1001, 7:52–58. The specification does not require a DBMS (or similar software) or impose a persistence requirement.

On the complete record, we maintain our construction of database, namely, "a collection of logically related data." This is the construction most consistent with both the intrinsic evidence and dictionary definitions. However, we note that Petitioner contends, and we find, that the prior art shows a database with persistence and associated tools for interacting with the stored data, as explained below.

### *B. Asserted Grounds of Unpatentability*

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

In an obviousness analysis, some reason must be shown as to why a person of ordinary skill would have combined or modified the prior art to achieve the patented invention. *See Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008). A reason to combine or modify the prior art may be found explicitly or implicitly in market forces; design incentives; the "interrelated teachings of multiple patents"; "any need or problem known in the field of endeavor at the time of invention and addressed by the patent"; and the background knowledge, creativity, and common sense of the person of ordinary skill. *Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1328–29 (Fed. Cir. 2009) (quoting *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418–21 (2007)).

### *1. Level of Ordinary Skill*

Neither party proposes a level of ordinary skill in the art. Nevertheless, both parties' experts testify to similar levels of skill. Specifically, Dr. Lavian testifies that a skilled artisan "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." Ex. 1002 ¶ 13. For his part, Dr. Carbonell testifies that a skilled artisan "would have had a bachelor's degree in

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

computer science (or a related field) and at least one year of work experience in programming in computer communication methods" and notes that his "opinions herein would not change even if the person having ordinary skill in the art were to be found to have the level of skill proposed by Dr. Lavian." Ex. 2005 ¶ 18. We adopt Dr. Lavian's proposal, as it is consistent with the level of skill reflected in the prior art of record. Nevertheless, we discern no material difference between his proposal and that of Dr. Carbonell. Thus, our findings and conclusions would be the same under either proposal.

### *2. Scope and Content of the Prior Art*

Petitioner contends that the challenged claims would have been obvious over Roseman, alone or in combination with Rissanen, Vetter, Pike, and Lichty. Pet. 5–6; '659 Pet. 9–10.

#### *a. Overview of Roseman*

Roseman describes a system for multimedia conferencing, in which parties are linked by both video and audio media. Ex. 1003, Abstract. In Roseman, a conference is represented visually as a common virtual conference table, in which each participant can place a document onto the table electronically, manipulate and write on the document, write on a virtual notepad, and move a pointer to draw other users' attention. *Id.* at 2:38–45, 7:55–8:37. Participants can see the events as they occur. *Id.* at 2:46–47. Figure 9, reproduced below, illustrates an example conference room:

FIG. 9

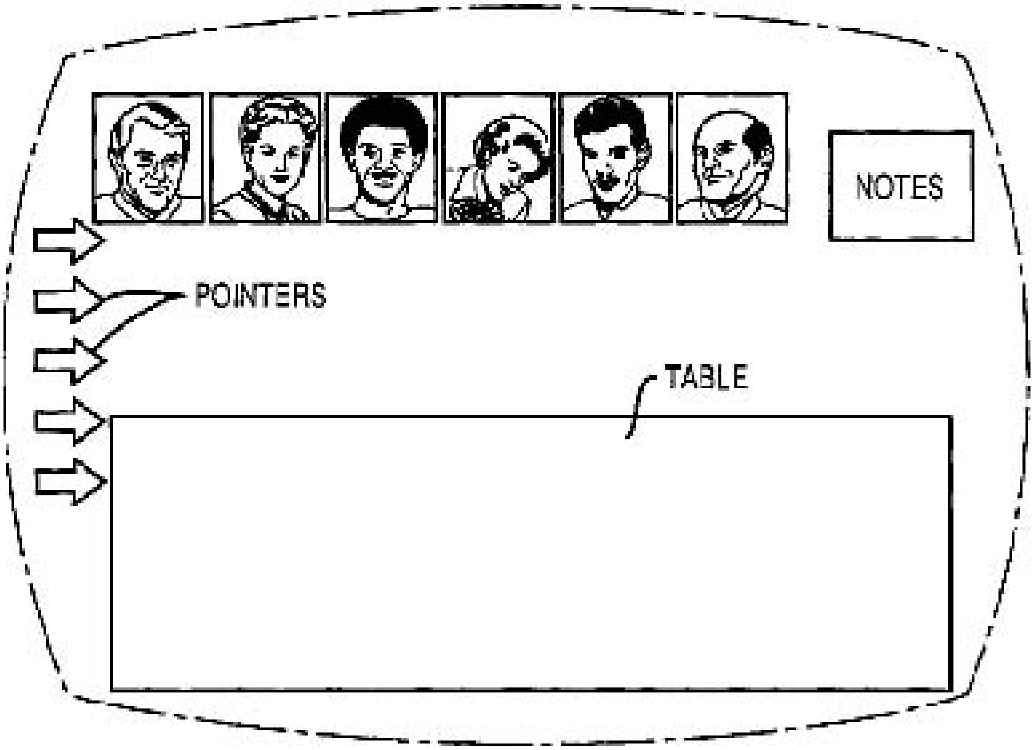


Figure 9 is a picture of a video screen that is generated by a host computer and distributed to all participants in a conference. *Id.* at 2:16–18.

The parties operate their own local computers (which include video cameras and speaker-type telephones) and, when a conference is established, connect to a host computer via commercially available local area networks ("LANs") and wide area networks ("WANs"). *Id.* at 1:34–41. In the conference, the host computer generates a common video screen (e.g., Figure 9, reproduced above) displayed at each of the local computers, and the parties send information, such as drawings, to be displayed on the common screen. *Id.* at 1:42–46. The telephones and video cameras allow the parties to see and speak with each other. *Id.* at 1:47–49.

Roseman includes a pseudo code appendix that details how its features are implemented. *Id.* at 12:66–13:2. According to the pseudo code, a participant interacts with the conference table, for example, by dragging an icon onto the table, which causes a data file to be transmitted to the host. *Id.* at 14:53–55. The host then transmits the icon to the table of each participant. *Id.* at 14:56–57. If another participant activates the icon, the host sends the open file to the tables of all participants. *Id.* at 14:58–61. If the participant drags the icon from the table to his own screen and activates the icon on his screen, the data file is presented to the participant. *Id.* at 14:62–66.

Roseman describes additional features, such as a party's ability to "whisper" to another party without being heard by others in the conference room, and the ability to "pass notes" by dragging a note to the picture of another party, while the other parties are unaware of the note. *Id.* at 9:16–31. Each room may also have "doors" to committee rooms or child-rooms. A child-room is created in the same way as a parent room and is dependent upon the parent room for access and existence. *Id.* at 10:18–23.

A meeting requester creates a conference by selecting the participants, the attributes of the virtual conference room (e.g., virtual equipment and room décor), and the rules of the conference (e.g., whether the requester has absolute control over voice and message interaction of the parties). *Id.* at 3:22–56. According to Roseman, "[t]he conference room itself is actually a combination of stored data and computer programs," the stored data can include conference proceedings, and "both the conference room and the proceedings of the conference have persistence in time." *Id.* at 12:16–25.

The meeting requester specifies a level for each invitation and compiles an invitation list. *Id.* at 9:34–36. Invitations include "keys" specifying the level, e.g., whether the invitation is for the invitee only or can be passed to a delegate or to anyone. *Id.* at 9:35–48. For example, "Level 1 keys may not be passed to any other person and may not be copied" while "Level 2 keys may be passed to exactly one other person and may not be copied." *Id.* at 9:42–45. According to Roseman, "[t]he meeting room 'knows' about each key and its invitation level. Persons with improper keys are not admitted to the room." *Id.* at 9:49–51. A key is distributed electronically as an object attached to the invitation. *Id.* at 9:54–55. To attend a meeting, a party walks a virtual "hallway" to the meeting room and opens the meeting room door by dropping the key onto a virtual "door lock." *Id.* at 10:30–32, 10:61–65. Moreover, the host "can automatically prevent filibustering" by "monitor[ing] the speech of each person, and plac[ing] a limit on the total time allowed to each person." *Id.* at 12:29–38.

### *b. Overview of Rissanen*

Rissanen describes a system and method for validation of spoken passwords. Ex. 1004, 2:17–21. Rissanen's Background of the Invention discusses systems in which "business computer systems are arranged to initially record and store passwords assigned to users," a user is prompted for entry of a password, 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." *Id.* at 1:21–28. In Rissanen's proposed solution, "[u]sers 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." *Id.* at 2:26–29.

Petitioner makes clear that "[a]lthough Rissanen also describes using spoken voice passwords, this Petition cites it for its more pedestrian teachings relating to database storage of passwords of any form." Pet. 11.

#### *c. Overview of Vetter*

Vetter is an IEEE Computer Society Magazine article discussing available tools for conducting teleconferencing over the Internet. According to Vetter, "[v]ideoconferences are becoming increasingly frequent on the Internet and are generating much research interest." Ex. 1005, 77. Vetter states that "the emerging multicast backbone (or MBone) can efficiently send traffic from a single source over the network to multiple recipients," and, "[a]t 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." *Id.* Vetter concludes that "[t]he 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." *Id.*

Vetter also describes challenges that faced implementation of audio, graphic, and video tools on the Internet, including "disturbing feedback when the microphones at multiple sites were left 'open' during a discussion," taking too much time to broadcast a simple graphic image to multiple participants when using "Whiteboard tools" (collaborative software tools that support a shared desktop whiteboard among a group of distributed users on the Internet), and use of video during a classroom presentation that

caused the workstations in the classroom lab to lock up. *Id.* at 78–79. Vetter also notes that the physical distance between two points on the Internet can be different from the electronic distance between those points. *Id.* at 79.

Vetter discusses in particular a CU-SeeMe platform from Cornell University that supported video and audio conferencing over the Internet, and a CU-SeeMe Reflector that allowed multiparty conferencing with CU-SeeMe. *Id.* at 78.

### *d. Overview of Pike*

Pike is a reference and guide book for using the Web browser Mosaic. Ex. 1006, 2. Petitioner cites to Pike's discussion of URLs and hyperlinks. According to Pike, URLs were developed as a standard way of referencing items on the World Wide Web. *Id.* at 38. "A *URL* is a complete description of an item, containing the location of the item that you want to retrieve. 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.*

### *e. Overview of Lichty*

Lichty is a book intended as a "tour guide" of America Online ("AOL"), an online email service, Internet gateway, and community. Ex. 1007, 1–3. Petitioner (Pet. 34) focuses on Lichty's description of AOL's real-time interactive "People Connection" feature. Ex. 1007, 251–78. People Connection includes chat rooms in which a user communicates with others by posting text messages to the other participants in a chat room. *Id.* at 252–55. Lichty describes, in particular, that a People Connection interface includes an "Ignore" button. *Id.* at 268–69. According to Lichty, "[i]f you wish to exclude a member's comments (or those of all the members in a 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." *Id.* at 269; *see also id.* at 510 (glossary definition of "Ignore—(1) Chat blinders; a way of blocking a member's chat from your view in a chat/conference room window. Ignore is most useful when the chat of another member becomes disruptive in the chat room.").

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

Petitioner contends that Roseman teaches each limitation of claim 189, but cites the remaining references for the following, should we determine that Roseman lacks such a teaching:

Rissanen for a teaching that tokens could have been stored in a database;

Vetter for a teaching that Roseman's communications could have been over the Internet;

Pike for a teaching of URLs; and

Lichty for a teaching of content filtering, in particular an "ignore" feature, which Petitioner equates to "censoring."

Pet. 6; '659 Pet. 9–10.

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

Petitioner contends that Roseman's host computer is a controller computer. Pet. 15. Petitioner identifies Roseman's local computers as independent participator computers and argues that Roseman's various ways of communicating information (placing documents on a virtual table, shared notes, whisper conversations) are examples of affording information to those participator computers. Pet. 14–15, 23–24. As detailed above, Roseman describes a system in which individual computers are connected to a central host computer via a combination of LANs and WANs. Ex. 1003, 3:14–19. According to Roseman, "[t]he 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." *Id.* at 1:50–52. We find that Roseman's host computer is a "controller computer," that Roseman's local computers are "participator computers," and that Roseman's various ways of communicating information from the host to the local computers are examples of "affording information to each of a plurality of participator computers which are otherwise independent of each other," as recited in claim 189.[7]

[7] Patent Owner argues that "Petitioner does not address the issue that the **database** affords information to each of a plurality of computers." PO Resp. 20. Claim 189, however, does not recite that the database affords information to the plurality of computers.

The parties dispute whether Roseman describes "a database which serves as a repository of tokens for other programs to access." First, Petitioner contends that Roseman's "keys" are tokens. Pet. 15–16. As explained above, the parties agree that a "token" is "a piece of information associated with user identity." As also explained above, Roseman describes that an invitor, in setting up a meeting, creates an invitation that includes a key that conforms to an invitation level. Ex. 1003, 9:34–48. A key "is an electronic object attached to the invitation." *Id.* at 9:54–55. The "level" of a key determines who can use it. For example, "Level 1 keys may not be passed to any other person and may not be copied." *Id.* at 9:42–44. According to Roseman, "[t]o 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." *Id.* at 10:61–64. Petitioner argues that this evidence shows that Roseman's keys are "pieces of information associated with a user identity," and thus, are "tokens." Pet. 17.

Patent Owner argues that Roseman's keys are not tokens because they are associated only with conference rooms, rather than user identities. PO Resp. 18. Patent Owner points to Roseman's Figure 8, which shows a key associated with "CONFERENCE ROOM 17L (DATE, TIME)." *Id.* In describing Figure 8, however, Roseman explains "the key is, essentially, a block of data, or a code," that can be used if the Invitee may send a delegate, to give the Absentee-Invitee a "key," which enables access to the meeting. Ex. 1003, 6:54–61. "The Requester can leave the key in his local computer, in the form of an icon residing on the display, as shown in FIG. 8. Anyone entering the office can use the key." Ex. 1003, 6:60–63. In this example, the key can be used only with a particular user's computer. Figure 8 also shows the "key" icon contained within a "vault" icon. *Id.* at 6:64–65. In this example,

> a user must use a "combination" to the "vault" to obtain the "key." In this latter example, the [] "combination" (ie, a pass-code) is obtained from the Absentee-Invitee in some appropriate way. At conference time, the Delegate opens the "vault," obtains the "key," and enters the conference room, by using the key.

*Id.* at 6:65–7:3. Patent Owner argues that Roseman's keys are "transferable to anyone—like a key to a door lock." PO Resp. 18. Patent Owner contends that Roseman teaches away from keys being associated with a specific user through its description that "***[k]eys may be copied and redistributed, if permitted***, or sent to another individual, if permitted." PO Resp., 18–19 (quoting Ex. 1003, 9:55–57) (emphasis by Patent Owner).

Patent Owner's arguments are not persuasive. Roseman describes keys that are transferable (Level 2 and 3 keys) and keys that are not transferable (Level 1 keys). Ex. 1003, 9:42–48. Petitioner's contentions (Pet. 17) are directed to Level 1 keys, which "may not be passed to any other person and may not be copied." *Id.* at 9:43–44. We find that keys that may not be passed to any other person are keys associated with that person. Figure 8 of Roseman is consistent with this because it describes passing a key to an "Absentee-Invitee" when the Invitee sends a delegate, i.e., a Level 2 key.

As to Level 1 keys, Patent Owner argues that a key is merely an attachment to an invitation, which "offers the only suggestion of an association with specific invitee." PO Resp. 19. Dr. Carbonell testifies (without identifying a basis) that Roseman's system could prevent the transfer of a key using a "no-transfer or no-duplication policy of such a key to insure that [it] always stays in the possession of the first user," by making transferability an attribute of the key and having the system simply assume, without recording transfers, that a user in possession of a key is authorized to use it. Ex. 2005 ¶ 31. As Petitioner argues, however, the claim construction to which Patent Owner agreed does not require an association between a key and a user to be implemented in a certain way. Reply 16. Even if Dr. Carbonell is correct as to how Roseman's keys would be implemented, such a non-transferable key would still be associated with the person who is prevented from transferring it.

Petitioner further argues that Roseman discloses storing keys in "a database which serves as a repository of tokens," as recited in claim 189, because a meeting room that is accessed by a key "'knows' about each key and its invitation level." Pet. 17–18 (quoting Ex. 1003, 9:49–51). According to Petitioner, a copy of each key must be stored on the host computer for the meeting room to "know" about each key. *Id.* at 18. Petitioner argues that a skilled artisan would have understood a database to be a stored collection of tokens. *Id.* Roseman does not expressly describe storing tokens in a database. Thus, we understand Petitioner to argue that tokens necessarily are stored in a database in light of Petitioner's cited disclosure—in other words, that a database is inherent in Roseman.

Patent Owner, relying on Dr. Carbonell's testimony, argues that a meeting room's knowledge of a key could be implemented using a hash function, which would not have required storage of the key in a database. PO Resp. 20–21 (citing Ex. 2005 ¶ 40). Petitioner characterizes Patent Owner's argument as "based on pure speculation and conjecture" and inconsistent with Roseman's disclosure. Reply 11–12. Nevertheless, we view both parties' respective theories of Roseman's implementation as speculation. Because Petitioner's position is speculative, it is insufficient to show that a database is inherent in Roseman.[8]

In the alternative, Petitioner argues that Rissanen teaches storing user authentication information, such as user identity information and passwords, in a database, and that such teaching would have been applicable to the keys of Roseman. Pet. 18–20. Petitioner argues that Roseman's keys are analogous to user identity and passwords. *Id.* at 19. Petitioner further argues that storing keys in a database is one of a finite number of known solutions for verifying whether a previously issued key matches to a key later presented by a user to access a conference room. *Id.* at 20 (citing Ex. 1002 ¶¶ 52–53).

Patent Owner admits that "[Rissanen] does disclose a database," but argues that its database is used in a different type of system. PO Resp. 22. Thus, Patent Owner does not contest that Rissanen's database stores user identities and passwords in a persistent manner and is used in conjunction with tools such as a DBMS. For Petitioner, Dr. Lavian testifies that "Rissanen clearly discloses a relational database whose data is stored

[8] Patent Owner also argues that Roseman does not suggest storing keys in a manner that is persistent and does not disclose tools such as a DBMS. PO Resp. 21–22. Roseman does teach that the data associated with its conference rooms is stored in a manner that is persistent, Ex. 1003, 12:16–28, and this at least suggests that keys also would be stored in such a manner. As to a DBMS, we explain above that the construction of "database" does not require this feature. Nevertheless, as explained below, Rissanen teaches a database even under Patent Owner's proposed construction.

persistently and includes tools for interacting with the data such as a DBMS." Ex. 1021 ¶ 37. We find that Rissanen teaches a database that stores data with persistence and tools for interacting with the database.

Nevertheless, Patent Owner argues "[i]f one were going to combine Roseman and Rissenan in order to authenticate an individual (and not merely authenticate a key for a room) the necessary logic would be significantly more complicated." PO Resp. 22. Petitioner does not argue, however, that Rissanen's database would be bodily incorporated into Roseman's system. Rather, Petitioner argues that Rissanen teaches storing data "analogous to and serv[ing] the same purpose as" the keys in Roseman in a database. Pet. 19. *See In re Mouttet*, 686 F.3d 1322, 1332–33 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements. . . . Rather, the test for obviousness is what the combined teachings of the references would have suggested to those having ordinary skill in the art."). Given that Roseman describes using keys to access conference rooms that have persistence, we agree with Petitioner that a database, described in Rissanen as storing similar information for a similar purpose, would be a straightforward and predictable choice for storing Roseman's keys.

The parties also dispute whether Roseman and Rissanen teach that the database "serves as a repository of tokens *for other programs to access*, thereby affording information to each of a plurality of participator computers," as recited in claim 189. Petitioner argues that other programs access the stored collection of tokens, including the various meeting or conference rooms maintained on the host computer. Pet. 20–21. Petitioner relies on disclosure in Roseman that a meeting room is accessible from a virtual hallway with doors to other meeting rooms. *Id.* (citing Ex. 1003, 9:63–65). According to Petitioner, "[e]ach meeting room . . . 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." *Id.* at 21.

Patent Owner argues that "Petitioner does not identify any programs that could access a database of tokens and receive information, other than the singular conference calling software running on the host computer of Roseman." PO Resp. 24. According to Patent Owner, "to the extent that there are multiple conference rooms in existence is because the Roseman system has instantiated the same conference room program with different parameters as there is no suggestion that there is different software associated with each conference room." *Id.* Patent Owner does not explain why "other programs" require different software rather than different instantiations of the same software, or point to evidence supporting this view. We are not persuaded that the claims should be limited in this way. Nevertheless, as Petitioner points out (Reply 18), Roseman characterizes its conference rooms as collections of different programs (Ex. 1003, 12:16–18) and makes clear that different conference rooms will have different attributes (different virtual equipment, different tools, different appearances, etc.) (*id.* at 3:42–50, 10:9–12). We find that Roseman at least suggests different conference rooms with different programs, even under Patent Owner's view. These programs determine whether a participant can join a meeting room based on evaluations of keys that, in light of Rissanen, would have been stored in a database. Thus, we find that Roseman and Rissanen teach “a database which serves as a repository of tokens for other programs to access,” as recited in claim 189.

The parties also dispute whether Roseman and Vetter teach “communicating via an Internet network,” as recited in claim 189. As explained above, Roseman describes communicating between a host and local computers via commercially available LANs and WANs. Ex. 1003, 1:37–41, 3:14–19. Petitioner contends that a skilled artisan would have understood the Internet to be an example of the commercially available WAN described in Roseman. Pet. 24, 26; Ex. 1002 ¶¶ 53–64. According to Dr. Lavian, “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.” Ex. 1002 ¶ 63; *see also* Ex. 2006 (Lavian Dep.), 104:12–105:23 (“Q So Roseman could have been implemented in that 1994 to ’96 time frame with ATM technology? A If I’m looking at the specification of Roseman and what specifically Roseman disclose, it disclose as using a -- local computers become connected to host computer via commercially available Local Area Networks and Wide Area Networks. When you’re talking about Local Area Networks and Wide Area Networks, this is the Internet. That’s different name to Internet. Q So you’re saying that Roseman by itself teaches the Internet? A Roseman by itself reference to remote computers commercially available, commercially available that said Internet. Local Area Networks, definitely part of the Internet. Wide Area Networks, different name to the Internet. It’s actually the Internet itself. . . .”).

Petitioner further argues that Vetter teaches using the Internet to facilitate the same types of computer-based conferencing functions as described in Roseman. Pet. 24–25. Petitioner contends that Vetter itself identifies a reason to combine the teachings of Roseman and Vetter, namely "[v]ideoconferences are becoming increasingly frequent on the Internet" and the CU-SeeMe videoconferencing tool described in Vetter "is also becoming very popular." *Id.* at 25–26 (quoting Ex. 1005, 77 (emphases by Petitioner)).

Patent Owner argues that Vetter does not state that Internet videoconferencing would have been ubiquitous at the time of the invention; rather, Patent Owner argues, the Internet was beginning to support video conferencing. PO Resp. 26. Patent Owner further argues that Vetter discusses difficulties in applying videoconferencing on the Internet, including feedback when participants leave their microphones on, degraded performance when broadcasting simple graphic images, workstations that locked up in a classroom when video streams overwhelmed a network, and counter-intuitive paths that data can take when travelling from one site to another. *Id.* at 26–27 (citing Ex. 1005, 78–79). Dr. Carbonell testifies (without citation) that video traffic on the Internet would experience unpredictable delay that would interfere with re-assembling video streams at the receiving end in real time. Ex. 2005 ¶ 59. Dr. Carbonell testifies (again without citation to evidence) that one would not experience these problems on a private WAN because such a network would be of a more predictable configuration. *Id.* ¶ 61.

Patent Owner also points to a half-page article in a technical magazine by Robert Metcalfe, founder of 3Com, "[p]redicting the Internet's catastrophic collapse" at the end of 1995 due to reasons such as low user measurements, telecom company monopolies, and security and capacity concerns. PO Resp. 27–28 (quoting Ex. 2009). We agree with Petitioner, however, that "the incorrect prediction of a single individual would not have discouraged (and did not discourage) the industry from using the Internet." Reply 8. Patent Owner offers no persuasive evidence that Dr. Metcalfe's views were shared widely, or at all, by skilled artisans in 1995. Indeed, the article itself suggests the contrary. Ex. 2009 ("Almost all of the many predictions now being made about 1996 hinge on the Internet's continuing exponential growth.").

Citing Dr. Metcalfe's article, Dr. Carbonell testifies that other technologies such as Integrated Services Digital Network (ISDN) and Asynchronous Transfer Mode (ATM) would have been better suited than the Internet to handle video conferencing in the mid-1990's. Ex. 2005 ¶ 60. As explained above, Patent Owner has not explained persuasively why Dr. Metcalfe's magazine article is representative of the views of a skilled artisan. The article itself does not state that there were, or identify evidence of, technologies better suited than the Internet to handle videoconferencing. Ex. 2009. Thus, we are not persuaded that the Internet would have been an inferior technology for videoconferencing in 1995. Moreover, claim 189 on its face does not require videoconferencing. In any case, the Federal Circuit has explained that "just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes." *Mouttet*, 686 F.3d at 1334.

Roseman expressly states that its local computers and host communicate via a commercially available WAN. We credit Dr. Lavian's testimony that, to the extent that this is not an express reference to the

Internet, the most suitable and obvious commercially available WAN would have been the Internet. We also find that Vetter suggests using the Internet for purposes similar to those of Roseman. Vetter describes an example in which features such as audio, video, and virtual whiteboard tools are used to conference over the Internet. Ex. 1005, 77–78. Thus, to the extent Roseman does not expressly suggest using the Internet, Vetter includes an express suggestion to update a system such as Roseman using modern electronic components, such as the Internet, to gain the commonly understood benefits of such adaptation. *See Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1162 (Fed. Cir. 2007); *cf., Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1326–27 (Fed. Cir. 2008) ("The record in this case demonstrates that adapting existing electronic processes to incorporate modern internet and web browser technology was similarly commonplace at the time the '099 patent application was filed."). Vetter reinforces our finding that the Internet would have been the most suitable commercially available WAN for use in Roseman's system.

To be sure, Vetter discusses challenges encountered in implementing videoconferencing on the Internet, but Vetter also teaches that existing tools can be tailored to specific applications on the Internet "so that their limitations can be *promptly recognized and corrected*." Ex. 1005, 79 (emphasis added). The Federal Circuit has recognized that "a given course of action often has simultaneous advantages and disadvantages, and this does not necessarily obviate motivation to combine." *Medichem, S.A. v. Rolabo, S.L.*, 437 F.3d 1157, 1165 (Fed. Cir. 2006). We find that addressing the challenges discussed in Vetter would have been well within the skill of an ordinarily skilled artisan, an engineer experienced in computer networking. Thus, we find that Roseman, Rissanen, and Vetter teach "[a] method of communicating via an Internet network" as recited in claim 189.

In sum, we find that the combination of Roseman, Rissanen, and Vetter teaches "[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," as recited in claim 189.

### *b. "affording some of the information to a first of the participator computers via the Internet network, responsive to an authenticated first user identity; affording some of the information to a second of the participator computers via the Internet network, responsive to an authenticated second user identity"*

As explained above, Roseman describes admitting participants into a conference room when the participants present keys. Ex. 1003, 10:61–65. We find that this teaches "an authenticated first user identity" and "an authenticated second user identity." Additionally, Roseman describes various ways of affording information to local computers of users admitted to the conference room, including as follows:

> 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.

*Id.* at 11:18–26. *See also* Pet. 28–30. As explained in Section II.B.3.a above, Roseman and Vetter teach that such communications can be via an Internet network.

Accordingly, we find that Roseman and Vetter teach these limitations of claim 189. We note that Patent Owner does not contest that Roseman and Vetter teach these limitations.

#### *c. "determining whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications" and*

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

Petitioner contends that Roseman describes several examples of determining whether user identities are able to form groups. Pet. 32–33, 44. Petitioner argues that a host computer uses keys to determine whether users can form a group conference in a conference room. *Id.* at 32. Petitioner also argues that a host can form a "child room" in the same manner. *Id.* Petitioner also points to Roseman's "Whisper Mode" and private note passing features as examples of groups. *Id.* at 32–33. We agree with Petitioner that each of these is an example of Roseman's host computer determining whether multiple user identities are able to form a group.

Petitioner contends that communications in one of Roseman's conference rooms, such as placing documents on a table, drawing on a document, and moving a pointer, take place in real time because they are communicated to participants as the underlying events occur. *Id.* at 33–34, 45–46. For example, Roseman explains:

> 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 [] preceding three events as they occur.

Ex. 1003, 2:38–47. We find that these are specific examples in Roseman of real-time communications sent and received by the participator computers in a group.

As explained in Section II.B.3.a above, Roseman and Vetter teach that such communications can be via an Internet network.

Thus, we find that Roseman and Vetter teach these limitations of claim 189. We note that Patent Owner does not contest that Roseman and Vetter teach these limitations.

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

Petitioner argues that Roseman describes several examples of presenting data of different types, including:

a *pointer*: Ex. 1003, 14:53–62 (description of a user placing a file onto a virtual conference table, the host sending an icon (pointer) representing that file to the other participator computers in the group, and a participant clicking on the icon, causing the host computer to present the file to all participants);

*audio and video*: *id.* at 11:11–16 ("Audio and video connections are made if supported by the user, the room and the other users. A small picture of each user is displayed in the meeting room to indicate presence. If video links are enabled than [sic] the picture may be replaced with a video signal from the user, typically showing the user.");

*graphic*: *id.* at 8:1–4 ("Each Invitee can transmit a file (of any suitable kind: data, text, or graphic) to the host, and the host will place the file onto the table, where all participants can see it.");

*multimedia*: *id.* at Abstract (discussing "'multi-media' conferencing").

Pet. 35–36, 38–40. We agree that these are specific examples of data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

As to "determining whether the first user identity is individually censored from sending data in the communications," as recited in claim 189, Petitioner contends that Roseman's host computer can act as a "moderator" to regulate when and/or how long participants can speak during a conference. Pet. 41–42. Specifically, Roseman describes the following:

> 11. Host Can Act as Moderator. The Requestor may wish to hold a conference wherein ideas are freely exchanged among the participants. It is possible that this intent can be defeated by an aggressive person who dominates the conference, and, in effect, maintains a "filibuster."
>
> The host can automatically prevent filibustering, in several ways. One, the host can monitor the speech of each person, and place a limit on the total time allowed to each person. The limit can be overriden by the Requester, or by a vote taken by the host of the other participants.
>
> Two, while one participant is speaking, the host can monitor the audio input of the other participants. The host looks for instances when the speaker refuses to stop talking when the other participants speak. When the host finds such instances, the host issues a message to all participants stating that a filibuster appears to be occurring, and requests a vote as to whether to allow the filibuster to continue.

Ex. 1003, 12:29–45. We find that this is an example of "determining whether the first user identity is individually censored from sending data in the communications . . . by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities." Here, the first user identity is the party seeking to filibuster and the other of the user identities can be the requestor or the other participants who vote.

Petitioner also argues that Lichty teaches censoring. Pet. 42. In particular, Petitioner points to the "Ignore" button of Lichty's user interface. *Id.* Petitioner contends that a first member pressing the ignore button is "an other of the user identities" and the party the first member chooses to ignore corresponds to "the user identity" of claim 189. *Id.* Petitioner argues that both Roseman and Lichty state essentially the same reason for their respective moderator and "ignore" features, namely solving the common problem of dealing with potentially unwanted communications from conference participants. *Id.* at 43–44; *see also* Ex. 1003, 12:29–33 ("The requestor may wish to hold a conference wherein ideas are freely exchanged among the participants. It is possible that this intent can be defeated by an aggressive person who dominates the conference, and, in effect, maintains a 'filibuster.'"); Ex. 1007, 510 ("Ignore is most useful when the chat of another member becomes disruptive in the chat room."). Petitioner argues that Lichty's solution would be equally applicable to Roseman. Pet. 44. We agree with Petitioner that Lichty teaches another example of "determining whether the first user identity is individually censored from sending data in the communications . . . by determining whether a respective at least one parameter corresponding to the first user identity has been determined by an other of the user identities." We find that Lichty's "ignore" feature would have been a predictable solution for the common problem described in both Roseman and Lichty, namely, dealing with unwanted communications from disruptive users.

On the complete record, we find that Roseman and Lichty teach these limitations of claim 189. We note that Patent Owner does not contest that Roseman and Lichty teach these limitations.

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

Petitioner contends that Roseman teaches sending a document from a first participator computer to a second participator computer by using a document icon that the host computer places on a virtual conference table for retrieval by the second participator computer. Pet. 41–42. Petitioner contends that Pike provides a teaching of "basic and familiar Internet concepts, such as hypertext links and URLs." *Id.* at. 36. Petitioner argues that it would have been obvious to combine this teaching with the teachings of Roseman and Vetter, with the predictable result that Roseman's clickable icons include URLs to identify the location of the corresponding document on the host computer. *Id.* at 37. Petitioner argues that a person of ordinary skill would have known that this would be advantageous as it would alleviate a need to communicate the file content itself from the host computer to the participant computer unless requested by the participant. *Id.* at 37–38. As explained in detail above, it would have been obvious to implement Roseman's system to communicate over the Internet. We find that it would have been straightforward and obvious to implement Roseman's icon as a URL, as Pike illustrates that it was well-known to implement pointers as URLs when communicating over the Internet. Ex. 1006, 43.

On this record, we are persuaded that Petitioner's evidence supports a finding that Roseman teaches this limitation of claim 189. We note that

Patent Owner does not contest that Roseman, Vetter, and Pike teach this limitation.

### 4. *Claim 465*

Petitioner contends that independent claim 465 recites an apparatus with limitations that are substantially similar to the steps of claim 189. Pet. 53. Petitioner shows in a claim chart where each limitation of claim 465 overlaps with claim 189. *Id.* at 54–55. Petitioner argues that claim 465 would have been obvious for the same reasons given for claim 189. *Id.* at 55–56. Patent Owner does not advance any additional arguments for claim 465. PO Resp. 30–31. We agree with Petitioner's identification of overlap and find that claim 465 is taught by Roseman, Rissanen, Vetter, and Lichty for the reasons given for claim 189, above.

### 5. *Intermediate Claims 202, 208, 214, 220 and Challenged Claims 203, 209, 215, 221*

Petitioner challenges dependent claims 203, 209, 215, and 221, which depend indirectly from challenged claim 189. '659 Pet. 6. The challenged dependent claims depend directly from claims 202, 208, 214, and 220, respectively, which are not challenged. Nevertheless, to determine the patentability of claims 203, 209, 215, and 221, we must evaluate unchallenged intermediate claims 202, 208, 214, and 220.

Claims 202, 208, 214, and 220 recite "wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of," respectively:

"the data presenting the video" (claim 202);

"the data presenting the audio" (claim 208);

"the data presenting the graphic" (claim 214); and

"the data presenting the multimedia" (claim 220).

Petitioner makes essentially the same argument for each of these claims. For example, for claim 202, Petitioner refers to examples of communicating video that it presented for the limitation of claim 189, "determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia,"[9] and incorporates the arguments it presents for claim 189[d] to show censoring. Pet. 51–52; s*ee also id.* at 57–61 (similar arguments for claims 208, 214, and 220).

Patent Owner argues that "Lichty merely discloses ignoring a user, not specifically excluding video, audio, graphic or multimedia from being presented to a certain identity" and that "Lichty excludes a user, not content or data from being presented." Supp. PO Resp. 9–10. Patent Owner also argues that "Petitioner's assertion that the same reasoning from limitation 189[d] applies to the present limitations is incorrect for at least the reason that 189[d] fails to apply to the level of particularity of claims 202, 208, 214, and 220, and thus Petitioner fails to address each and every limitation of the claims." Supp. PO Resp. 10.

In reply, Petitioner argues that "[t]he Petition cited Lichty for its disclosure of its censoring feature, and relied on the host in Roseman to carry out the other features of the claim, including the transmission of video, audio, content, graphic or multimedia content" and that "under the

[9] Petitioner refers to this limitation as limitation "189[d]."

combination of Roseman and Lichty, when a first user is blocked from sending data to a second user via the censoring features of Lichty, that user is blocked from sending video, audio, graphic or multimedia content, whatever the case may be." Reply 7. In other words, Petitioner argues that, by censoring a user from sending any content, the user effectively is censored from sending individual types of content, including video, audio, graphic, or multimedia, even if there is no determination specific to the type of content. Petitioner does not contend that Roseman and Lichty teach making a determination as to whether a user can send data based on the type of data the user seeks to send. For example, Petitioner does not contend that Roseman and Lichty teach censoring a user from sending video data, but permitting the user to send audio data.

Claim 189 recites "determining whether the first user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia." On its face, claim 189 does not require a determination that the user is censored from sending a particular type of data. Rather, claim 189 recites determining whether the user identity is censored from sending data. Claims 202, 208, 214, and 220, however, more narrowly recite determining whether the first user identity is censored from sending particular types of data. Claim 202, for example, recites "determining that the first user identity is censored from the sending of the data presenting the video." Claim 202, thus, positively recites a determination of censorship based on data type. Contrary to Petitioner's reading, claim 202 recites more than just a result of a general censorship of all data sent by the user. Claims 208 (audio), 214 (graphic), and 220 (multimedia) similarly recite determination of censorship based on data type.

In Section II.A.1 above, we construe "censor," by itself, to mean "control what is said in a group," and "the first user identity is individually censored from sending data," as recited in claim 189, to refer to control of data sent by the at least one of the user identities, individually. Nevertheless, claims 202, 208, 214, and 220 include additional language reciting determinations based on data type. This is consistent with the description in the specification that "[c]ensorship also can use the tokens for real time control of data (ascii, text, video, audio) from and to users, as well as control over multimedia URLs—quantity, type, and subject." Ex. 1001, 8:17–19.

As explained above, Roseman describes censoring users from sending all communications based on a determination that the user is conducting a filibuster. Ex. 1003, 12:29–45. Petitioner points to no description in Roseman of determining that a user is censored from sending a particular type of data—it is all or nothing. Likewise, Lichty describes an ignore feature for blocking all communications from a disruptive user, regardless of data type—again, all or nothing. Ex. 1007, 269, 510. We find that Roseman and Lichty do not teach determining that a user is censored from sending certain types of data.

In sum, Petitioner has not shown that Roseman, Rissanen, Vetter, Lichty, and Pike teach the limitations of intermediate claims 202, 208, 214, and 220. Accordingly, Petitioner has not shown by a preponderance of the evidence that Roseman, Rissanen, Vetter, Lichty, and Pike render obvious claims 203, 209, 215, and 221.

### 6. *Intermediate Claims 476, 481, 486, 491*

Petitioner challenges independent claim 465 and dependent claims 477, 482, 487, and 492, which depend indirectly from claim 465. '659 Pet. 6. The challenged dependent claims depend directly from claims 476, 481, 486, and 491, respectively, which are not challenged. Nevertheless, to determine the patentability of claims 477, 482, 487, and 492, we must evaluate unchallenged intermediate claims 476, 481, 486, and 491.

Claim 476 recites "wherein data presents the video"; claim 481 recites "wherein the data presents the audio"; claim 486 recites "wherein the data presents the graphic"; and claim 491 recites "wherein the data presents the multimedia." For the reasons given in Section II.B.3.d above, we find that Roseman teaches examples of the data presenting video, audio, graphics, and multimedia. Thus, Roseman teaches the additional limitations of claims 476, 481, 486, and 491. We note that Patent Owner does not raise any additional arguments for these claims.

### 7. *Claims 334, 477, 482, 487, 492, 580 ("two client software alternatives")*

Claim 334 depends from claim 189 and adds

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

Claim 580 depends from claim 465 and recites the same limitation. Claims 477, 482, 487, and 492 depend from intermediate claims 476, 481, 486, and 491, respectively, and recite substantially the same limitation.

In the Institution Decision, we determined that the claim language "the computer system provides access via any of two client software alternatives" refers to separate software platforms implementing user interfaces on two different participator computers, with both providing access to the control computer. Dec. 34. This is the reading most consistent with the '657 patent's description. Ex. 1001, 2:25–31 ("Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message."), 4:32–35 ("While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled."), 5:1–5 ("The Participator Computers 5 are each running and under the control of Participator Software 4, which directs each of the Participator Computers 5 to handle a user Interface permitting one said user to send a multimedia information Message 8 to the Controller Computer 3 . . . .").

Petitioner argues that Roseman describes its local computers as using a Windows operating system, but notes that other environments are within the level of skill in the art. Pet. 48 (citing Ex. 1003, 12:1–5, 12:9–10); '659 Pet. 53. Dr. Lavian testifies that it was well-known to provide software products for multiple computing platforms, such as Windows and Macintosh because it was more commercially attractive and would increase the number of users who could use the software. Ex. 1002 ¶ 119. Petitioner argues that it would have been obvious to provide alternatives for local computer software that would operate on Windows and Macintosh platforms. Pet. 48; ’659 Pet. 53.

Patent Owner argues that “Roseman does not indicate how a second alternative would be able to communicate with the host computer to receive the common image or to interact with it” and that “Roseman’s disclosure of the ‘Windows Context’ is not an affirmative teaching of another client software alternative.” PO Resp. 33; Supp. PO Resp. 5–6. Petitioner, however, does not argue that Roseman expressly teaches two client software alternatives. Rather, Petitioner argues that Roseman describes one software alternative, for the Windows platform, and expressly teaches that software for other platforms would have been within the level of skill in the art. Pet. 48; ’659 Pet. 53; Reply 20 (“The Petition explained that the claimed two client software alternatives were obvious, among other reasons, because it would have been obvious to adapt the participator software in Roseman to run on multiple computing platforms, such as Windows and Macintosh.”); Supp. Reply 3.

Patent Owner argues that Roseman does not “indicate how any of its client software could be modified so as to make [a] second software alternative.” PO Resp. 33; Supp. PO Resp. 6. According to Patent Owner, Dr. Lavian admitted in deposition that it is not always possible to make the same software programs for different operating systems. PO Resp. 34 (citing Ex. 2006, 157:6–158:11); Supp. PO Resp. 6–7. Although it might not be possible to adapt every software program to work on every operating system, Roseman itself suggests adapting its software to different environments beyond Windows. Ex. 1003, 12:1–10. Thus, Patent Owner's argument is not persuasive.[10]

Patent Owner also argues that Windows and Macintosh are not client software, but instead are operating systems. PO Resp. 33; Supp. PO Resp. 6. Petitioner, however, does not argue that Windows and Macintosh are the two software alternatives. Rather, Petitioner argues that Roseman describes a client software alternative that would work with the Windows operating system and suggests that another client software alternative working with the Macintosh operating system would have been within the level of skill in the art. Pet. 48; '659 Pet. 53; Reply 20 ("But the Petitioner did not point to Windows and Macintosh *themselves* as the two client software alternatives, but rather, to versions of the participator software in Roseman adapted to run on those platforms."); Supp. Reply 3. Thus, Patent Owner's argument is not persuasive.

Patent Owner further contends that a skilled artisan would not have used two separate software alternatives to implement Roseman's client software with Windows and Macintosh platforms because the skilled artisan would have used Java instead. PO Resp. 34–35; Supp. PO Resp. 7–8. According to Patent Owner, "Java and byte-code are cross-platform solutions that can run on both Windows and Macintosh." PO Resp. 34; Supp. PO Resp. 7. Dr. Carbonell testifies that

[10] Patent Owner also argues that a Telnet-based solution for Roseman would not work without graphical user interface (GUI) support. PO Resp. 33; Supp. PO Resp. 6. This is inapposite, as Petitioner does not argue that Roseman would have been modified to accommodate a Telnet-based solution.

> one of ordinary skill in the art who was motivated to provide software that could work across different platforms and operating systems would have been motivated to utilize a single platform independent software implementation, such as a Java implementation and would not have been motivated to provide additional alternatives to that cross-platform software.

Ex. 2005 ¶ 71.

Petitioner argues that the claim language does not exclude platform-specific embodiments and that the '657 patent specifically describes such embodiments as within the scope of the invention. Reply 21 (citing Ex. 1001, 4:32–35 ("While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled."). We agree with Petitioner. As noted above, "just because better alternatives exist in the prior art does not mean that an inferior combination is inapt for obviousness purposes." *Mouttet*, 686 F.3d at 1334. Thus, even if Java would have been advantageous in some circumstances, we still find that platform-specific client software embodiments would have been an apt extension of Roseman's system.

In light of Roseman's description of client software for the Windows environment and its express teaching that the software for other environments is within the level of skill, Ex. 1003, 12:1–10, we are persuaded that Roseman at least suggests client software for other platforms that were common at the time, such as Macintosh. We credit Dr. Lavian's testimony that providing software for use with both Windows and Macintosh would have made Roseman's system more commercially attractive by increasing the number of users who could use the software. Ex. 1002 ¶ 119. *See also KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007) ("When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one.”). Thus, we find that Roseman suggests “wherein the computer system provides access via any of two client software alternatives,” as recited in claim 334 and similarly recited in claims 477, 482, 487, and 492.

Petitioner contends that Roseman’s software running on a local computer, which can be a software implementation for a Windows platform and a Macintosh platform, allows user identities to be recognized by the host computer. Pet. 50–51; ’659 Pet. 55–56. Petitioner argues that a group of local computers is formed when a user of a local computer in Roseman drags other participants into a child-room. Pet. 51; ’659 Pet. 56. In another example, Petitioner argues that Roseman’s description of creating a virtual conference room, involving identifying the participants of the conference room and requiring invited users to have appropriate keys, teaches permitting at least a first user identity and a second user identity to form a group. Pet. 32; ’659 Pet. 34.

We agree with Petitioner. When Roseman’s users, via software running on their respective local computers, access conference rooms using keys, Roseman’s host computer recognizes the users and allows them to send and receive communications from each other. Ex. 1003, 3:22–56. Thus, we find that Roseman teaches “wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications,” as recited in claim 334, and similarly recited in claims 477, 482, 487, 492, and 580.

### *8. Remaining Challenged Dependent Claims*

Claim 342 depends from claim 189 and adds "wherein at least one of the communications includes data presenting a human communication of sound." Claim 584 depends from claim 465 and adds a similar limitation. As Petitioner observes (Pet. 52), Roseman describes communicating in virtual conference rooms via audio connections. Ex. 1003, 11:11–16. Thus, Roseman teaches the additional limitation of claims 342 and 584.

Claim 348 depends from claim 189 and adds "providing the first user identity with access to a member-associated image corresponding to the second user identity." Claim 592 depends from claim 465 and adds a similar limitation. Petitioner points to Roseman's description of including photographs of each participant in the common screen presented to the users. Pet. 52–53 (citing Ex. 1003, 7:35–39, Fig. 9). This is shown in Figure 9 of Roseman, reproduced above. Based on this evidence, we find that Roseman teaches the subject matter of claims 348 and 592.

### *9. Conclusion of Obviousness*

As explained above, Roseman, Rissanen, Vetter, Lichty, and Pike teach each limitation of claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592. Petitioner has introduced persuasive evidence that a skilled artisan would have had reasons to combine the teachings of Roseman, Rissanen, Vetter, Lichty, and Pike. Patent Owner does not argue or introduce evidence of objective indicia of nonobviousness. In sum, upon consideration of all the evidence, we conclude that Petitioner has proved by a preponderance of the evidence that claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 would have been obvious over Roseman, Rissanen, Vetter, Lichty, and Pike. Petitioner has not proved, by a preponderance of the evidence, that claims 203, 209, 215, and 221 are unpatentable.

## III. PATENT OWNER'S MOTION TO EXCLUDE

Patent Owner filed a paper styled "Motion to Exclude Evidence," seeking to exclude certain portions of the 2nd Lavian Declaration that it argues exceeds the proper scope of a reply. Paper 39, 1. Specifically, Patent Owner moves to exclude portions of paragraphs 54, 74, and 75 of the 2nd Lavian Declaration. *Id.* at 2–5.

Petitioner opposes this motion on the ground that it is not directed to the admissibility of evidence and, therefore, is procedurally improper. Paper 42, 2. Patent Owner contends that arguments that exceed the scope of a reply are irrelevant, prejudicial, confusing, or misleading under Federal Rules of Evidence 401, 402, and 403. Paper 44, 1–2. As Petitioner points out, however, the Board repeatedly has denied, as improper, motions to exclude that merely argue that evidence is outside the proper scope of a reply. Paper 42, 2–3. Despite its invocation of Rules 401, 402, and 403, we agree that Patent Owner's Motion to Exclude is nothing more than an argument that Petitioner's Reply exceeds its proper scope. Accordingly, we deny Patent Owner's Motion.

Nevertheless, we have considered Patent Owner's argument with respect to those portions of Petitioner's Reply that are relied upon in this decision, and determine they do not belatedly raise new issues or present evidence that should have been presented in the Petition. In any case, we do not rely on paragraphs 54, 74, and 75 of the 2nd Lavian Declaration.

## IV. CONCLUSION

Petitioner has proved by a preponderance of the evidence that claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 are unpatentable, but has not proved that claims 203, 209, 215, and 221 are unpatentable.

## V. ORDER

For the reasons given, it is:

ORDERED, based on a preponderance of the evidence, that claims 189, 334, 342, 348, 465, 477, 482, 487, 492, 580, 584, and 592 are unpatentable; and

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

PETITIONER:

Heidi Keefe
hkeefe@cooley.com

Phillip Morton
pmorton@cooley.com

Andrew Mace
amace@cooley.com

PATENT OWNER:

Peter Lambrianakos
plambrianakos@brownrudnick.com

Vincent Rubino
vrubino@brownrudnick.com

US008458245B1

# (12) United States Patent
Marks

(10) Patent No.: US 8,458,245 B1
(45) Date of Patent: Jun. 4, 2013

(54) **REAL TIME COMMUNICATIONS SYSTEM**

(76) Inventor: **Daniel L Marks**, Urbana, IL (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 620 days.

(21) Appl. No.: **11/510,463**

(22) Filed: **Aug. 24, 2006**

**Related U.S. Application Data**

(63) Continuation of application No. 09/399,578, filed on Sep. 20, 1999, and a continuation of application No. 08/617,658, filed on Apr. 1, 1996, now Pat. No. 5,956,491, said application No. 09/399,578 is a continuation of application No. 08/617,658, filed on Apr. 1, 1996, now Pat. No. 5,956,491.

(51) **Int. Cl.**
***G06F 15/16*** (2006.01)

(52) **U.S. Cl.**
USPC ............ **709/202**; 709/206; 709/207; 709/217

(58) **Field of Classification Search**
USPC .................................... 709/204, 205; 715/753
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 5,347,632 A * | 9/1994 | Filepp et al. | .................. | 709/202 |
| 5,408,470 A * | 4/1995 | Rothrock et al. | ............ | 715/753 |
| 5,440,624 A | 8/1995 | Schoof, II et al. | | |
| 5,452,299 A | 9/1995 | Thessin et al. | | |
| 5,616,876 A | 4/1997 | Cluts | ............................... | 84/609 |
| 5,771,355 A | 6/1998 | Kuzma | | |
| 5,774,668 A | 6/1998 | Choquier et al. | | |
| 5,793,365 A | 8/1998 | Tang et al. | ..................... | 345/329 |
| 5,880,731 A | 3/1999 | Liles et al. | ..................... | 345/349 |
| 5,941,947 A * | 8/1999 | Brown et al. | ................. | 709/225 |
| 6,560,707 B2 | 5/2003 | Curtis et al. | .................. | 713/163 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| EP | 336 552 A2 | 10/1989 |

OTHER PUBLICATIONS

Pavel Curtis et al., MUDs Grow Up: Social Virtual Reality in the Real World, Xerox PARC, Jan. 1993, 6 pages.*
Bentley et al.. Supporting Collaborative Information Sharing with the World Wide Web: The BSCW shared workspace system, Proceedings of the 4th International World Wide Web Conference, Dec. 1995, 12 pages.*
Atul Prakash et al., DistiVew for Building Efficient Collaborative Applications using Replicated Objects, Proceeding of the 1994 ACM conference on Computer supported cooperative work, 12 pages.*

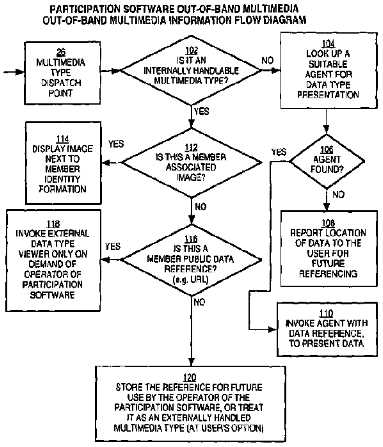
(Continued)

*Primary Examiner* — Patrice Winder
(74) *Attorney, Agent, or Firm* — Peter K. Trzyna, Esq.

(57) **ABSTRACT**

A computerized human communication arbitrating and distributing system, including a controller digital computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information from a human user and an output device for presenting information to the user, each said user having a user identity. A connection, such as Internet, links the controller computer with each of the participator computers. Controller software runs on the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups through the controller computer and to distribute real time data to the respective ones of the groups. Participator software runs on each of the participator computers to handle a user interface permitting one said user to send a multimedia information message to the controller computer, which arbitrates which of the participator computers receive the multimedia information message and conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

**58 Claims, 22 Drawing Sheets**


PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM
26 MULTIMEDIA TYPE DISPATCH POINT
102 IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104 LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114 DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112 IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106 AGENT FOUND?
NO
NO
118 INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116 IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
108 REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
NO
110 INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120 STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

## OTHER PUBLICATIONS

Kankanahalli Srinivas et al., MONET: A Multi-media System for Conferencing and Application Sharing in Distributed Systems, Feb. 1992, CERC Techinical Report Series Research Note, 19 pages.*

Vinod Anupam et al., Collaborative multimedia scientific design in Shastra, Proceedings of the first ACM Internation conference on Multimedia, Multimedia '93, Aug. 1993, pp. 447-456.*

Vinod Anumpam et al., Shastra—An Architecture for Development of Collaborative Applications, Proceedings on Second Workshop on Enabling Technologies: Infrastructure for Collaboration Enterprises, Apr. 1993, pp. 155-166.*

Andreas Dieberger, Providing Spatial Navigation for the World Wide Web, Spatial Information theory a Theoretical Baisi for GIS, Lecture Notes in Computer Science, vol. 988, 1995, pp. 93-106.*

Lee Newberg et al., Integrating the Worl-Wide Web and Multi-User Domains to Support Advanced Network-Based Learning Experiments, Conference Proceedings of ED-MEDIA 1995, pp. 494-499.*

T Y Hou et al., An active multimedia System for Delayed Conferencing, Proceedings of the SPIE Conference on High-Speed Networking and Multimedia Computing, San Jose CA, 1994, pp. 97-104.*

Office Action-Final Rejection Dated Apr. 8, 2004 from U.S. Appl. No. 09/399,578.

"Complaint: *Brian Hollander* vs. *Peter K. Trzyna and PTK Technologies, LLC*," Dated Nov. 13, 2007, pp. 1-18.

Tim Meyer et al., A MOO-Based Collaboration Hypermedia System for WWW, Proceedings for Second International Conference for WWW, Oct. 1994.

Paul Kindberg et al., Mushroom: a framework for collaboration and interaction across the Internet, In the Proceedings of ERCIM Workshop on CSCW and the Web, Feb. 1996, 11 pages.

"Amendment and Response" filed on Feb. 5, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Oct. 5, 2009, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Response to Notice of Non-Responsive reply and Supplemental Amendment and Response" filed on Feb. 6, 2009, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"MUDS Grow Up: Social Virtual Reality in the Real World". Curtis P. and Nichols, D.A. Xerox PARC. (Jan. 1993) pp. 1-6.

"Office Action-Non-Final Rejection" mailed Jul. 22, 2009, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Jan. 19, 2010, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Office Action" mailed on Mar. 18, 2008, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Sep. 18, 2008, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment After Final" filed on Jun. 11, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Final Rejection" mailed on May 12, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

Atul Prakash et al., DistView for Building Efficient Collaborative Applications using Replicated Objects, Proceedings of the 1994 ACM conference on Computer supported cooperative work. pp. 153-164.

K.J. Maly et al., Mosaic + XTV = CoReview, Computer Networks and ISDN Systems, vol. 27 Issue 6, Apr. 1995, pp. 849-860, Proceedings of the Thrid International World Wide Web Conference.

"Fourth Preliminary Amendment" filed on May 25, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Third Preliminary Amendment" filed on May 7, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Apr. 14, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

Meloan, Steve. CU-SeeMe. Tech Toys. 1995 Urban Desires. pp. 1-2 http://desires.com/1.6/Toys/Cuseeme/cuseeme.html.

Oikarinen, J. & Reed, D. Internet Relay Chat Protocol. May 1993. pp. 1-69.

Expert Report of Bruce M. Maggs. pp. 1-134, received Aug. 2005.

Anupam, Vinod "Collaborative Multimedia Environments for Problem Solving." A Thesis Submitted to Purdue University. (Aug. 1994), pp. 1-212, Ann Arbor, MI.

Bajaj, Chandrajit et al. "Collaborative Multimedia in Shastra." 3rd International Conference on Multimedia, San Francisco, CA (1995). pp. 365-366.

Anupam, Vinod et al. "Collaborative Multimedia in Scientific Design." Proceedings: First ACM Multimedia Conference ACM Multimedia 93, Anaheim, California, ACM Press, (1993). pp. 447-456.

Anupam, Vinod et al. "Shastra—An Architecture for Development of Collaborative Applications." Proceedings: Second IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Morgantown, (1993). pp. 155-166.

Bajaj, Chandrajit et al. "Brokered Collaborative Infrastructure for CSCW." Proceedings: Fourth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Berkeley Springs, West Virginia, IEEE Computer Society Press, (1995), pp. 207-213.

Anupam, Vinod et al. "Shastra: Multimedia Collaborative Design Environment." IEEE Multimedia, 1,2, (1994), pp. 39-49.

Anupam, Vinod et al. "Distributed and Collaborative Visualization." IEEE Computer, 27, 7, (Jul. 1994), pp. 37-43.

Bajaj, Chandrajit et al. "Web based Collaborative Visualization of Distributed and Parallel Simulation." In Proceedings of the 1999 IEEE Symposium on Parallel Visualization and Graphics, (Oct. 24-29, 1999), San Francisco, CA, pp. 47-54.

Bajaj, Chandrajit et al. "NLS: Collaborative Virtual Environment to Promote Shared Awareness." Proceedings: Workshop on New Paradigms in Information Visualization and Manipulation NPIV'96, In conjunction with Fifth ACM International Conference on Information and Knowledge Management (CIKM'96), (1996), pp. 41-45.

Bajaj, Chandrajit et al. "Web Based Collaboration-Aware Synthetic Environments" Proceedings of the 1997 GVU/NIST TEAMCAD workshop, Atlanta, GA, 1997. 143-150.

Trzyna, Peter K., "Amendment After Final and Request for Reconsideration" filed Jan. 16, 2013, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007. pp. 1-14. USA.

Trzyna, Peter K., "Amendment After Final" filed Feb. 19, 2013, for U.S. Appl. No. 09/399,578, filed Sep. 20, 1999. pp. 1-177. USA.

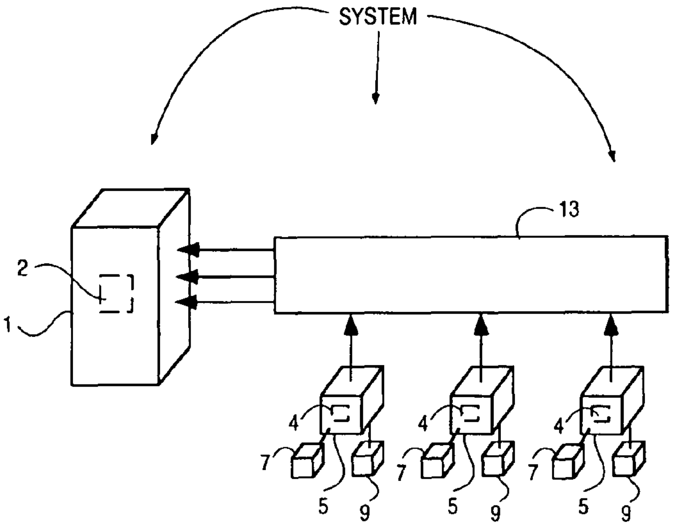
Trzyna, Peter K., "Amendment and Request for Reconsideration" filed Jul. 16, 2012, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006. pp. 1-32. USA.

T. Socolofsky et al., Request for Comments (RFC) 1180: A TCP/IP Tutorial, Network Working Group, Jan. 1991, pp. 1-29.

Paul Tarau et al., LogiMOO: an Extensible Multi-User Virtual World with Natural Language Control, The Journal of Logic Programming, 1993, vol. 12, pp. 1-23.

* cited by examiner

FIG. 1



COMMUNICATIONS OVERVIEW

FIG. 2

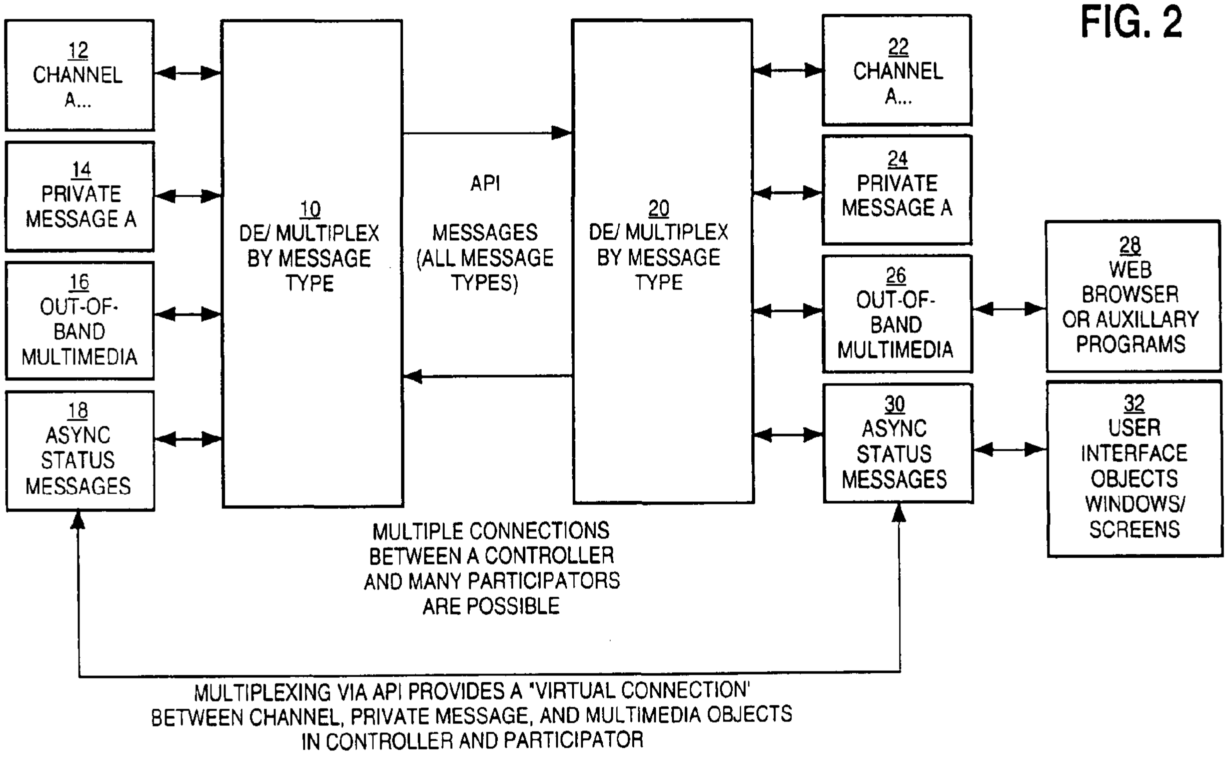

12 CHANNEL A...
14 PRIVATE MESSAGE A
16 OUT-OF-BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DE/ MULTIPLEX BY MESSAGE TYPE
API MESSAGES (ALL MESSAGE TYPES)
20 DE/ MULTIPLEX BY MESSAGE TYPE
22 CHANNEL A...
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILLARY PROGRAMS
32 USER INTERFACE OBJECTS WINDOWS/ SCREENS
MULTIPLE CONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A 'VIRTUAL CONNECTION' BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

FIG. 3

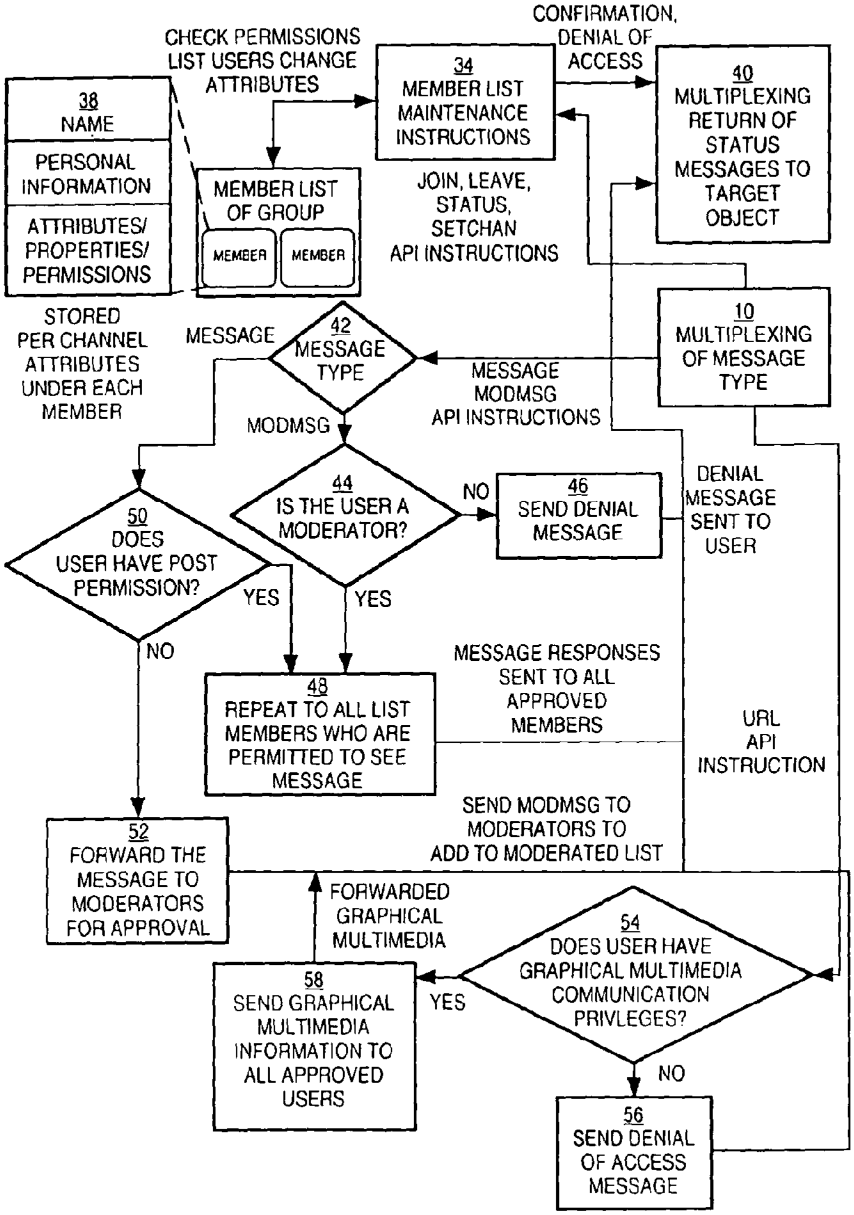

CHECK PERMISSIONS LIST USERS CHANGE ATTRIBUTES
CONFIRMATION, DENIAL OF ACCESS
34 MEMBER LIST MAINTENANCE INSTRUCTIONS
40 MULTIPLEXING RETURN OF STATUS MESSAGES TO TARGET OBJECT
38 NAME
PERSONAL INFORMATION
ATTRIBUTES/ PROPERTIES/ PERMISSIONS
MEMBER LIST OF GROUP
MEMBER
MEMBER
JOIN, LEAVE, STATUS, SETCHAN API INSTRUCTIONS
STORED PER CHANNEL ATTRIBUTES UNDER EACH MEMBER
MESSAGE
42 MESSAGE TYPE
10 MULTIPLEXING OF MESSAGE TYPE
MESSAGE MODMSG API INSTRUCTIONS
MODMSG
44 IS THE USER A MODERATOR?
NO
46 SEND DENIAL MESSAGE
DENIAL MESSAGE SENT TO USER
50 DOES USER HAVE POST PERMISSION?
YES
YES
NO
48 REPEAT TO ALL LIST MEMBERS WHO ARE PERMITTED TO SEE MESSAGE
MESSAGE RESPONSES SENT TO ALL APPROVED MEMBERS
URL API INSTRUCTION
SEND MODMSG TO MODERATORS TO ADD TO MODERATED LIST
52 FORWARD THE MESSAGE TO MODERATORS FOR APPROVAL
FORWARDED GRAPHICAL MULTIMEDIA
54 DOES USER HAVE GRAPHICAL MULTIMEDIA COMMUNICATION PRIVLEGES?
YES
58 SEND GRAPHICAL MULTIMEDIA INFORMATION TO ALL APPROVED USERS
NO
56 SEND DENIAL OF ACCESS MESSAGE

FIG. 4

CENTRAL CONTROLLER LOOP COMMUNICATIONS

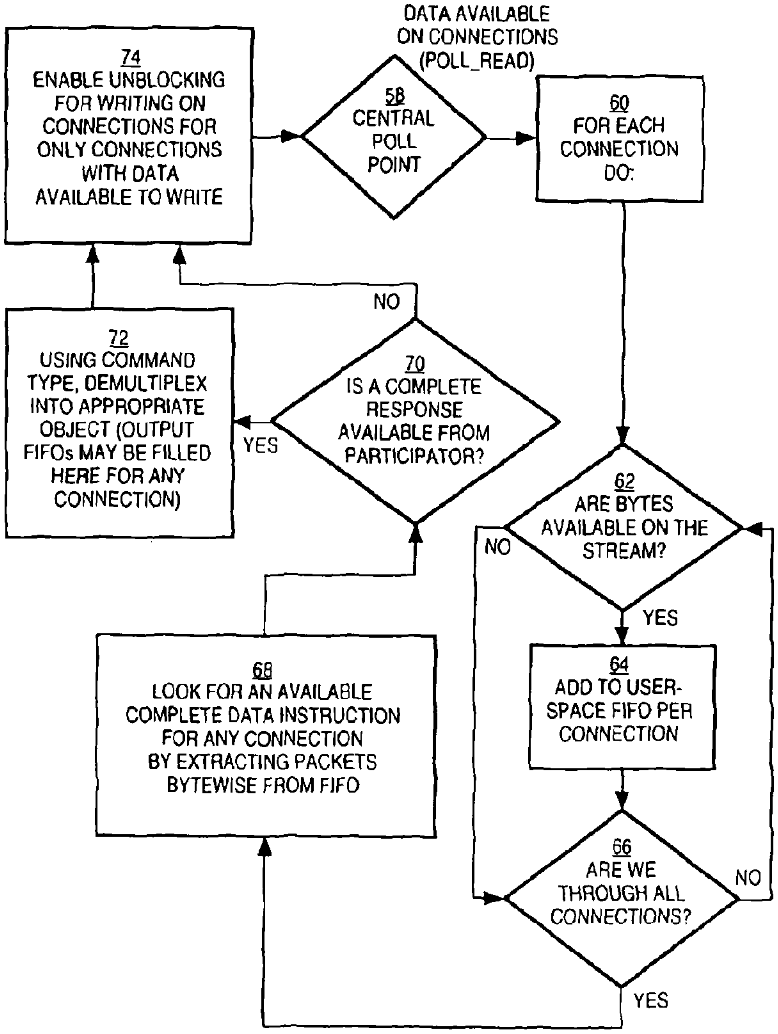

DATA AVAILABLE ON CONNECTIONS (POLL_READ)
74 ENABLE UNBLOCKING FOR WRITING ON CONNECTIONS FOR ONLY CONNECTIONS WITH DATA AVAILABLE TO WRITE
58 CENTRAL POLL POINT
60 FOR EACH CONNECTION DO:
NO
72 USING COMMAND TYPE, DEMULTIPLEX INTO APPROPRIATE OBJECT (OUTPUT FIFOs MAY BE FILLED HERE FOR ANY CONNECTION)
YES
70 IS A COMPLETE RESPONSE AVAILABLE FROM PARTICIPATOR?
62 ARE BYTES AVAILABLE ON THE STREAM?
NO
YES
64 ADD TO USER-SPACE FIFO PER CONNECTION
68 LOOK FOR AN AVAILABLE COMPLETE DATA INSTRUCTION FOR ANY CONNECTION BY EXTRACTING PACKETS BYTEWISE FROM FIFO
66 ARE WE THROUGH ALL CONNECTIONS?
NO
YES

FIG. 5

CLIENT CHANNEL DATA STRUCTURE AND INFORMATION FLOW DIAGRAM

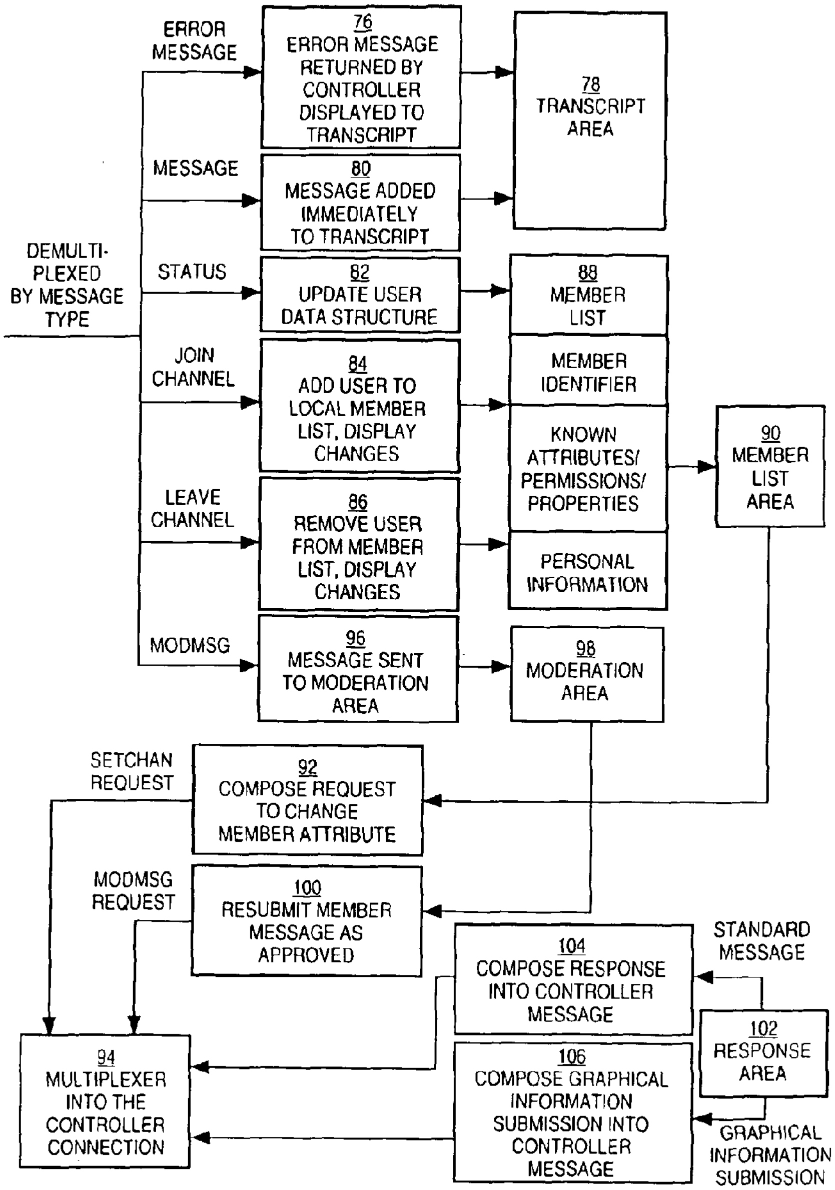

ERROR MESSAGE
76 ERROR MESSAGE RETURNED BY CONTROLLER DISPLAYED TO TRANSCRIPT
78 TRANSCRIPT AREA
MESSAGE
80 MESSAGE ADDED IMMEDIATELY TO TRANSCRIPT
DEMULTI-PLEXED BY MESSAGE TYPE
STATUS
82 UPDATE USER DATA STRUCTURE
88 MEMBER LIST
JOIN CHANNEL
84 ADD USER TO LOCAL MEMBER LIST, DISPLAY CHANGES
MEMBER IDENTIFIER
KNOWN ATTRIBUTES/ PERMISSIONS/ PROPERTIES
90 MEMBER LIST AREA
LEAVE CHANNEL
86 REMOVE USER FROM MEMBER LIST, DISPLAY CHANGES
PERSONAL INFORMATION
MODMSG
96 MESSAGE SENT TO MODERATION AREA
98 MODERATION AREA
SETCHAN REQUEST
92 COMPOSE REQUEST TO CHANGE MEMBER ATTRIBUTE
MODMSG REQUEST
100 RESUBMIT MEMBER MESSAGE AS APPROVED
104 COMPOSE RESPONSE INTO CONTROLLER MESSAGE
STANDARD MESSAGE
102 RESPONSE AREA
94 MULTIPLEXER INTO THE CONTROLLER CONNECTION
106 COMPOSE GRAPHICAL INFORMATION SUBMISSION INTO CONTROLLER MESSAGE
GRAPHICAL INFORMATION SUBMISSION

FIG. 6

PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM

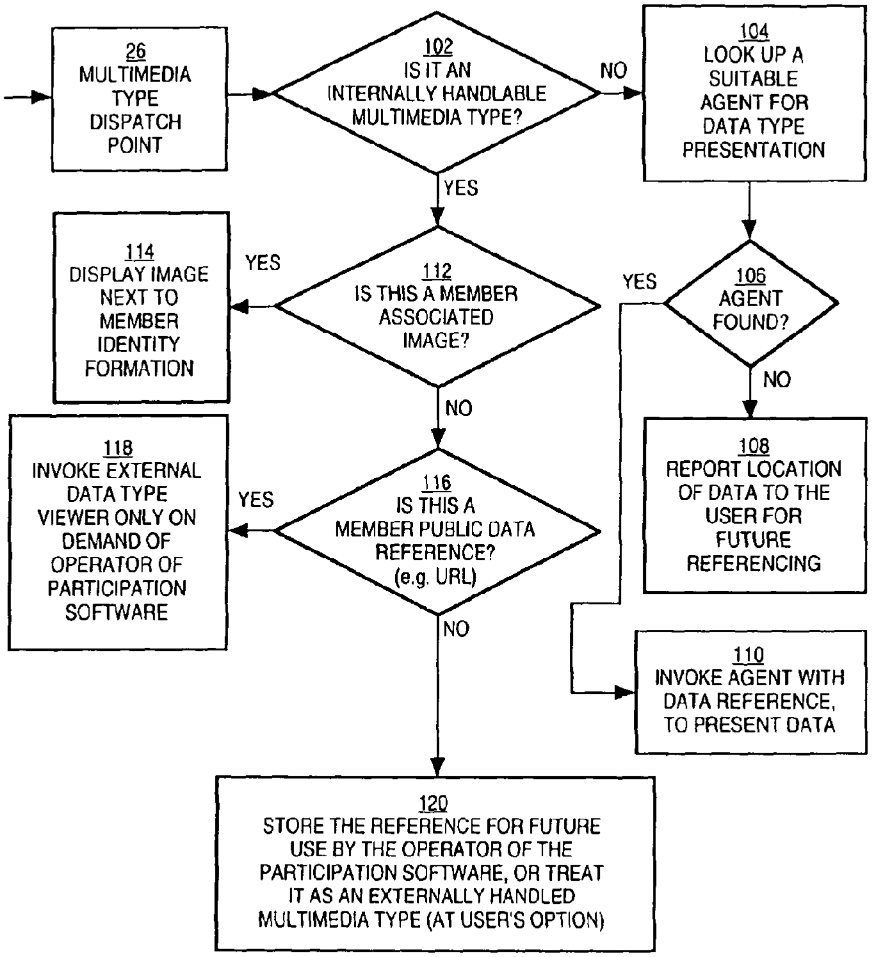
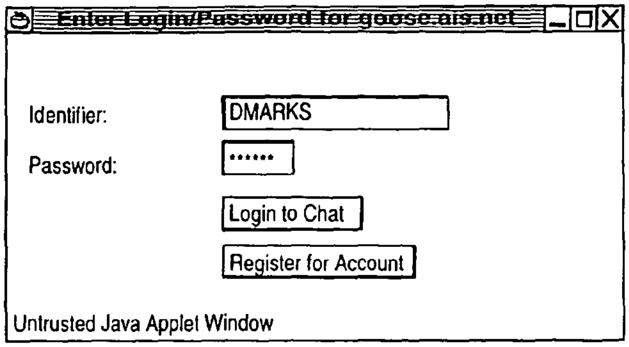

26
MULTIMEDIA TYPE DISPATCH POINT
102
IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104
LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114
DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112
IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106
AGENT FOUND?
NO
NO
118
INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116
IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
108
REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
NO
110
INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120
STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

FIG. 7



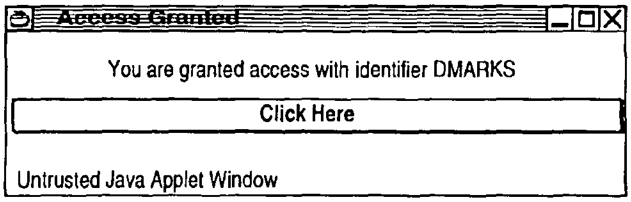
Enter Login/Password for goose.ais.net

Identifier: DMARKS

Password: ••••••

Untrusted Java Applet Window

FIG. 8

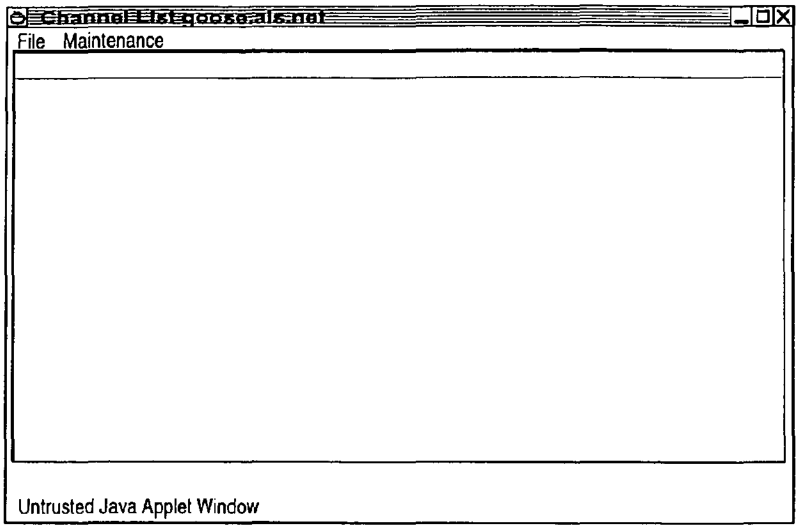


Access Granted

You are granted access with identifier DMARKS

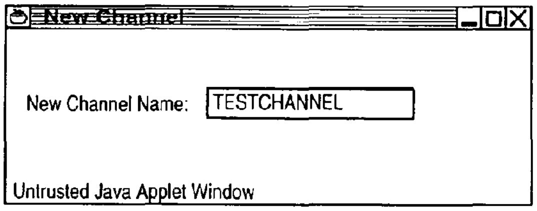
Untrusted Java Applet Window

FIG. 9



Untrusted Java Applet Window

FIG. 10



New Channel Name: TESTCHANNEL

Untrusted Java Applet Window

FIG. 11

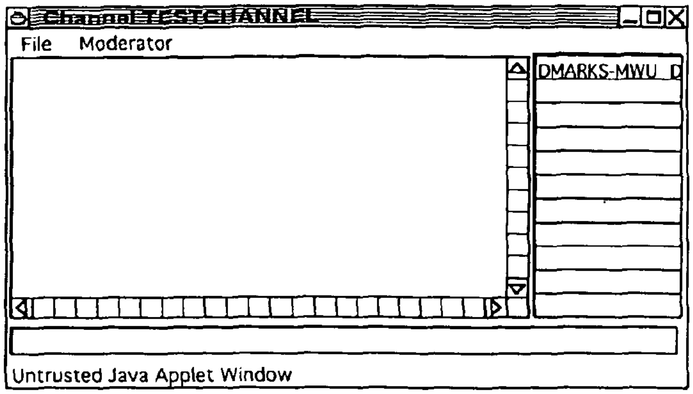

Channel TESTCHANNEL
File
Moderator
DMARKS-MWU D
Untrusted Java Applet Window

FIG. 12

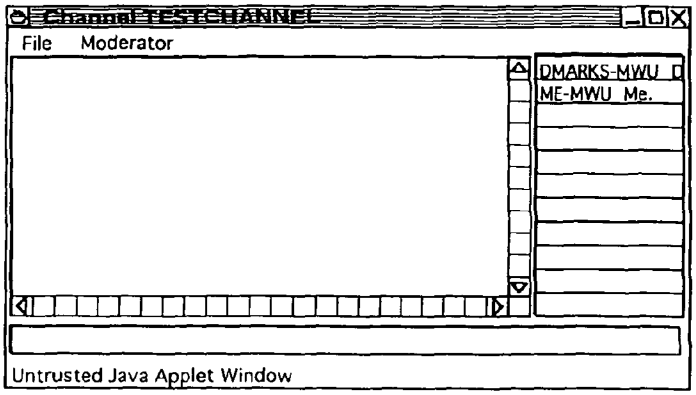
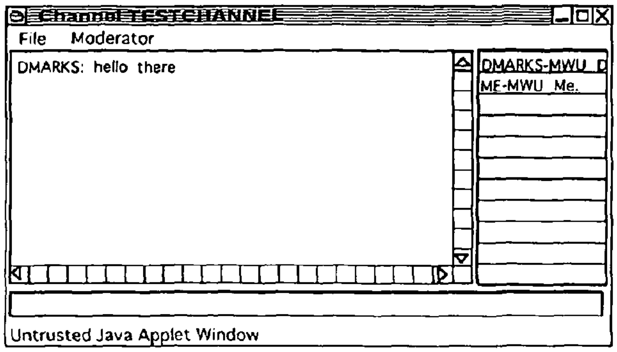
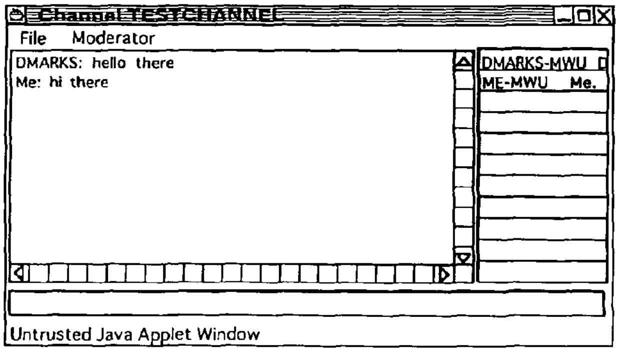

Channel TESTCHANNEL
File
Moderator
DMARKS-MWU D
ME-MWU Me.
Untrusted Java Applet Window

FIG. 13



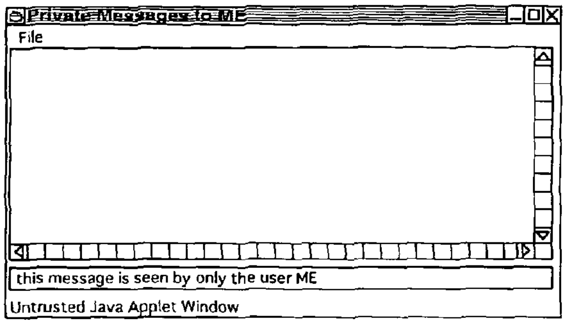
DMARKS: hello there

FIG. 14



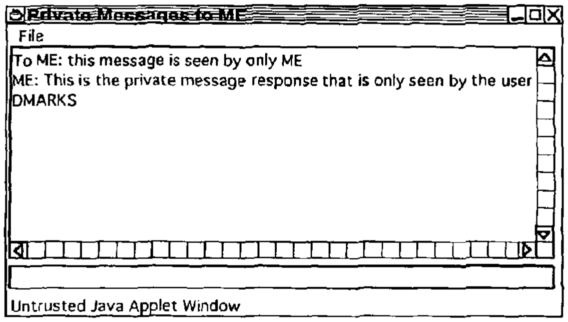
DMARKS: hello there
Me: hi there

FIG. 15



this message is seen by only the user ME

FIG. 16



To ME: this message is seen by only ME
ME: This is the private message response that is only seen by the user DMARKS

FIG. 17

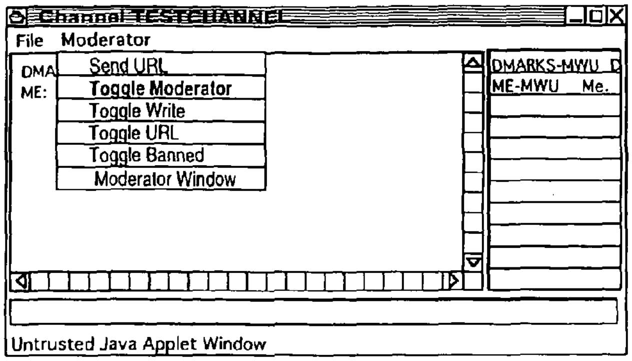
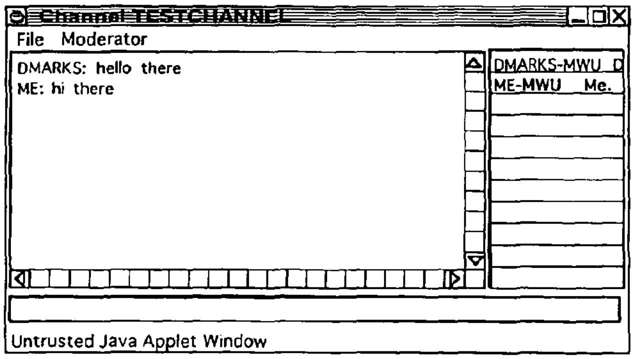
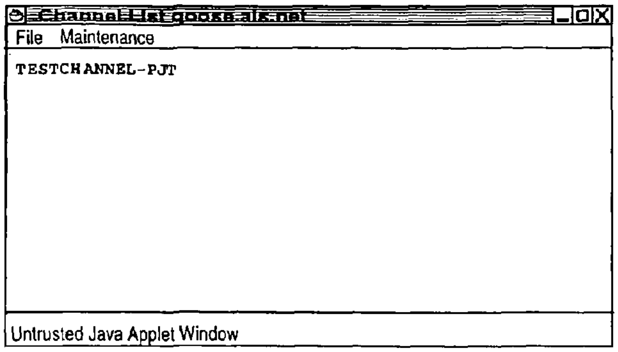


FIG. 18



DMARKS: hello there
ME: hi there

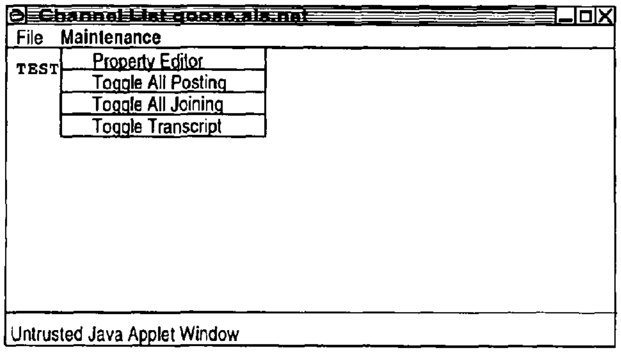
FIG. 19



TESTCHANNEL-PJT

Untrusted Java Applet Window

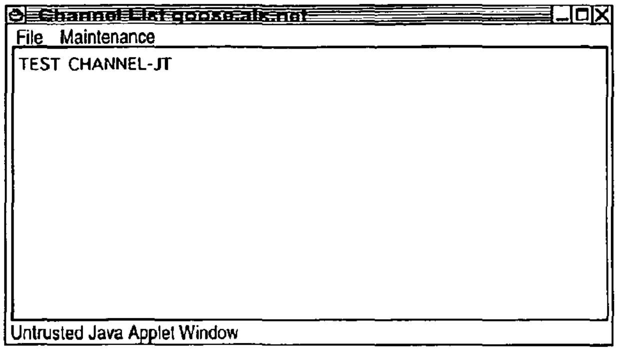
FIG. 20



TEST

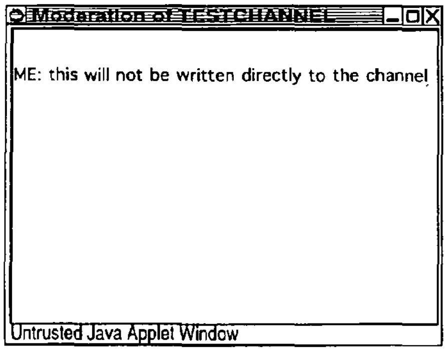
Untrusted Java Applet Window

FIG. 21



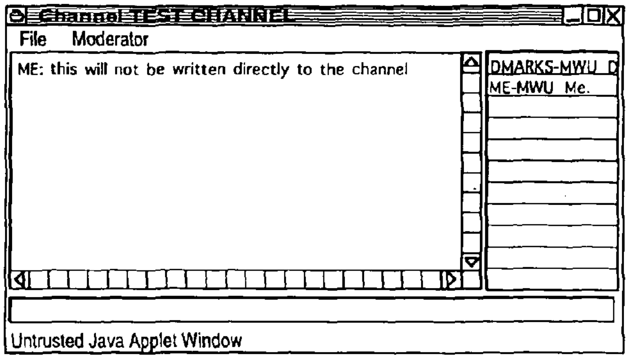
TEST CHANNEL-JT

FIG. 22



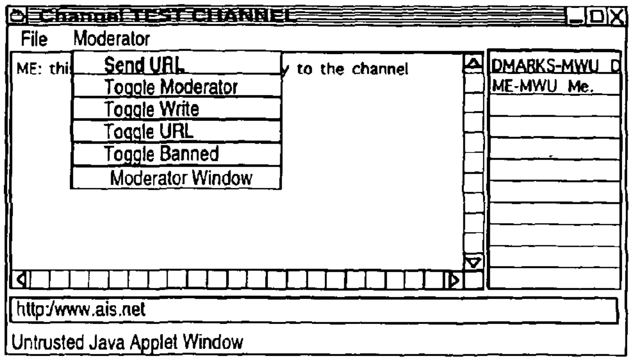
ME: this will not be written directly to the channel

FIG. 23



ME: this will not be written directly to the channel

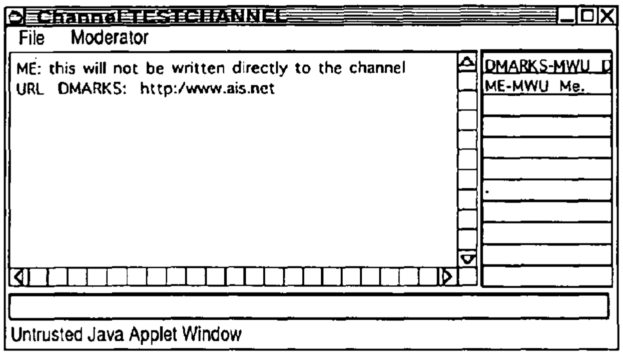
FIG. 24



ME: thi y to the channel

http:/www.ais.net

FIG. 25

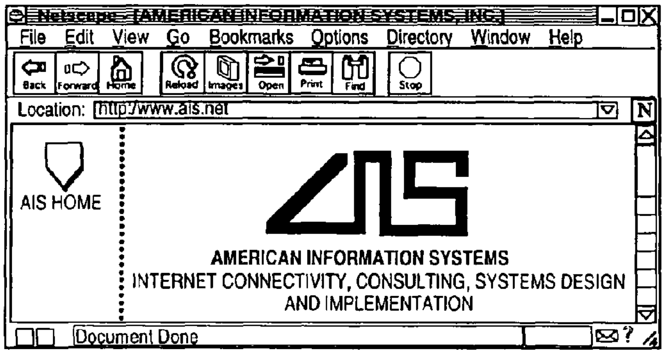


ME: this will not be written directly to the channel
URL DMARKS: http:/www.ais.net

DMARKS-MWU D
ME-MWU Me.

Untrusted Java Applet Window

FIG. 26



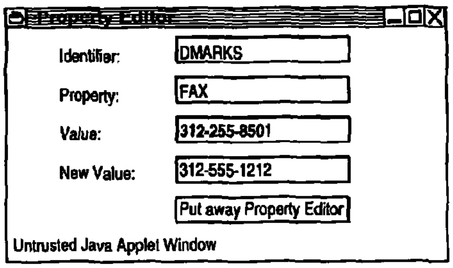
Location: http:/www.ais.net

AIS HOME

AMERICAN INFORMATION SYSTEMS
INTERNET CONNECTIVITY, CONSULTING, SYSTEMS DESIGN AND IMPLEMENTATION

Document Done

FIG. 27



Property Editor

Identifier: DMARKS

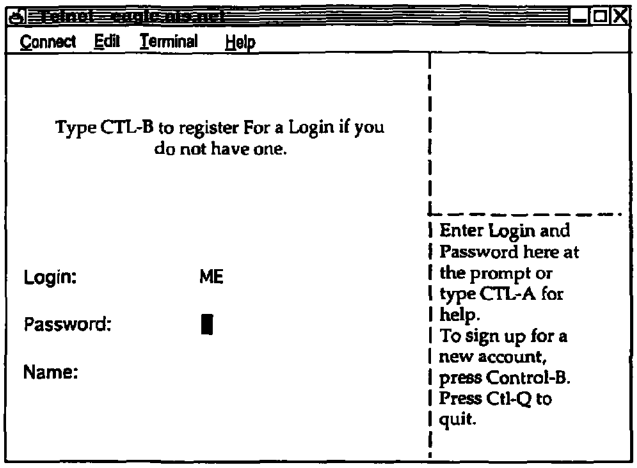
Property: FAX

Value: 312-255-8501

New Value: 312-555-1212

Untrusted Java Applet Window

FIG. 28



Type CTL-B to register For a Login if you do not have one.

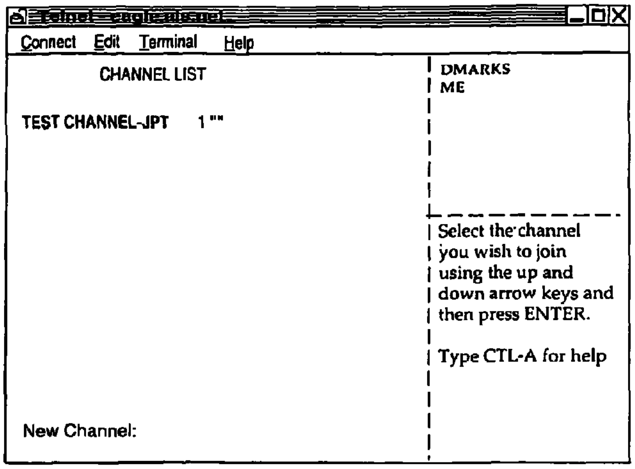
Login: ME

Password: ▮

Name:

Enter Login and Password here at the prompt or type CTL-A for help.
To sign up for a new account, press Control-B.
Press Ctl-Q to quit.

FIG. 29



CHANNEL LIST

TEST CHANNEL-JPT 1 ""

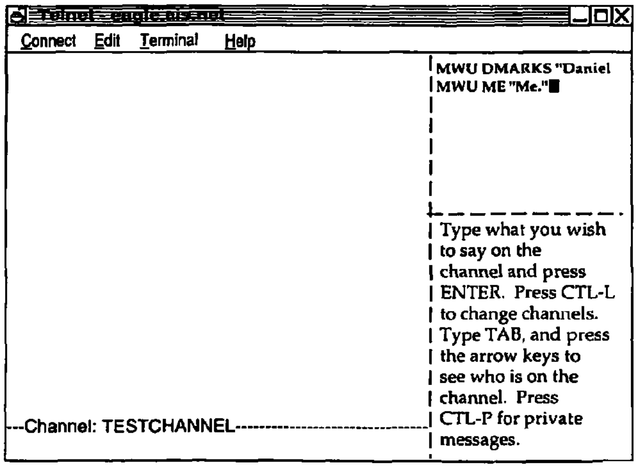
New Channel:

DMARKS
ME

Select the channel you wish to join using the up and down arrow keys and then press ENTER.

Type CTL-A for help

FIG. 30

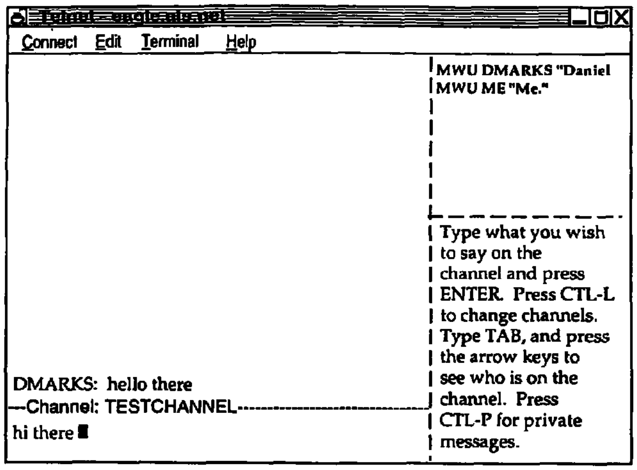


MWU DMARKS "Daniel
MWU ME "Me."█

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

---Channel: TESTCHANNEL---------------------------------

FIG. 31

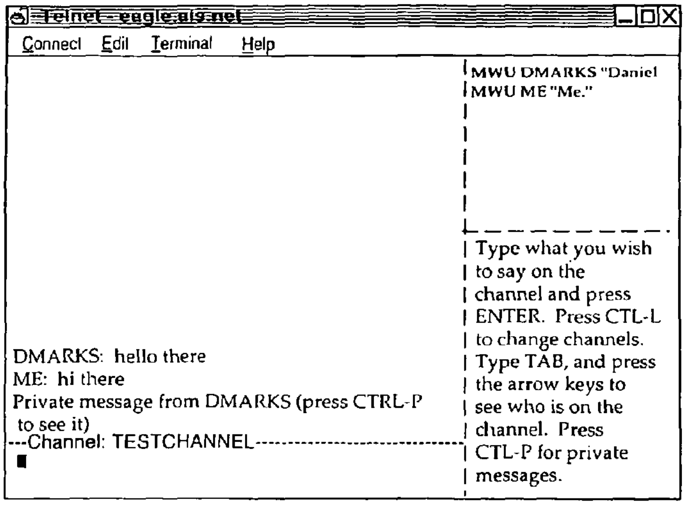


```
MWU DMARKS "Daniel
MWU ME "Me."
```

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

```
DMARKS:  hello there
—Channel: TESTCHANNEL----------------------------
hi there ▮
```

FIG. 32

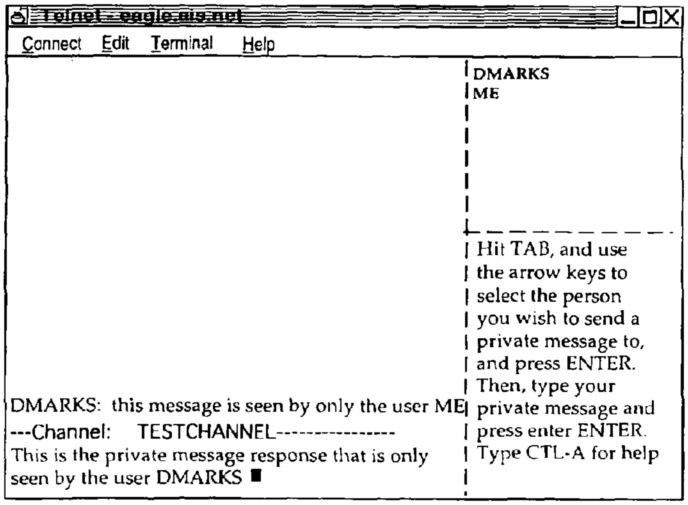


```
MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish
to say on the
channel and press
ENTER. Press CTL-L
to change channels.
Type TAB, and press
the arrow keys to
see who is on the
channel. Press
CTL-P for private
messages.

DMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P
 to see it)
---Channel: TESTCHANNEL-------------------------------
■
```

FIG. 33

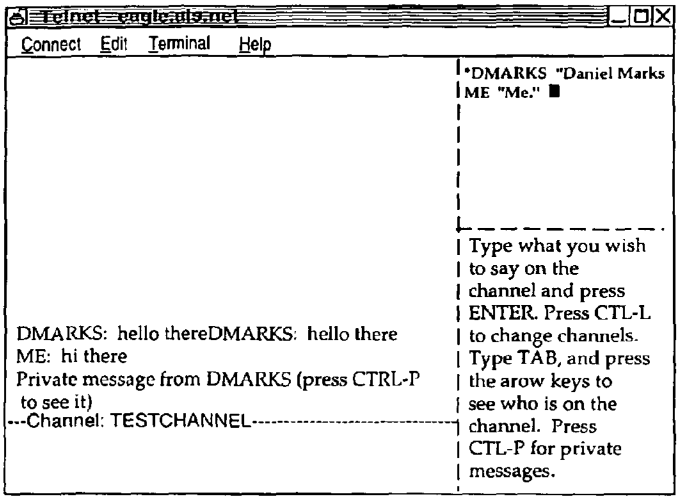


```
DMARKS
ME

Hit TAB, and use
the arrow keys to
select the person
you wish to send a
private message to,
and press ENTER.
Then, type your
private message and
press enter ENTER.
Type CTL-A for help

DMARKS: this message is seen by only the user ME
---Channel:    TESTCHANNEL----------------
This is the private message response that is only
seen by the user DMARKS ■
```

FIG. 34



```
                                                    |*DMARKS  "Daniel Marks
                                                    |ME  "Me."  ■
                                                    |
                                                    |
                                                    |
                                                    |
                                                    |
                                                    L- - - - - - - - -
                                                    | Type what you wish
                                                    | to say on the
                                                    | channel and press
                                                    | ENTER. Press CTL-L
DMARKS:  hello thereDMARKS:  hello there            | to change channels.
ME:  hi there                                       | Type TAB, and press
Private message from DMARKS (press CTRL-P           | the arow keys to
 to see it)                                         | see who is on the
---Channel: TESTCHANNEL-----------------------------| channel.  Press
                                                    | CTL-P for private
                                                    | messages.
```

# REAL TIME COMMUNICATIONS SYSTEM

## I. PRIORITY DATA

The present patent application is a continuation of and incorporates by reference U.S. patent application Ser. No. 09/399,578 filed by the same inventor on Sep. 20, 1999, as well as U.S. patent application Ser. No. 08/617,658, issuing as U.S. Pat. No. 5,956,491, on Sep. 21, 1999, titled Group Communications Multiplexing System that was filed by the same inventor on Apr. 1, 1996. U.S. patent application Ser. No. 09/399,578, filed Sep. 20, 1999, is a continuation of U.S. patent application Ser. No. 08/617,658, filed Apr. 1, 1996, issuing as U.S. Pat. No. 5,956,491, on Sep. 21, 1999.

## II. FIELD OF INVENTION

This invention is directed to an apparatus, a manufacture, and methods for making and using the same, in a field of digital electrical computer systems. More particularly, the present invention is directed to a digital electrical computer system involving a plurality of participator computers linked by a network to at least one of a plurality of participator computers, the participator computers operating in conjunction with the controller computer to handle multiplexing operations for communications involving groups of some of the participator computers.

## III. BACKGROUND OF THE INVENTION

Multiplexing group communications among computers ranges from very simple to very complex communications systems. At a simple level, group communications among computers involves electronic mail sent in a one way transmission to all those in a group or subgroup using, say, a local area network. Arbitrating which computers receive electronic mail is a rather well understood undertaking.

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

Even more complex is linking of computers to communicate in what has become known as a "chat room." Chat room communications can be mere text, such as that offered locally on a file server, or can involve graphics and certain multimedia capability, as exemplified by such Internet service providers as America On Line. Multiplexing in multimedia is more complex for this electronic environment.

On the Internet, "chat room" communications analogous to America On Line have not been developed, at least in part because Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications. Further, unlike the an Internet service provider, which has control over both the hardware platform and the computer program running on the platform to create the "chat room", there is no particular control over the platform that would be encountered on the Internet. Therefore, development of multiplexing technology for such an environment has been minimal.

Even with an emergence of the World Wide Web, which does have certain graphical multimedia capability, sophisticated chat room communication multiplexing has been the domain of the Internet service providers. Users therefore have a choice between the limited audience of a particular Internet Service provider or the limited chat capability of the Internet.

## IV. SUMMARY OF THE INVENTION

It is an object of the present invention to overcome such limitations of the prior art and to advance and improve the

technology of group computer multiplexing to enable better computerized group communications.

It is another object of the present invention to provide a computerized human communication arbitrating and distributing system.

It is yet another object of the present invention to provide a group communication multiplexing system involving a controller digital computer linked to a plurality of participator computers to organize communications by groups of the participator computers.

It is still another object of the present invention to link the controller computer and the plurality of computers with respective software coordinated to arbitrate multiplexing activities.

It is still a further object of the present invention to provide a chat capability suitable for handling graphical, textual, and multimedia information in a platform independent manner.

These and other objects and utilities of the invention, which apparent from the discussion herein, are addressed by a computerized human communication arbitrating and distributing system. The system includes a controller digital electrical computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information and an output device for presenting information to a user having a user identity. A connection such as the Internet links the controller computer with each of the participator computers.

Controller software runs on the controller computer, programming the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups communicating through the controller computer and to distribute real time data to the respective ones of the groups.

Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message. The controller computer also conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

Therefore, for a computer system involving a plurality of programmed participator computers running the participator computer program can interact through a programmed controller computer with the controller computer multiplexing the communications for groups formed from the plurality, as well as arbitrating communications behavior.

## V. BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a depiction of hardware suitable for performing the present invention;

FIG. **2** is a communications overview of the present invention.

FIG. **3** is a data and communications dependency diagram for the controller group channel structure of the present invention.

FIG. **4** is a flow chart of the central controller loop communications for the controller computer.

FIG. **5** is a client channel data structure and information flow diagram of the present invention.

FIG. **6** is a participator software out-of-band multimedia information flow diagram of the present invention.

FIG. **7** is an illustration of a login/password screen of the present invention.

FIG. **8** is an illustration of a confirmation screen of the present invention.

FIG. **9** is an illustration of a channel list area screen of the present invention.

FIG. **10** is an illustration of a New Channel option pull-down menu screen of the present invention.

FIG. **11** is an illustration of a member on a new channel screen of the present invention.

FIG. **12** is an illustration of a second member on the new channel screen of the present invention.

FIG. **13** is an illustration of a communication on the new channel screen of the present invention.

FIG. **14** is an illustration of a private message window on the new channel screen of the present invention.

FIG. **15** is an illustration of a private message displayed on the private message window on the new channel screen of the present invention.

FIG. **16** is a further illustration of the private message on the private message window on new channel screen of the present invention.

FIG. **17** is an illustration of an attribute revocation on the new channel screen of the present invention.

FIG. **18** is a further illustration of the new channel screen of the present invention.

FIG. **19** is an illustration of the channel list window screen of the present invention.

FIG. **20** is an illustration of the toggle posting option on a screen of the present invention.

FIG. **21** is an illustration of a moderated version of the new channel screen of the present invention.

FIG. **22** is an illustration of a communication on a moderation window screen of the present invention.

FIG. **23** is an illustration of the communication passed on to the moderated version of the new channel screen of the present invention.

FIG. **24** is an illustration of a communication, for sending a graphical multimedia message, on to the moderated version of the new channel screen of the present invention

FIG. **25** is an illustration of a communication, for passing a URL (Uniform Resource Locator) to channel members, on a moderator pull-down menu screen of the present invention.

FIG. **25** is an illustration, showing the name of the URL, on a moderated version of the new channel screen of the present invention.

FIG. **26** is an illustration of data associated with the graphical multimedia message on a moderated version of the new channel screen of the present invention.

FIG. **27** is an illustration of a proprietary editor, suitable for a dialog to change tokens, on a screen of the present invention.

FIG. **28** is an illustration of a text-based interface login/password screen of the present invention.

FIG. **29** is an illustration of a text-based interface group screen of the present invention.

FIG. **30** is another illustration of a text-based interface group screen of the present invention.

FIG. **31** is another illustration of a text-based interface group screen of the present invention.

FIG. **32** is an illustration of a text-based interface private message screen of the present invention.

FIG. **33** is another illustration of a text-based interface private message screen of the present invention.

FIG. **34** is another illustration of a text-based interface group with moderator screen of the present invention.

## VI. DETAILED DESCRIPTION OF THE DRAWINGS

In providing a detailed description of a preferred embodiment of the present invention, reference is made to an appendix hereto, including the following items.

### APPENDIX CONTENTS

ALLUSER C
ALLUSER H
CHANNEL C
CHANNEL H
CHANNEL HLP
CLIST C
CLIST H
CLIST HLP
EDITUSER C
EDITUSER H
ENTRYFRM C
ENTRYFRM H
ENTRYFRM HLP
HELP C
HELP H
HELPSCR C
HELPSCR H
LINEEDIT C
LINEEDIT H
LIST C
LIST H
LOGIN HLP
MAIN C
MAKEFILE
MESSAGE C
MESSAGE H
MODERAT HLP
PRIVATE C
PRIVATE H
PRIVATE HLP
SOCKIO C
SOCKIO H
STR C
STR H
UCCLIENT
USER C
USER H
WINDOW C
WINDOW H

Note that the appendix includes code for two different embodiments: a Tellnet embodiment and a JAVA embodiment. Documentation and error messages, help files, log files, are also included in the appendix. While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled.

Referring now to FIG. **1**, the overall functioning of a computerized human communication arbitrating and distributing System **1** of the present invention is shown with odd numbers designating hardware or programmed hardware, and even numbers designating computer program logic and data flow. The System **1** includes a digital Controller Computer **3**, such as an Internet service provider-type computer. The Controller Computer **3** is operating with an operating system.

System **1** also includes a plurality of digital Participator Computers **5**, each of which may be an IBM-compatible personal computer with a processor and a DOS operating system. Each of the Participator Computers **5** includes an Input Device **7** for receiving human-input information from a respective human user. The Input Device **7** can be, for example, a keyboard, mouse or the like. Each of the Participator Computers **5** also includes an Output Device **9** for presenting information to the respective user. The Output Device **9** can be a monitor, printer (such as a dot-matrix or laser printer), or preferably both are used. Each of the Participator Computers **5** also includes a Memory **11**, such as a disk storage means.

The System **1** includes a Connection **13** located between, so as to link, the Controller Computer **3** with each of the Participator Computers **5**. The Connection **13** can be an Internet or more particularly, a World Wide Web connection.

The Controller Computer **3** is running and under the control of Controller Software **2**, which directs the Controller Computer **3** to arbitrate in accordance with predefined rules including a user identity, which ones of the Participator Computers **5** can interact in one of a plurality of groups through the Controller Computer **3** and to distribute real time data to the respective ones of the groups.

The Participator Computers **5** are each running and under the control of Participator Software **4**, which directs each of the Participator Computers **5** to handle a user Interface **6** permitting one said user to send a multimedia information Message **8** to the Controller Computer **3**, which arbitrates which of the Participator Computers **5** receives the multimedia information Message **8** and which conveys the multimedia information Message **8** to the selected participator computers **5** to present the multimedia information Message **8** to the respective user.

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**.

Turning now to FIG. **2**, there is shown a communications overview of the present invention. Beginning with the Controller Computer Software **2**, reference is made to Block **10**, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **10** links to Block **12**, which is illustrative of channel A . . . . Block **10** also links to Block **14**, which illustrates handling private message A. Block **10** also links to Block **16**, illustrative of handling out-of-band media. Block **10** additionally links to Block **18**, which illustrates asynchronous status messages.

Multiple connections between the controller computer **3** and a plurality of participator computers **5** permit communication implemented via the interplay of controller software **2** and participator software **4**. With particular regard to the participator software **4** illustrated in FIG. **2**, Block **20** is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **20** links to Block **22**, which is illustrative of channel A . . . . Block **20** also links to Block **24**, which illustrates handling private message A. Block **20** also links to Block **26**, illustrative of handling out-of-band media via Block **28**, which is illustrative of a Web browser or auxiliary computer program. Block **20** also links to Block **30**, which illustrates asynchronous status message handling via Block **32**, illustrative of user interface objects windows and screens.

De/multiplexing via API provides a "virtual connection" between Channel, Private Message, and Multimedia objects in the controller computer **3** and each participator computer **5**. An alternate architecture is to allow for a separate connection between each object so that multiplexing/demultiplexing is not necessary and each object handles its own connection. This would influence system performance, however.

Turning now to FIG. **3**, a data and communications dependency diagram controller group channel structure is illustrated. Beginning from what is designated as a portion of Block **10** the logic flows to Block **34** to consider JOIN, LEAVE, STATUS, SETCHAN API instructions. Block **34** examines member list maintenance instructions, accessing Block **36** to check permissions, list users, and change attributes. Note the exploded window **38** shows a display of member information including a user's name, personal information, and attributes/properties/permissions (operations involving the subsequently discussed tokens), i.e., stored per channel attributes under each member. In any case, confirmation or denial of access is communicated via Block **40** for multiplexing return of status messages to a target object.

From the portion of Block **10**, the logic flows to Block **42** for MESSAGE and MODMSG API instructions. Block **42** tests which of the two instructions were received, and for MODMSG, the logic flows to Block **44**, which tests whether the user is a moderator. If the user is not a moderator, the logic flows to Block **46**, which sends a denial message through Block **40**. If, however, the in Block **44** the user is a moderator, the logic flows to Block **48** for a repeat to all list members who are permitted to see the message, via Block **40**.

Returning to Block **42**, if MESSAGE is detected, the logic flows to Block **50**, which tests whether a user has post permission. If the user has post permission, the logic flows to Block **48**, etc. If the user does not have post permission, the logic flows to Block **52** to forward the message to moderators for approval, via Block **40**.

Additionally, the logic flows from Block **10** to Block **54** for a URL API instruction. Block **54** tests whether the user has graphical multimedia communication privileges, and if not, the logic flows via Block **56**, which sends a denial message via Block **40**. Otherwise, if the user does have graphical multimedia communications privileges in Block **54**, Block **58** sends graphical multimedia information to all approved users via Block **40**.

Turning now to FIG. **4**, central controller loop communications is illustrated. For the data on central poll point **58** (see Appendix POLL_POINT), a "do" loop begins at Block **60** for each connection. Block **62** tests whether bytes are available on the data stream. If they are, the bytes are added to user space FIFO per connection at Block **64**, leading to Block **66**, which tests whether there are any more connections. Note that in FIG. **4**, if there are no more bytes available in Block **62**, the logic skips to Block **66**, and if Block **66** is not finished with all connections, the loop returns to Block **62**. When all connections have been completed in Block **62**, the logic flows to Block **68**, which looks for an available complete data instruction for any connection by extracting packets byte-wise from the FIFO. Thereafter, Block **70** tests whether there is a complete response available from the participator computer. If the response is complete, the logic flows to Block **72** which, using a command type, demultiplexes into an appropriate object (output FIFOs may be filled here for any connection). The logic from Block **72** joins the "no" branch from Block **70** at Block **74**, which enables unblocking for writing connections for only connections with data available to write, looping back to Block **58**.

FIG. **5** shows a client channel data structure and information flow diagram. From a message that is demultiplexed by message type, there are six possibilities: ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG. ERROR MESSAGE is communicated to Block **76**, where the error message is displayed to the transcript in the transcript area of Block **80**. MESSAGE is communicated to Block **78** where the message is immediately added to the transcript in transcript area **78**. STATUS is communicated to Block **82** to update user data structure; JOINCHANNEL is communicated to Block **84** to remove a user from the member list and display the change; and LEAVECHANNEL is communicated to Block **86**. From Block **82**, Block **84**, and Block **88**, the logic flows to Block **88**, which includes a member list, a member identifier, known attributes/permissions/properties, and personal information. From Block **88**, the logic proceeds to Block **90**, a member list area, and on to Block **92** to compose a request to change a member attribute. This "SETCHAN request is then communicated to Block **94**, which is the multiplexer leading to the controller computer connection.

MODMSG is communicated to Block **96**, which sends the message to the moderation area of Block **98**, and then to Block **100** to resubmit a member message as approved, thereby conveying a MODMSG request to Block **94**.

Note that a response is prepared in the response area of Block **102**. If the response is a standard message, it is conveyed to Block **104** to compose the response into a controller message, thereby sending a MESSAGE request to box **94**. If, however, the message is a graphical information submission, the logic flows from Block **102** to Block **106** to compose the graphical information submission into a controller message, thereby sending a URL request to Block **94**.

FIG. **6** is a participator software out-of-band multimedia information flow diagram, which begins with Block **26**, the multimedia type patch point. Block **26** leads to Block **102**, which tests whether there is an internally handlable multimedia type. If not, Block **104** looks up a suitable agent for data type presentation, which leads to Block **106**, which tests whether an agent was found. If not, Block **108** reports location of data to the user for future referencing. If the agent is found in Block **106**, the logic flows to Block **110**, which invokes the agent with a data reference to present the data.

If the multimedia type is internally handlable from Block **102**, the logic flows to Block **112**, which tests whether this is a member associated image. If it is a member associated image, Block **114** displays the image next to member identity information, and if it is not, the logic flows to Block **116**, which tests if this is a member public data reference (e.g., a URL). 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).

With further regard to the manner of interaction between the controller computer **3** and the participator computers **5**, and their respective computer programs **2** and **4**, includes a moderation capability that is controlled, or arbitrated, pursuant to system **1** recognizing user identity. Note that using the user identity for moderation purposes is a use additional to the use of the user identity for security purposes.

One embodiment of the present invention is to bring chat capability to the internet and World Wide Web. However, another embodiment involves non-internet relay chat. In either embodiment, System **1** is state driven such that synchronous and asynchronous messages can be communicated. For an asynchronous notification, each message is sent through the system **1** (API), which updates the information on the output device of the participator computers **5**. For a synchronous notification, a participator computer **5** must interrogate the system **1** for a message.

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. The control computer database serves as a repository of tokens for other programs to access, thereby affording information to otherwise independent computer systems. In the database, the storage of tokens can be by user, group, and content, and distribution controls can also be placed on the user's tokens as well as the database.

Each token is used to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process. The arbitration also includes controlling a user's ability to moderate communications involving a group or subgroup of the participator computers **5**. Once in a group, temporary tokens are assigned for priority to moderate/submoderate groups (a group is sometimes known as a channel in multiplexing terminology).

Accordingly, tokens are used by the controller computer **5** to control a user's group priority and moderation privileges, as well as controlling who joins the group, who leaves the group, and the visibility of members in the group. Visibility refers to whether a user is allowed to know another user is in the chat group.

Tokens are also used 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.

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

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

With regard to controlling communications in a group (which is in essence a collection of user identities), control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages.

Note that tokens for members in group can involve multiples formed in real time, say, within the span of a conversation. For example, for private communication, tokens are immediately formed to define a group of 2 users. Hierarchical groups within groups can also be formed, with each inheriting the properties of the group before it. Thus, a subgroup can include up to all members or more by adding any surplus to the former group.

With further regard to the controller computer **3**, e.g., a server, information is controlled for distribution to the user interfaces at selected ones of the participator computers **5**. The controller computer program, in one embodiment, can be a resident program interface (such as a JAVA application). There can be a token editor object (window/tear down, etc.) per group, private communication, user, channel listings, user listings, etc. Each can link up in a token hierarchy for arbitration control.

The controller computer **5**, by means of the controller computer program **2**, keeps track of states and asynchronous messages as well as generating a synchronous message as a user logs in or interrogates system **1**.

With regard to multimedia information messages **8**, such messages are of independent data types, e.g., audio/video data types. The content of the message (e.g., a URL) permits the System **1** to automatically determine the handling of the message: either the Controller Computer **3** passes the content of Message **8** directly, or the Controller Computer **3** determines from the Message **8** how to find the content, say via Netscape. Accordingly, Message **8** can communicate video and sound (or other multimedia, e.g., a URL) to users, subject only to the server arbitration controls over what can be sent.

Turning now to an illustration of using the invention, the session starts with verifying the user's identity (at FIG. **7**). The login/password screen is shown, and the user enters his/her assigned login/password combination and clicks the "Login To Chat" button. If the password was entered correctly, a confirmation box appears on the screen.

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

To create a new group, the "New Channel" option is selected from a pull-down menu (at FIG. **9**). The name of the channel is entered by the input device **7**.

If the user has permission (this one does), a new channel is created for the group (at FIG. **10**). The window that displays the channel area has three regions: the bottom region, where responses are entered; the largest region, where a transcript of the communication is followed; and the rightmost region, which lists the group's current members. This list is continuously updated with asynchronously generated status messages received immediately when a new member joins the group. Only "DMARKS" is currently in this group. The "MWU" is the properties currently associated with DMARKS—the ability to moderate, write to the channel, and send multimedia messages.

A new member has joined the channel, and the member list status area is updated right away (at FIG. **11**). This new member has a login of "ME."

The user DMARKS now types "hello there" into the response area and presses RETURN (at FIG. **12**). This message is passed to the controller computer **5**, which sends the message to all channel members, i.e., those using participator computers **5**, including DMARKS.

The user ME now sends a message to the controller: "hi there" (at FIG. **13**). This message is also sent to all members by the controller computer **5**. Now user DMARKS clicks (using input device **7**, a mouse) on the name of the user "ME" in the member list window. The participator software **4** will now create a private message window, so that the users ME and DMARKS can exchange private messages. Private messages are only sent to the intended recipient by the controller, and no one else.

A private message window appears in response to DMARKS's request to open private communications with ME (at FIG. **14**). Now DMARKS types a message into the private message window's response area to ME: "this message is seen only by the user ME." When complete, the participator software **4** will forward this message to the controller computer **3**.

In response, the user ME has entered "This is the private message response that is only seen by the user DMARKS," which has been forwarded to user DMARKS (at FIG. **15**). This message is displayed immediately on DMARKS's window.

DMARKS now returns to the channel window for the group "TESTCHANNEL" (at FIG. **16**). To modify the permission attributes associated with user ME on the channel TEST CHANNEL, DMARKS (who is a moderator of the channel), clicks on the user ME in the member list to select ME, pulls down the Moderator menu, and selects "Toggle Moderator." This removes the moderator privileges from ME.

As a result of the attribute revocation, the "M" has disappeared from next to ME's name in the member list (at FIG. **17**), indicating that the property is no longer associated with the user ME.

Now DMARKS returns to the Channel List window (at FIG. **18**). DMARKS wishes to fully moderate the contents of the channel TESTCHANNEL, censoring all unwanted communications to the channel. DMARKS returns to the channel list, and selects the channel TESTCHANNEL by clicking on its name in the channel list.

Now DMARKS selects the "Toggle All Posting" option in the Maintenance pull-down menu (at FIG. **19**). This will turn off the channel property "posting," (or sending communications to the channel without moderator approval) which will be indicated by the removal of the letter "P" from next to the name TESTCHANNEL (at FIG. **20**).

Now the letter "P" is removed from after the name TESTCHANNEL in the Channel List window (at FIG. **21**), indicating that this channel is now moderated and will only have free posting ability by designated members.

Now, type user ME (who is also on channel TESTCHANNEL) wishes to send communications: "this will not be written directly to the channel" (at FIG. **22**). The controller, instead of sending it immediately to the channel to be seen by all members, will instead forward the message to the moderators for approval. The moderator, DMARKS, will then see the message on the Moderation Window, which provides a preview of any messages to be sent. To approve a message for general viewing, DMARKS now clicks on the message.

Now that DMARKS has clicked directly on the message, it is displayed inside the group's Channel window for all members to see (at FIG. **23**).

DMARKS now wishes to send a graphical multimedia message. This implementation sends graphical multimedia images by allowing a channel member to specify an Internet URL of a graphical multimedia resource to be presented to the group members. In this example, DMARKS wishes to send the URL "http://www.ais.net" (corresponding to the World Wide Web home page of American Information Systems, Inc.) to the channel members. DMARKS enters the URL into the response window, and selects "Send URL" from the Moderator pull-down menu (at FIG. **24**).

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.

Finally, DMARKS wishes to manually modify the attribute tokens associated with the user (at FIG. **27**). The user invokes the Property Editor dialog, which allows the user to view and change the tokens associated with a user. A property of a given user is determined by the Identifier and Property names. An old value of the property is shown, and a token value can be changed in the "New Value" field. With this property editor, a user with sufficient permissions (tokens) can change any of the tokens or security parameters of any user, or a user's ability to change security parameters can be restricted.

To start with an alternate embodiment using a text-based interface, a user is presented by the login/password screen (at FIG. **28**). This screen is where a user enters the information that proves his/her identity. The user must now enter his/her login and password to identify themselves.

After the user has been identified by the controller the Channel List screen appears (at FIG. **29**). The names of channels and their associated properties are shown on this screen. By using the arrow keys and highlighting the desired channel, ME may enter any publicly joinable group. Currently, there is only one group TESTCHANNEL, which ME will join.

Now the screen for the channel TESTCHANNEL appears (at FIG. **29**). The screen is split into four regions. The bottom left region is the response line, where messages users wish to enter appear. The upper left region is the transcript area where the communications of the group's channel appear as they occur. The upper right region is the Member List region, where a continuously updated list of members' names appear, with their attributes.

A message appears in the transcript area. The controller has forwarded a message to the group from DMARKS, "hello there" (at FIG. **31**), which is seen by all members of the group, including ME. Now ME will respond, by entering "hi there" into the response area.

When ME is finished entering his response, the participator software forwards the response to the controller, which sends it to the members of the channel. In the transcript area, the participator software notifies the user that it has received a private message from DMARKS, which is waiting inside the private message screen. To see the private message, ME presses the private message screen hot key.

A private message screen appears (at FIG. **32**), and the private message from DMARKS is at the bottom of the transcript area. Now to reply, ME types his response into the response area.

Now ME will return to the screen for the channel TESTCHANNEL. The member list area has changed because DMARKS has revoked ME's moderator permission. ME is no longer permitted to see the permissions of other users, so this information has been removed from his display (at FIG. **33**). The only information he can see now is who is moderator (at FIG. **34**). A "*" next to the identifier of a member of the group indicates the member is a moderator of the group. ME is no longer a moderator, and therefore a "*" does not appear the identifier ME.

To further exemplify the use of the present invention, the following is a transcript of communications produced in accordance herewith.

POWERQUALITY JOHNMUNG: unclear about meaning of "first contingency"
POWERQUALITY SAM: mike, that is correct on IEEE 519
POWERQUALITY SKLEIN: In assessing network security (against outage) the first contingencies are tested to see how the power system should be reconfigured to avoid getting a second contingency and cascading into an outage.
POWERQUALITY MSTEARS: These outages point out the need for reliability as part of the overall customer picture of PQ
POWERQUALITY BRIAN: Hi Jennifer, hit crt-p for private messagae
POWERQUALITY SKLEIN: In simpler terms, a single point failure shouldn't crash the system.
POWERQUALITY SKLEIN: Are we all chatted out?
POWERQUALITY ANDYV: brian, johnmung has been banned!!! why?
POWERQUALITY BRIAN: no way, new subject
POWERQUALITY BRIAN: just a sec, andy
POWERQUALITY BRIAN: No banning on this channel, John is back on
POWERQUALITY TKEY: ieee 519 limits the harmonic current a customer can inject back into the pcc and limit the vthd the utility provides at the PCC
POWERQUALITY JOHNMUNG: thanks guys, for unbanning me—i've been thrown out of better places than this!
POWERQUALITY BRIAN: New subject . . . now . . .
POWERQUALITY BRIAN: good one john . . . :)
POWERQUALITY MSTEARS: For critical facilities dual feeds or other backup capability need to be economically evaluated to keep the facility in operation
POWERQUALITY SAM: John, I remember that club very well
POWERQUALITY JOHNMUNG: question: please comment on frequency of complaints involving spikes, sags or harmonics
POWERQUALITY WARD: Problems caused by sags is the main complaint.
POWERQUALITY BRIAN: What subject does anyone want to see the next chat
POWERQUALITY WARD: Surges is probably next; harmonics really don't cause that many problems, although they are certainly there.
POWERQUALITY ANDYV: what is the solution ward?
POWERQUALITY TKEY: Agree they are the most frequent (sags) and the panel sesion on the cost of voltage sags at PES drew **110** people
POWERQUALITY SAM: harmonics tend to be an interior problem within a facility, rather than on the distribution system
POWERQUALITY WARD: The best solution is making the equipment less susceptible to sags. This requires working with the manufacturers.
POWERQUALITY ANDYV: won't that cost more
POWERQUALITY MSTEARS: The complaint of surges covers many things in the customers eyes sags have become a real problem because they are harder to resolve
POWERQUALITY GRAVELY: John—The latest EPRI results confirms the 90+% of the time SGS are the problem and short term ones.
POWERQUALITY WINDSONG: What is the topic for the 25??
POWERQUALITY WARD: Each problem can be dealt with as it occurs, but the time involved gets very expensive.
POWERQUALITY JOHNMUNG: making equipment less susceptible causes legal problems for manufacturers—as each improvemnt can be cited by compinant as example of malfeasance
POWERQUALITY WARD: AndyV: The cost to the manufacturer increases. The overall cost to everyone involved decreases.

POWERQUALITY TKEY: customer pays any way you cut it, if the eqpt is more immune customers pay only once instead of every time the process fails

POWERQUALITY BRIAN: The topic is regarding Power Quality

POWERQUALITY BRIAN: This chat is available for everyone 24 hours a day

POWERQUALITY ANDYV: ddorr>>will the manufacturer spend more to produce a better product

POWERQUALITY WARD: And as Tom says, the cost to the customer is far less.

POWERQUALITY BRIAN: This chat will be functioning 24 hrs/day

POWERQUALITY BRIAN: please usae it

POWERQUALITY BRIAN: The next panel discussion is Nov 15th

POWERQUALITY WARD: Andy, that's where standards come in.

POWERQUALITY SKLEIN: Is the customer capable of resolving the fingerpointing among the manufacturers and utilities?

POWERQUALITY DDORR: andy, only if the end userss create a market for pq compatible eqpt by demanding better products

POWERQUALITY MSTEARS: The manufacturers problems in including fixes is being competative with some who doesn't provide the fix

POWERQUALITY ANDYV: how will we educate the general consumer?

POWERQUALITY GRAVELY: Is it possible to have a basic theme topic or some core questions for 15 Nov chat?

POWERQUALITY WARD: Stan, the customer cannot be expected to resolve the fingerpointing. The manufacturers and utilities need to work together.

POWERQUALITY ANDYV: about power quality and reliability?

POWERQUALITY SKLEIN: If electric power is going to be treated as a fungible commodity, there has to be a definition. Like, everyone knows what number 2 heating oil is.

POWERQUALITY SAM: Ideally a manufacturer would not be able to compete if they don't add the protective function in their products, but alot more public education is required before we get to this point.

POWERQUALITY WARD: Andy, there are many ways to educate the customers, but they require a lot of contact between the utility and the customers. The Western Resources Power Technology Center in Wichita is doing it, just as an example.

POWERQUALITY DDORR: standard power vs premium power is one solution as is std qpt vs Pq compatible eqpt

POWERQUALITY SKLEIN: I want to buy number 2 electric power and to be able to check the nameplates of my appliances to be sure they can take it. Just like I buy regular gasoline.

POWERQUALITY MSTEARS: Sam—I agree, that is partly the utilities responsibility since we serve the customers

POWERQUALITY BBOYER: What differentiates number 2 from number 1?

POWERQUALITY SKLEIN: I used the analogy of number 2 heating oil. I don't know what number 1 heating oil is.

POWERQUALITY DDORR: Number two has cap switching and all the normal utility operational events while number one is much better

POWERQUALITY SKLEIN: Perhaps we can just say regular vs high test.

POWERQUALITY SAM: mike, yes a joint effort between the utiliy, manufacturer and standards juristictions is a goal for utilicorp as we move forward with offering from our strategic marketing partners, and bring PQ technologies to the public

POWERQUALITY TKEY: We are finding that many mfgrs want to produce pq compatible equipment, but they have no clue as to what to test for

POWERQUALITY ANDYV: Tom>>will the IEC standards help?

POWERQUALITY TKEY: Its up to the utility to help define normal events IEC will take time

POWERQUALITY SKLEIN: You can't have a commodity product with all the variation in specifications we have been discussing. It has to be regular, premium, and super premium or it won't work.

POWERQUALITY JOHNMUNG: Tom as a former manufacturer i sympathize—your work at PEAC is invaluable but anecdotal knowledge from utility people on the firing line is equally important

POWERQUALITY TKEY: Super premium, does that mean a UPS?

POWERQUALITY ANDYV: how do you stop a facility from affecting you super-premium power?

POWERQUALITY TKEY: John, Good Point

POWERQUALITY SAM: Tkey, a ups, local generation or redundant service

POWERQUALITY SKLEIN: This is what I meant earlier by electricity being a non-virtualizable service. You can't make each customer see the power system as though they had their own dedicated generating plant.

POWERQUALITY BRIAN: THE CHAT CHANNEL WILL BE OPEN 24/HRS/DAY 7 DAYS A WEEK

POWERQUALITY TKEY: I must sign out for about 5 minutes but I'll be back

POWERQUALITY BRIAN: OK TOM

POWERQUALITY MSTEARS: PQ for facilities need to be done with a system perspective to to get the right resolution

POWERQUALITY BBOYER: Andy's question is still relevant—how do stop a facility from downgrading utility service to other customers?

POWERQUALITY BRIAN: MIKE>>LETS SWITCH BACK TO RETAIL WHEELING

POWERQUALITY WARD: You work with that customer to do whatever is needed to correct their disturbances.

POWERQUALITY BBOYER: Be more specific

POWERQUALITY MSTEARS: Interaction between facilites can be evaluated and designed for

POWERQUALITY JOHNMUNG: as a key to hardening it helps to identify the most sensitive circuits, i.e. microprocessor logic, test for vulnerability under common surges, sags, rfi, and then notify users that their equipment contains these subsystems—for a start

POWERQUALITY BRIAN: hI DOUG

POWERQUALITY GRAVELY: Brian: Are you saving this session as a file? Can we get a list of chat session participants?

POWERQUALITY BRIAN: s, we may

POWERQUALITY DMARKS: gravely: hit TAB and use the arrow keys to page through the list of participants

POWERQUALITY SKLEIN: Will the session be available for downloading?

POWERQUALITY BRIAN: yes, Mike we will publish in PQ Magazine

POWERQUALITY WARD: Part of the agreement for high quality power should be that the customer receiving the power will not disturb the utility system.

POWERQUALITY BRIAN: if john let's us . . .

POWERQUALITY GRAVELY: I tried that, however, netcruiser has a software problem and I cannot see all of the names.

POWERQUALITY SAM: most utilities rules and regulations already require that a customer not put anything back out on the utility system

POWERQUALITY BRIAN: MIKE G.>>WE WILL PUBLISH THIS IN PQ MAG NEXT MONTH IF ASNDY LETS US

POWERQUALITY BRIAN: HOW ABOUT IT ANDY?

POWERQUALITY ANDYV: ok

POWERQUALITY BRIAN: COOL

POWERQUALITY WARD: Standards will have to be set for what constitutes a disturbance, and then the utility should work with customers, install filters, etc., to be sure they stay within the rules.

POWERQUALITY BRIAN: THANKS ANDY

POWERQUALITY ANDYV: a meeting review or a sumary of events

POWERQUALITY GRAVELY: It would be good to take a few minutes to recommend how the 15 Nov session could be more effective.

POWERQUALITY BRIAN: A SYNAPSE OF THIS CHAT WILL BE IN NEXT MONTHS PQ MAG

POWERQUALITY WINDSONG:

POWERQUALITY SKLEIN: I don't get PQ mag. Will it be on the Net?

POWERQUALITY BRIAN: STAN SIGN UP FOR IT ON OUR HOME PAGE

POWERQUALITY DOUGC: the transcript of this conference will be available on the EnergyOne pages.

POWERQUALITY BRIAN: YOU CAN SIGN UP ON LINE

POWERQUALITY BRIAN: HTTP://WWW.UTILICORP.COM

POWERQUALITY WINDSONG: Good comment Gravely Comments from the users would be greatly appreciated!!

POWERQUALITY SAM: PQ magazine is available online on the UCU Internet bulletin board, http://www.utilicorp.com

POWERQUALITY ANDYV: or link from powerquality.com

POWERQUALITY BRIAN: YOU CAN GET A FREE MAG SUBSCRIPTION FROM UTILICORP'S HOME PAGE

POWERQUALITY SKLEIN: Thanks

POWERQUALITY BRIAN: ALSO, THERE IS A PQ FORUM ON OUR HOME PAGE

POWERQUALITY JOHNMUNG: for nov 15 shall we pick five key topics? suggest health care, energy storage rfi/emc as a few topics—also new gas turbine 25 kw generator just announce today—just some suggestions

POWERQUALITY BRIAN: GOOD SUGGESTION JOHN

POWERQUALITY ANDYV: lets develop an outline of topics for next time.

POWERQUALITY BRIAN: OK

POWERQUALITY GRAVELY: One suggestion for 15 Nov—Have participants place a list of desired topics on your other chat box and prioritize by interest level.

POWERQUALITY SKLEIN: How about deregulation and retail wheeling.

POWERQUALITY BRIAN: COMMENTS SHOULD BE SENT TO ME BY EMAIL

POWERQUALITY BRIAN: BSPENCER@UTILICORP.COM

POWERQUALITY BRIAN: 15 minutes remaining

POWERQUALITY ANDYZYREK: Let's discuss the new standard IEEE 1159.

POWERQUALITY ANDYV: may be we could generate an online questionaire to see what people are needing discussed.

POWERQUALITY BRIAN: but the chat is available for 24 hrs/day 7 days a week

POWERQUALITY ANDYV: what does IEEE1159 address?

POWERQUALITY BRIAN: Please send all suggestion to me for our next chat

POWERQUALITY BRIAN: Bobbin is not banned now

POWERQUALITY BRIAN: my fault

POWERQUALITY ANDYZYREK: New PQ measuring techniques. We have not received our issue yet.

POWERQUALITY ANDYV: You should have it my now.

POWERQUALITY BRIAN: Bobbin is not banned anymore

POWERQUALITY ANDYV: you can e-mail me or john at: editors@powerquality.com

POWERQUALITY BRIAN: is two hours right fdo rhtis feature

POWERQUALITY JOHNMUNG: do i understand that many programmable logic controllers can be hardened by addition of simple CVT like a sola?

POWERQUALITY ANDYZYREK: Yes, but it is being delivered by snail mail.

POWERQUALITY ANDYV: no 2nd class

POWERQUALITY BRIAN: 15 minutes to go

POWERQUALITY ANDYV: Please e-mail me you complete name and addess and I will mail you one today 1st class . . . now is that serice or what?

POWERQUALITY BRIAN: Is two hours long enough for tthis chat?

POWERQUALITY TKEY: Im back

POWERQUALITY WARD: Brian, I think two hours is about right.

POWERQUALITY BRIAN: hi tom

POWERQUALITY BRIAN: good . . .

POWERQUALITY ANDYV: yes I agree 2 hrs

POWERQUALITY BRIAN: anyone else

POWERQUALITY ANDYV: it the time of day correct?

POWERQUALITY BRIAN: questions now . . .

POWERQUALITY SKLEIN: The topic foremost in my mind right now is what to eat for lunch. I enjoyed the discussion, which I understand has been historic in some sense. But I think I will sign off now and go eat.

POWERQUALITY SAM: 2 hours seems to work very well

POWERQUALITY DANIELH: time of day is good

POWERQUALITY BILLMANN: 2 hrs is fine

POWERQUALITY MSTEARS: Two hours work well, the middle of the day allows east and west coast to be involved

POWERQUALITY BRIAN: good, Will everyone be back for the next chat

POWERQUALITY GRAVELY: Brian, I will forward my recommendations on email, thanks.

POWERQUALITY BILLMANN: yes i'll be back

POWERQUALITY ANDYZYREK: Brian, would it be possible to have a forum published on your home page prior to Nov 15.

POWERQUALITY BRIAN: I would like to do another chat before Nov 15th. any thoughts

POWERQUALITY ANDY: U bet

POWERQUALITY SAM: I believe that this chat may set an attendance record for most participants during a first session

POWERQUALITY JOHNMUNG: a parting thought—"harmonics make the music rich, they make the tone insprinng—harmonics in your power line WILL BLOW THE BUILDINGS WIRING" tIM MUNGENAST

POWERQUALITY BRIAN: Your're all invited to return

POWERQUALITY BRIAN: the next chat

POWERQUALITY BRIAN: This chat feature will help set standards of how we view our industry

POWERQUALITY WARD: For me this was two hours very well spent, and it was quite enjoyable.
POWERQUALITY BRIAN: Tell a colleague about our chat Nov 15th
POWERQUALITY BRIAN: Thanks Ward
POWERQUALITY BRIAN: I would like to do this on a weekly basis, any thoughts yet
POWERQUALITY GRAVELY: John: talk it up in Germany!!
POWERQUALITY ANDY: I would like to thank utilicorp and everyone envolved.
POWERQUALITY BRIAN: Thanks Andy for your help
POWERQUALITY WARD: Did this notice go out to the Power Globe mailing list?
POWERQUALITY BRIAN: No, but could help us Ward with that
POWERQUALITY BRIAN: Lets all get the word out about this chat
POWERQUALITY WARD: I'm on the list and will be glad to forward anything you wish to it.
POWERQUALITY BRIAN: Please use it whenver you wish, even schedule your own chats whenver
POWERQUALITY JOHNMUNG: MANY THANKS TO uTILICORP AND ALL INVOLVED—FROM AN OLD STEAM BOATER :-)
POWERQUALITY BRIAN: thanks ward
POWERQUALITY BRIAN: Hi duane
POWERQUALITY BRIAN: This chat is offically over, but do stick around for foir more chatting
POWERQUALITY BRIAN: Thanks to all, cya on Nov 15th
POWERQUALITY MSTEARS: Ward, Tom, and John I appreciate your participation
POWERQUALITY BRIAN: Thanks Guys and Ladies!!!!!!!!!!
POWERQUALITY SWPPD: WHAT IS HAPPENING ON NOV. 15
POWERQUALITY BRIAN: our next chat with a panel of experts
POWERQUALITY BRIAN: topic yet to be decided
POWERQUALITY DPSWOBO: Hi Brian, Sorry I was on the phone and could not respond right away. Did I get the time incorrectly for the chat?
POWERQUALITY BRIAN: please send us a suggestions
POWERQUALITY ANDY: good bye ;-)
POWERQUALITY BRIAN: Yeah, but stick around to chat with some friends
POWERQUALITY BRIAN: We had a total of 50 people and avg of 20 people at one time
POWERQUALITY BRIAN: Thanks everyone!!!Lunch Time
POWERQUALITY BRIAN: Next Chat Nov 15th at 10-12 ct
POWERQUALITY BRIAN: But this chat line is available 24 hrs/day/7 days a week
POWERQUALITY BRIAN: Please use it whenever
POWERQUALITY GRAVELY: Thanks to the panel and Utilicorp for the session!
POWERQUALITY BRIAN: Talk to your collegues and friends about any particular topic
POWERQUALITY BRIAN: Come see our home page for new topics and chats
POWERQUALITY BRIAN: http://www.utilicorp.com
POWERQUALITY BRIAN: Thanks Power Quality Assurance Magazine and All our panel members
POWERQUALITY BRIAN: :)
POWERQUALITY SWPPD: MISSED THIS SESSION. ICAN WE GET HARD COPY INFO?
POWERQUALITY BRIAN: yes swwp, it will be published in pq mag and our home page
POWERQUALITY BRIAN: catch our next session on nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY SWPPD: THANKS A BUNCH!!
POWERQUALITY SWPPD: GOOD BYE!
POWERQUALITY BRIAN: no prob
POWERQUALITY BRIAN: cya
POWERQUALITY DESWETT:
POWERQUALITY TKEY: Good session brian, ddorr and I will be signing off now, look forward to the next session
POWERQUALITY DPSWOBO: Thanks for the info on the next session, we will get on next time
POWERQUALITY DMARKS: I hope everyone enjoyed this session.
POWERQUALITY MSTEARS: I am logging off Thanks
POWERQUALITY SAM: This is Tony and I am watching the action . . . we made history. Great work guys.
POWERQUALITY BRIAN: Lunch time
POWERQUALITY BRIAN: Next chat is nov 15th
POWERQUALITY BRIAN: 10-12ct
POWERQUALITY BRIAN: please continuie to look at utilicorp's hp
POWERQUALITY BRIAN: for more info
POWERQUALITY BRIAN: email if you have any questions regarding the chat
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: later
SUPPORT BRIAN: hi guys
SUPPORT BRIAN: success
SUPPORT BRIAN: yess!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
SUPPORT BRIAN: thanks for the help
SUPPORT BRIAN: cya
POWERQUALITY BRIAN: next chat on Nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: any suggestion on topics please contact me by email
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: hi chuck
POWERQUALITY BRIAN: hi randy
POWERQUALITY CPREECS: hello brian
POWERQUALITY BRIAN: How are you chuck
POWERQUALITY CPREECS: how has the participation been?
POWERQUALITY BRIAN: I am sorry you missed the offical chat, but do come back at any time for some chatting
POWERQUALITY BRIAN: great 20 people avg. 50 total people
POWERQUALITY CPREECS: ?yes, i got some conflicting info
POWERQUALITY BRIAN: transcripts will be in PQ mag next month and on utilicorp's home page
POWERQUALITY CPREECS: what were the topics discussed?
POWERQUALITY BRIAN: how is that chuck
POWERQUALITY BRIAN: power quality, standards,
POWERQUALITY BRIAN: retail wheeling
POWERQUALITY BRIAN: cya, lunch time
POWERQUALITY CPREECS: later
POWERQUALITY BRIAN: bye all
POWERQUALITY BRIAN: email me chuck
POWERQUALITY RB: sorry I missed it. I got 12-2 est off the net. bye.
POWERQUALITY BRIAN: sorry RB
POWERQUALITY BRIAN: miss information

POWERQUALITY BRIAN: next chat is 10-12

POWERQUALITY BRIAN: ct

POWERQUALITY BRIAN: nov 15th

POWERQUALITY BRIAN: bye

POWERQUALITY RB: thanks

POWERQUALITY BRIAN: no prob, tell all

POWERQUALITY ANDY: Is anyone still here talking about power quality?

POWERQUALITY DAVE: Just signed on that is what I was trying to find out

POWERQUALITY ANDY: the PQ chat was running from 11:00-1:00est

POWERQUALITY ANDY: Were you involved then?

POWERQUALITY DAVE: No I just got a chance to sign on now

POWERQUALITY ANDY: there were some great discussions.

POWERQUALITY ANDY: The transcripts will be available to down load at utilicorp.com Brian Spencer says.

POWERQUALITY ANDY: What is your experience in PQ

POWERQUALITY DAVE: That is what I was looking for, are they available to down load now, I work in a data center and have worked with UPS systems for about 12 years

POWERQUALITY DAVE: I did field service for Exide

POWERQUALITY ANDY: Brian just went to Lunch in KS I don/t know when it will availalbe.

POWERQUALITY DAVE: Thanks for the Info on the downloads, I hope they do this again

POWERQUALITY ANDY: so do I.

POWERQUALITY DAVE: What is your experience on PQ

POWERQUALITY ANDY: I am the editor or Power quality mag.

POWERQUALITY DAVE: Good mag., I pick up alot in it

POWERQUALITY ANDY: do your receive power quality assurance magazine?

POWERQUALITY ANDY: great glad to hear it.

POWERQUALITY DAVE: We get it at work but I have asked to have it sent to my home PS POWERQUALITY ANDY: did you get the latest issue witht the lighting on the cover?

POWERQUALITY DAVE: Not yet, have seen it on line though

POWERQUALITY ANDY: great.

POWERQUALITY ANDY: any suggestion for editorial?

POWERQUALITY DAVE:

POWERQUALITY DAVE: no it is good

POWERQUALITY ANDY: ok.

POWERQUALITY ANDY: I am currently editing an article about VRLA battery charging.

POWERQUALITY DAVE: I am working on a resonant problem with Utility and was looking for info

POWERQUALITY ANDY: explain

POWERQUALITY ANDY: by the way my e-mail is andy@powerquality.com

POWERQUALITY DAVE: we are running a lot of 5th har. across our system in a large data center

POWERQUALITY ANDY: I see

POWERQUALITY ANDY: I will try to address this in an upcomming issue. may be march/april or even sooner.

POWERQUALITY DAVE: we have 4800 kw of UPS cap on two transformers and we have alot of 5th on our other boards

POWERQUALITY ANDY: If you are interested in writing up a case history including you solutions I would like to review it and poss. publish

POWERQUALITY MSTONEHAM: Is this chat session still active?

POWERQUALITY ANDY: YES

POWERQUALITY ANDY: We can'nt get enough! ! !

POWERQUALITY DAVE: when we can get it fixed, It looks like we have a problem with input filtering on a couple of UPS,s

POWERQUALITY ANDY: input fro the utility or a generator?

POWERQUALITY DAVE: utility

POWERQUALITY MSTONEHAM: I understand there was a chat session earlier today with some guest "chatters". Is there an archive of the discussion since I missed it?

POWERQUALITY DAVE: we have 66 kv to 12 kv then to 480 v by 4 trans on property

POWERQUALITY ANDY: What are you leaning towards in a solution dave

POWERQUALITY ANDY: MTONEHAM>>yes but I don't know when. contact BSPENCER@utilicorp.com

POWERQUALITY DAVE: the computer seem to have no problem, but we have alot of motor heating/bad PF

POWERQUALITY MSTONEHAM: Thanks!

POWERQUALITY DAVE: we currently are working with a consulant but I am looking for more info

POWERQUALITY ANDY: will capacitors solve your ptoblem

POWERQUALITY ANDY:

POWERQUALITY ANDY: there also is a forum under utilicorp.com where you can post you questions.

POWERQUALITY DAVE: Each 600 kw UPS has Input filtering/may need trap for 5th

POWERQUALITY ANDY: or you can access it form powerquality.com

POWERQUALITY DAVE: thanks

POWERQUALITY ANDY: Talk to ya later dave

POWERQUALITY DAVE: is PQ.com your Mag

POWERQUALITY ANDY: bye

POWERQUALITY DAVE: bye

POWERQUALITY ANDY: yes

POWERQUALITY DAVE: thanks

POWERQUALITY ANDY: :-)

POWERQUALITY MSTONEHAM:

POWERQUALITY MSTONEHAM: Is anyone else hear? There doesn't seem to be much traffic.

POWERQUALITY MSTONEHAM:

POWERQUALITY CILCOJRG: Hello—is the conference over?

POWERQUALITY CILCOJRG:

POWERQUALITY CILCOJRG: hello

POWERQUALITY BRIAN: yes

POWERQUALITY BRIAN: the conference was from 10-12 ct

POWERQUALITY BRIAN: someone gave out the wrong information

POWERQUALITY BRIAN: hello cilco

POWERQUALITY BRIAN: anyone still there

SUPPORT BRIAN: hi all

SUPPORT BRIAN: anyone there

POWERQUALITY BRIAN: jenny>>are you there

POWERQUALITY CJBOUTCHER: is anyone here a utility employee?

POWERQUALITY BRIAN: Hi chris

POWERQUALITY BRIAN: how are you?

POWERQUALITY CJBOUTCHER: hi brian it is quiet in here

POWERQUALITY BRIAN: the conference was at 10:00ct

POWERQUALITY CJBOUTCHER: ah I see

POWERQUALITY CJBOUTCHER: when is the next one?

POWERQUALITY BRIAN: nov 15th

POWERQUALITY BRIAN: 10-12

POWERQUALITY BRIAN: ct

POWERQUALITY CJBOUTCHER: is the channel open at other times?
POWERQUALITY BRIAN: yes 24 hours a dfay
POWERQUALITY CJBOUTCHER: but not much discussion?
POWERQUALITY BRIAN: not right now,
POWERQUALITY BRIAN: cya
POWERQUALITY CJBOUTCHER: bye
POWERQUALITY BRIAN: hi jenny
POWERQUALITY JOSH: hello?
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: are you awake yet?
POWERQUALITY BRIAN: just giving present this a.m.
POWERQUALITY BRIAN: :)
POWERQUALITY BRIAN: who is guest96
POWERQUALITY GUEST96: test

While a particular embodiment of the present invention has been disclosed, it is to be understood that various different modifications are possible and are within the true spirit of the invention, the scope of which is to be determined with reference to the claims set forth below. There is no intention, therefore, to limit the invention to the exact disclosure presented herein as a teaching of one embodiment of the invention.

The invention claimed is:

**1**. A computer apparatus distributing a communication over an Internet network, the apparatus including:

a controller computer system adapted to communicate responsive to a respective authenticated user identity corresponding respectively to each of a plurality of participator computers,

each said participator computer communicatively connected to said Internet network, each said participator computer programmed to enable the communication, the communication including at least one of a prestored sound, video, graphic, and multimedia,

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 the participator computers which are otherwise independent of each other; wherein

one said authenticated user identity is used to communicate a pointer-triggered private message from a first of said participator computers to said controller computer and from said controller computer to a second of said participator computers that invokes said pointer-triggered private message to fetch and receive the communication from a computer other than said first or said second said participator computers in real time over the Internet network

such that the second of said participator computers internally determines whether or not the second of the participator computers can present the communication, if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication, and otherwise presenting the communication independent of the first of the independent participator computers and the computer.

**2**. The apparatus of claim **1**, wherein the computer system includes a world wide web communication.

**3**. The apparatus of claim **1**, wherein the computer system includes data representing sound communications.

**4**. The apparatus of claim **1**, wherein the computer system includes data representing video communications.

**5**. The apparatus of claim **1**, wherein the computer system includes data representing sound and video communications.

**6**. The apparatus system of claim **1**, wherein the computer system further determines that the message is not censored.

**7**. An apparatus to communicate via an Internet network, the apparatus including:

a computer system communicatively connected to each of a plurality of participator computers responsive to communication of a respective login name and a password corresponding to a respective user identity,

a first of the participator computers running software communicating a private message to the computer system, the private message comprising a pointer,

the computer system, including a database which serves as a repository of tokens for other programs to access, thereby affording information to each of the participator computers which are otherwise independent of each other, wherein

the first participator computer of the computer system is running software communicating the private message to a second of the participator computers, and

the second of the participator computers is running software receiving a communication via the pointer provided within the private message from the first of the participator computers,

the communication being sent in real time and via the Internet network,

the communication including pre-stored data representing at least one of video, a graphic, sound, and multimedia, such that the second of the participator computers determines internally whether or not the second of the participator computers can present the communication,

if it is determined that the second of the participator computers can not present the communication then obtaining an agent with an ability to present the communication, and

otherwise presenting the communication independent of the first of the independent participator computers.

**8**. The apparatus of claim **7**, wherein the computer system further determines that the message is not censored.

**9**. The apparatus of claim **7**, wherein the computer system includes the pointer as a pointer that causes the communication to be produced on demand.

**10**. The apparatus of claim **7**, wherein the computer system includes data representing video communications.

**11**. The apparatus of claim **7**, wherein the computer system includes data representing sound communications.

**12**. The apparatus of claim **7**, wherein the computer system includes data representing sound and video communications.

**13**. The apparatus of claim **7**, wherein the computer system includes messaging data representing at least one of text communications and ASCII communications.

**14**. The apparatus of claim **7**, wherein the computer system includes data representing a member-associated image communications.

**15**. The apparatus of claim **7**, wherein the computer system provides a chat channel via the Internet network between at least two of the plurality of independent computers.

**16**. The apparatus of claim **7**, wherein the computer system includes at least one message as an out-of-band communication.

**17**. The apparatus of claim **8**, wherein the computer system includes a user age corresponding to each of the user identities.

**18**. The apparatus of claim **17**, wherein the computer system includes messaging data representing at least one of text communications and ASCII communications.

**19**. An apparatus to receive a communication via an Internet network, the apparatus including:

a computer system, and

a plurality of participator computers,

each of the participator computers communicatively connected to the computer system responsive to each of the plurality of participator computers being associated with a respective login name and a password;

a first of the plurality of participator computers being programmed to communicate such that a private message is sent to the computer system,

the private message including a pointer pointing to a communication that includes pre-stored data representing at least one of a video, a graphic, sound, and multimedia;

the computer system, including a computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of the participator computers which are otherwise independent of each other; wherein

the computer system communicates the private message to a second of the plurality of participator computers; and

the second participator computer is programmed to receive the communication provided within the private message, which originates from the first participator computer,

the communication being sent in real time and via the Internet network, and the second participator computer internally determines whether or not the second participator computer can present the pre-stored data, if it is determined that the second participator computer can not present the pre-stored data then obtaining an agent with an ability to present the pre-stored data, and otherwise presenting the pre-stored data independent of the first participator computer.

**20**. The apparatus of claim **19**, wherein the computer system is further programmed to determine whether the pointer is not censored.

**21**. The apparatus of claim **19**, wherein the computer system is further programmed to determine whether the message is not censored.

**22**. The apparatus of claim **19**, wherein the pointer produces the communication on demand.

**23**. The apparatus of claim **19**, wherein the communication includes the pre-stored data representing the video.

**24**. The apparatus of claim **19**, wherein the communication includes the pre-stored data representing the sound.

**25**. The apparatus of claim **19**, wherein the communication includes the pre-stored data representing the sound and the video.

**26**. The apparatus of claim **19**, wherein the computer system is further programmed to determine whether the communication is not censored.

**27**. The apparatus of claim **19**, wherein the message includes pre-stored data representing at least one of text and ASCII.

**28**. The apparatus of claim **19**, wherein the communication includes data representing a member-associated image.

**29**. The apparatus of claim **19**, wherein the computer system is further programmed to form a chat channel via the Internet network, between at least two of the plurality of independent computers.

**30**. The apparatus of claim **19**, wherein the computer system is further programmed to communicate the message as an out-of-band communication message.

**31**. The apparatus of claim **19**, wherein the computer system stores a user age corresponding to each of the user identities.

**32**. The apparatus of claim **31**, wherein the pre-stored data represents the sound.

**33**. The apparatus of claim **31**, wherein the pre-stored data represents the video.

**34**. The apparatus of claim **31**, wherein the pre-stored data represents the sound and the video.

**35**. The apparatus of claim **31**, wherein the message includes pre-stored data representing at least one of text and ASCII.

**36**. The apparatus of claim **19**, wherein the pre-stored data represents the multimedia.

**37**. A communication apparatus to allow communication via an Internet network, the apparatus including:

a plurality of participator computers,

each of the participator computers communicatively connected to a computer system responsive to each of the plurality of the participator computers being associated with a login name and a password,

the computer system including a computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of the participator computers which are otherwise independent from each other; wherein the participator computers of the computer system allow a first of the user identities and a second of the user identities to form a group in which members send private communications in real time and via the Internet network, and receive communications from another member,

one of the private communications including a pointer that produces a pointer-triggered message on demand,

one of the communications including pre-stored data representing sound, and

one of the communications including pre-stored data representing at least one of text and ASCII, wherein one of the participator computers that receives the one of the communications including the pre-stored data internally determines whether or not the one of the participator computers can present the pre-stored data, if it is determined that the one of the participator computer can not present the pre-stored data then obtaining an agent with an ability to present the communication, and otherwise presenting the pre-stored data.

**38**. Apparatus to communicate via an Internet network, the apparatus including:

a computer system interactively connected with a plurality of participator computers

responsive to receiving information indicative of a first user identity corresponding to a first of the plurality of participator computers and

responsive to receiving information indicative of a second user identity corresponding to a second of the plurality of participator computers,

the first of the plurality of participator computers running software,

the second of the plurality of participator computers running software, the computer system, including the participator computers and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of the participator computers which are otherwise independent of each other, the computer system allowing the first user identity and the second user identity to form a group in which members can communicate by sending private communications, and receiving communications from another of the members, in real time and via the Internet network, wherein

one of the private communications includes a pointer that produces a pointer-triggered message on demand,

one of the communications including pre-stored data representing sound, and

one of the communications include pre-stored data representing at least one of text and ASCII, wherein one of the participator computers that receives the pre-stored data internally determines whether or not the one of the participator computers can present the pre-stored data, if it is determined that the one of the participator computer can not present the pre-stored data then obtaining an agent with an ability to present the communication, and otherwise presenting the pre-stored data.

**39**. The apparatus of claim **38**, wherein the group includes a third of said participator computers.

**40**. The apparatus of claim **38**, wherein the computer system further determines that one of the communications is not censored.

**41**. An apparatus to distribute a communication via an Internet network, the apparatus including:

a first participator computer communicatively connected to a computer system, the first independent computer being connected in association with a user identity, and

a private communication link between the first participator computer and a second participator computer,

the computer system including a computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of the participator computers which are otherwise independent of each other; wherein

the first participator computer privately communicates a pointer within a private message from the first independent computer to the computer system, and

the second participator computer receives the pointer within the private message from the computer system and invokes the pointer to fetch and to receive the private communication from the first participator computer, via the private communication link, in real time, and via the Internet network, wherein the private communication includes pre-stored data representing at least one of a video, a graphic, sound, and multimedia, and the second participator computer internally determines whether or not the second participator computer can present the communication, if it is determined that the second participator computer can not present the communication then obtaining an agent with an ability to present the communication, and otherwise presenting the communication independent of the first participator computer.

**42**. The apparatus of claim **41**, wherein the computer system is further programmed to determine whether the pointer is censored.

**43**. The apparatus of claim **41**, wherein the computer system is further programmed to determine whether the data are censored.

**44**. The apparatus of claim **43**, wherein the communication includes data representing the pre-stored sound, and at least one of text and ASCII.

**45**. The apparatus of claim **41**, wherein the pointer produces the communication on demand.

**46**. The apparatus of claim **45**, wherein the communication includes the pre-stored data representing the sound.

**47**. The apparatus of claim **41**, wherein the communication includes the pre-stored data representing the video.

**48**. The apparatus of claim **41**, wherein the communication includes the pre-stored data representing the sound.

**49**. The apparatus of claim **41**, wherein the communication includes the pre-stored data representing the sound and the video.

**50**. The apparatus of claim **41**, wherein the communication includes the pre-stored data representing the multimedia.

**51**. The apparatus of claim **41**, wherein the data includes data representing a member-associated image.

**52**. The apparatus of claim **41**, wherein the computer system is further programmed to allow chat communication in real time via the Internet network.

**53**. The apparatus of claim **41**, wherein the computer system is further programmed to communicate out-of-band communication.

**54**. The apparatus of claim **41**, wherein the wherein the pre-stored data represents the multimedia.

**55**. The apparatus of claim **41**, wherein the computer system communicates asynchronous and synchronous communication.

**56**. The apparatus of claim **55**, wherein the communication includes the pre-stored data representing the sound.

**57**. The apparatus of claim **55**, wherein the communication includes the pre-stored data representing the video.

**58**. The apparatus of claim **55**, wherein the communication includes the pre-stored data representing the sound and the video.

* * * * *

US008407356B1

(12) **United States Patent**
**Marks**

(10) **Patent No.: US 8,407,356 B1**
(45) **Date of Patent: Mar. 26, 2013**

(54) **REAL TIME COMMUNICATIONS SYSTEM**

(76) Inventor: **Daniel L Marks**, Urbana, IL (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 1521 days.

(21) Appl. No.: **11/836,633**

(22) Filed: **Aug. 9, 2007**

**Related U.S. Application Data**

(63) Continuation of application No. 09/399,578, filed on Sep. 20, 1999, which is a continuation of application No. 08/617,658, filed on Apr. 1, 1996, now Pat. No. 5,956,491.

(51) **Int. Cl.**
***G06F 15/16*** (2006.01)

(52) **U.S. Cl.** .......................... **709/230**; 709/204; 709/206

(58) **Field of Classification Search** .......... 709/204–206, 709/230
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | | |
|---|---|---|---|---|---|
| 5,347,632 | A | | 9/1994 | Filepp et al. | |
| 5,408,470 | A | | 4/1995 | Rothrock et al. | |
| 5,440,624 | A | | 8/1995 | Schoof, II et al. | |
| 5,452,299 | A | | 9/1995 | Thessin et al. | |
| 5,616,876 | A | | 4/1997 | Cluts | 84/609 |
| 5,689,553 | A | * | 11/1997 | Ahuja et al. | 379/202.01 |
| 5,771,355 | A | | 6/1998 | Kuzma | |
| 5,774,668 | A | | 6/1998 | Choquier et al. | |
| 5,793,365 | A | | 8/1998 | Tang et al. | 345/329 |
| 5,880,731 | A | | 3/1999 | Liles et al. | 345/349 |
| 5,941,947 | A | * | 8/1999 | Brown et al. | 709/225 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| EP | 0 336 552 A2 * | 10/1989 |

OTHER PUBLICATIONS

Vinod Anupam et al., Shastra—An Architecture for development for Collaborative applications. Proceedings Second Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Apr. 1993, pp. 155-163.*

T. Socolofsky et al., Request for Comments (RFC) 1180: A TCP/IP Tutorial, Network Working Group, Jan. 1991, pp. 1-29.*

J. Oikarinen et al., Request for Comments (RFC) 1459: Internet Relay Chat Protocol, Network Working Group, May 1993, pp. 1-66.*

"Complaint: *Brian Hollander* vs. *Peter K. Trzyna* and *PTK Technologies, LLC*," Dated Nov. 13, 2007, pp. 1-18.

"Preliminary Amendment," for U.S. Appl. No. 11/510,351, filed Nov. 30, 2007.

"Response to Notice of Non-Responsive reply and Supplemental Amendment and Response," for U.S. Appl. No. 11/510,351, filed Feb. 6, 2009.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,351, mailed Jul. 22, 2009. pp. 1-14.

"Amendment and Response" for U.S. Appl. No. 11/510,351, filed Jan. 19, 2010. pp. 1-18.

"Preliminary Amendment," for U.S. Appl. No. 11/510,463, filed Nov. 30, 2007. pp. 1-12.

(Continued)

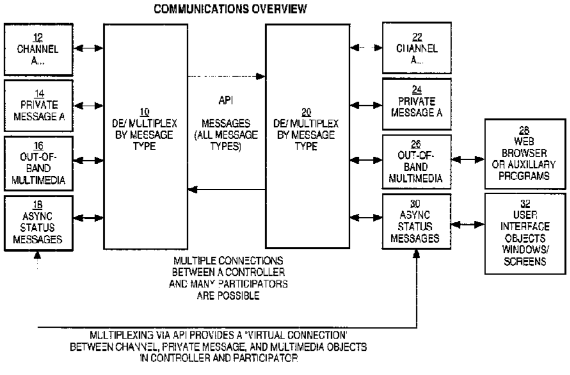
*Primary Examiner* — Patrice Winder

(74) *Attorney, Agent, or Firm* — Peter K. Trzyna, Esq.

(57) **ABSTRACT**

A computerized human communication arbitrating and distributing system, including a controller digital computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information from a human user and an output device for presenting information to the user, each said user having a user identity. A connection, such as Internet, links the controller computer with each of the participator computers. Controller software runs on the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups through the controller computer and to distribute real time data to the respective ones of the groups. Participator software runs on each of the participator computers to handle a user interface permitting one said user to send a multimedia information message to the controller computer, which arbitrates which of the participator computers receive the multimedia information message and conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

**37 Claims, 22 Drawing Sheets**


COMMUNICATIONS OVERVIEW
12 CHANNEL A...
14 PRIVATE MESSAGE A
16 OUT-OF-BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DE/MULTIPLEX BY MESSAGE TYPE
API
MESSAGES (ALL MESSAGE TYPES)
20 DE/MULTIPLEX BY MESSAGE TYPE
22 CHANNEL A...
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILLARY PROGRAMS
32 USER INTERFACE OBJECTS WINDOWS/ SCREENS
MULTIPLE CONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A "VIRTUAL CONNECTION" BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

## OTHER PUBLICATIONS

"Preliminary Amendment," for U.S. Appl. No. 11/510,473, filed Nov. 30, 2007. pp. 1-21.

"Office Action" for U.S. Appl. No. 11/510,351, mailed on Mar. 18, 2008. pp. 1-23.

Office Action-Non-Final Rejection for U.S. Appl. No. 11/510,473, mailed on Oct. 5, 2009. pp. 1-49.

Tim Meyer et al., A MOO-Based Collaboration Hypermedia System for WWW, Proceedings for Second International Conference for WWW, Oct. 1994.

Paul Kindberg et al., Mushroom: a framework for collaboration and interaction across the Internet, in the Proceedings of ERCIM Workshop on CSCW and the Web, Feb. 1996, 11 pages.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,463, mailed on Sep. 22, 2009. pp. 1-27.

Pavel Curtis et al., MUDS Grow Up: Social Virtual Reality in the Real World, Xerox PARC, Jan. 1993, 6 pages.

"Amendment and Response" for U.S. Appl. No. 11/510,351, filed Sep. 18, 2008. pp. 1-18.

"Amendment and Response," for U.S. Appl. No. 11/510,473, filed Feb. 5, 2010. pp. 1-26.

"Amendment and Response" for U.S. Appl. No. 11/510,463, filed Mar. 22, 2010. pp. 1-16.

"Corrected Amendment and Response" for U.S. Appl. No. 11/510,463, filed Apr. 1, 2010. pp. 1-16.

"Preliminary Amendment" Nov. 30, 2007, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Response to Notice of Non-Responsive reply and Supplemental Amendment and Response" filed on Feb. 6, 2009, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Non-Final Rejection" mailed Jul. 22, 2009, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Jan. 19, 2010, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Mar. 18, 2008, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Non-Final Rejection" mailed on Oct. 5, 2009, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Non-Final Rejection" mailed on Sep. 22, 2009, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"MUDS Grow Up: Social Virtual Reality in the Real World". Curtis P. and Nichols, D.A. Xerox PARC. (Jan. 1993) pp. 1-6.

"Amendment and Response" filed on Sep. 18, 2008, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Feb. 5, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Mar. 22, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Corrected Amendment and Response" filed on Apr. 1, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Final Rejection" mailed on Jun. 28, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

Bentley et al., Supporting Collaborative Information Sharing with the World Wide Web: The BSCW shared workspace system, Proceedings of the 4th International World Wide Web Conference, Dec. 1995, 12 pages.

Atul Prakash et al., DistiVew for Building Efficient Collaborative Applications using Replicated Objects, Proceeding of the 1994 ACM conference on Computer supported cooperative work, 12 pages.

Kankanahalli Srinivas et al., MONET: A Multi-media System for Conferencing and Application Sharing in Distributed Systems, Feb. 1992, CERC Techinical Report Series Research Note, 19 pages.

"Office Action-Final Rejection" mailed on May 12, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

K.J. Maly et al., Mosaic + XTV = CoReview, Computer Networks and ISDN Systems, vol. 27 Issue 6, Apr. 1995, pp. 849-860, Proceedings of the Thrid International World Wide Web Conference.

"Amendment After Final" filed on Jun. 11, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,473, mailed May 12, 2010, pp. 1-14.

Atul Prakash et al., DistView for Building Efficient Collaborative Applications using Replicated Objects, Proceedings of the 1994 ACM conference on Computer supported cooperative work, pp. 153-164.

Meloan, Steve. CU-SeeMe. Tech Toys. 1995 Urban Desires. pp. 1-2 http://desires.com/1.6/Toys/Cuseeme/cuseeme.html.

Oikarinen, J. & Reed, D. Internet Relay Chat Protocol. May 1993. pp. 1-69.

Andreas Dieberger, Providing Spatial Navigation for the World Wide Web, Spatial Information theory a Theoretical Baisi for GIS, Lecture Notes in Computer Science, vol. 988, 1995, pp. 93-106.

Lee Newberg et al., Integrating the World-Wide Web and Multi-User Domains to Support Advanced Network-Based Learning Experiments, Conference Proceedings of ED-MEDIA 1995, pp. 494-499.

T Y Hou et al., An active multimedia System for Delayed Conferencing, Proceedings of the SPIE Conference on High-Speed Networking and Multimedia Computing, San Jose CA, 1994, pp. 97-104.

Paul Tarau et al., LogiMOO: an Extensible Multi-User Virtual World with Natureal Language Control, The Journal of Logic Programming, 1993, col. 12, pp. 1-23.

Anupam, Vinod "Collaborative Multimedia Environments for Problem Solving." A Thesis Submitted to Purdue University. (Aug. 1994), pp. 1-212, Ann Arbor, MI.

Bajaj, Chandrajit et al. "Collaborative Multimedia in Shastra." 3rd International Conference in Multimedia, San Francisco, CA (1995). pp. 365-366.

Anupam, Vinod et al. "Collaborative Multimedia in Scientific Design." Proceedings: First ACM Multimedia Conference, ACM Multimedia 93, Anaheim, California, ACM Press, (1993). pp. 447-456.

Anupam, Vinod et al. "Shastra—An Architecture for Development of Collaborative Applications." Proceedings: Second IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Morgantown, (1993). pp. 155-166.

Bajaj, Chandrajit et al. "Brokered Collaborative Infrastructure for CSCW." Proceedings: Fourth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Berkeley Springs. West Virginia, IEEE Computer Society Press, (1995), pp. 207-213.

Anupam, Vinod et al. "Shastra: Multimedia Collaborative Design Environment." IEEE Multimedia, 1, 2, (1994), pp. 39-49.

Anupam, Vinod et al. "Distributed and Collaborative Visualization." IEEE Computer, 27, 7, (Jul. 1994), pp. 37-43.

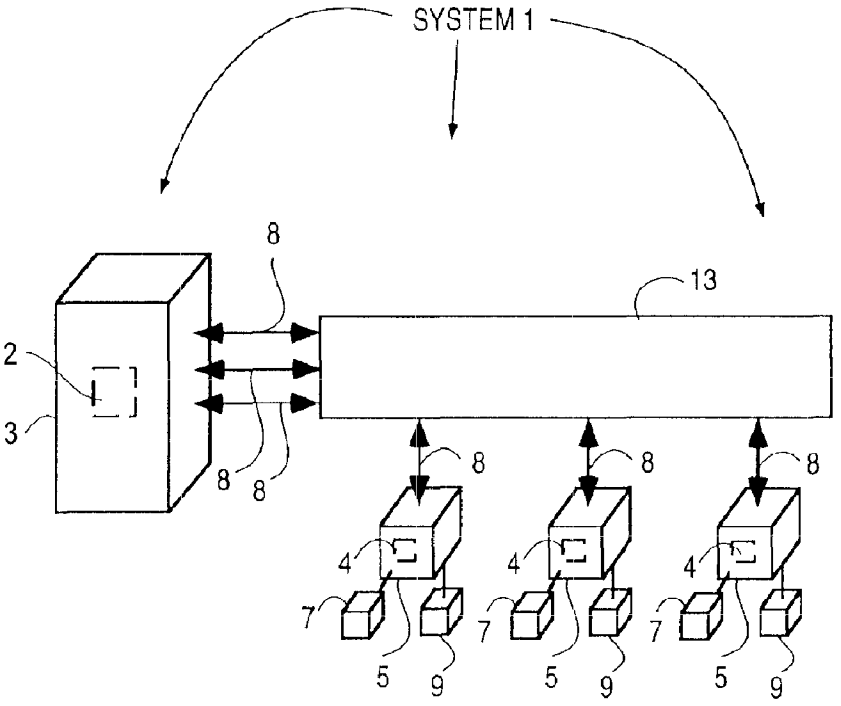
Bajaj, Chandrajit et al. "Web based Collaborative Visualization of Distributed and Parallel Simulation." In Proceedings of the 1999 IEEE Symposium on Parallel Visualization and Graphics, (Oct. 24-29, 1999), San Francisco, CA, pp. 47-54.

Bajaj, Chandrajit et al. "NLS: Collaborative Virtual Environment to Promote Shared Awareness." Proceedings: Workshop on New Paradigms in Information Visualization and Manipulation NPIV'96, In Conjunction with Fifth ACM International Conference on Information and Knowledge Management (CIKM'96), (1996), pp. 41-45.

Bajaj, Chandrajit et al. "Web Based Collaboration-Aware Synthetic Environments" Proceedings of the 1997 GVU/NIST TEAMCAD workshop, Atlanta, GA, 1997. 143-150.

* cited by examiner

FIG. 1



COMMUNICATIONS OVERVIEW

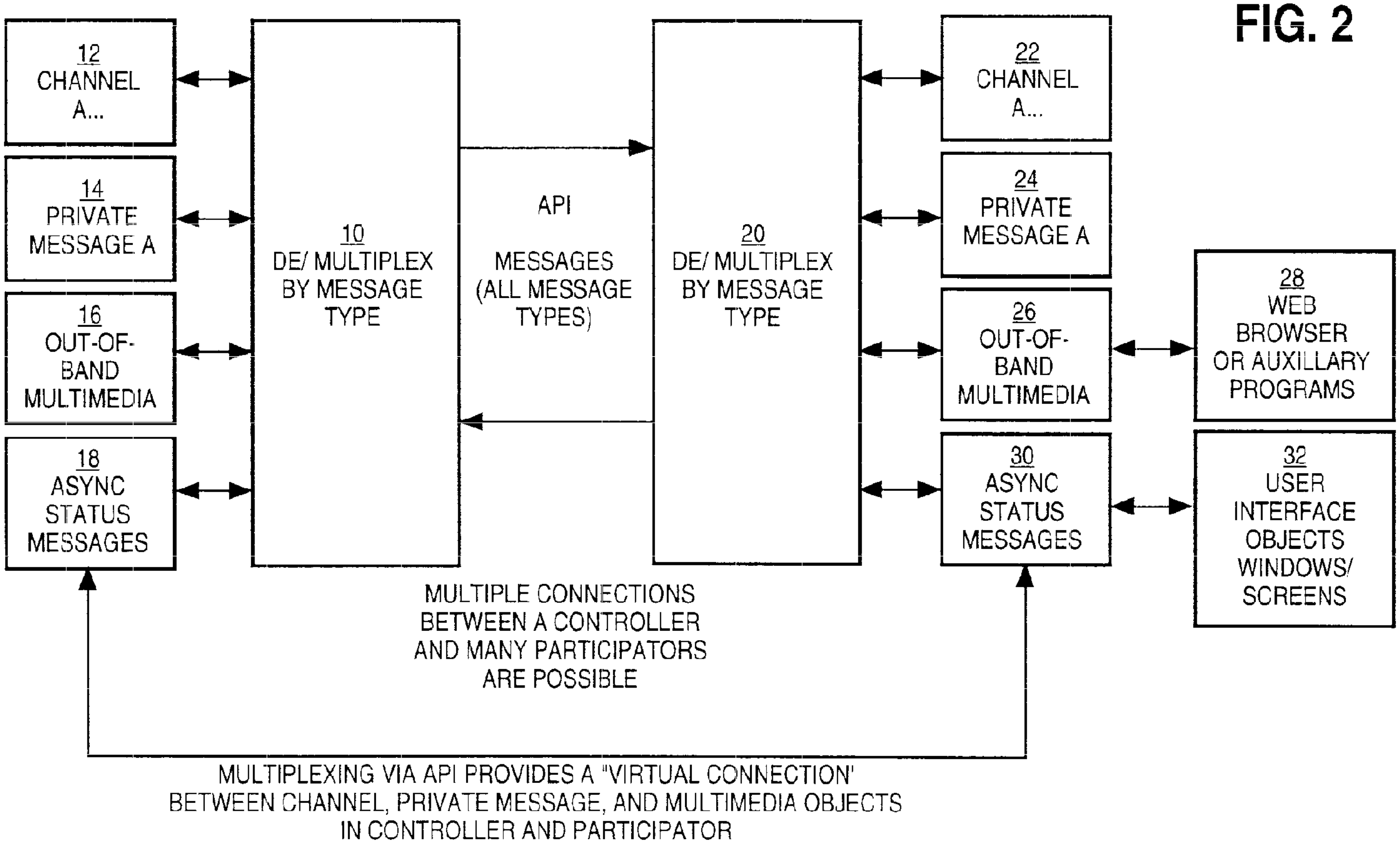

12 CHANNEL A...
14 PRIVATE MESSAGE A
16 OUT-OF-BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DE/ MULTIPLEX BY MESSAGE TYPE
API
MESSAGES (ALL MESSAGE TYPES)
20 DE/ MULTIPLEX BY MESSAGE TYPE
22 CHANNEL A...
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILLARY PROGRAMS
32 USER INTERFACE OBJECTS WINDOWS/ SCREENS
MULTIPLE CONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A "VIRTUAL CONNECTION' BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

FIG. 2

FIG. 3

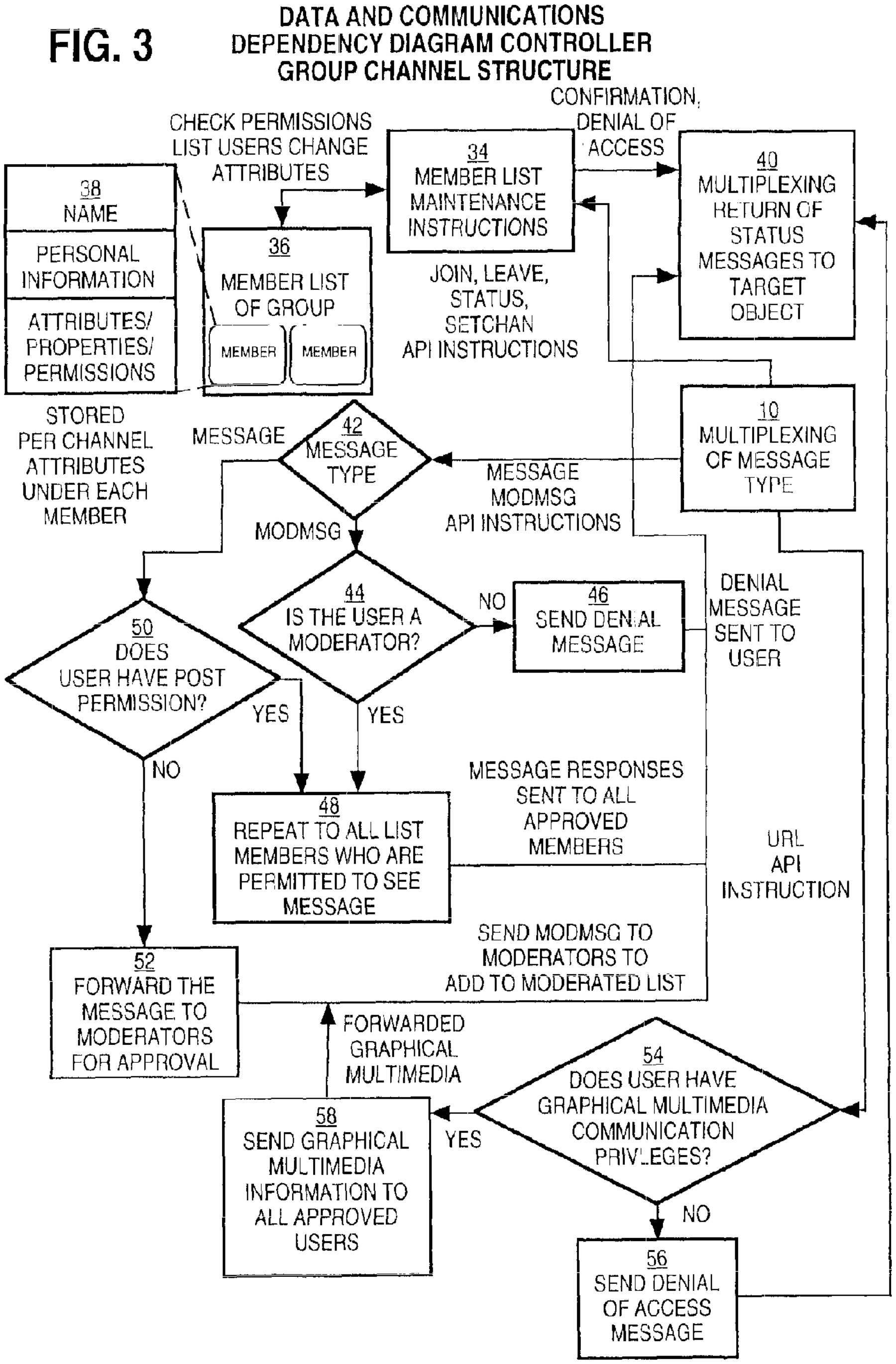

DATA AND COMMUNICATIONS
DEPENDENCY DIAGRAM CONTROLLER
GROUP CHANNEL STRUCTURE
CHECK PERMISSIONS LIST USERS CHANGE ATTRIBUTES
34 MEMBER LIST MAINTENANCE INSTRUCTIONS
CONFIRMATION, DENIAL OF ACCESS
40 MULTIPLEXING RETURN OF STATUS MESSAGES TO TARGET OBJECT
38 NAME
PERSONAL INFORMATION
ATTRIBUTES/ PROPERTIES/ PERMISSIONS
36 MEMBER LIST OF GROUP
MEMBER
MEMBER
JOIN, LEAVE, STATUS, SETCHAN API INSTRUCTIONS
STORED PER CHANNEL ATTRIBUTES UNDER EACH MEMBER
MESSAGE
42 MESSAGE TYPE
10 MULTIPLEXING OF MESSAGE TYPE
MESSAGE MODMSG API INSTRUCTIONS
MODMSG
44 IS THE USER A MODERATOR?
NO
46 SEND DENIAL MESSAGE
DENIAL MESSAGE SENT TO USER
50 DOES USER HAVE POST PERMISSION?
YES
YES
NO
48 REPEAT TO ALL LIST MEMBERS WHO ARE PERMITTED TO SEE MESSAGE
MESSAGE RESPONSES SENT TO ALL APPROVED MEMBERS
URL API INSTRUCTION
52 FORWARD THE MESSAGE TO MODERATORS FOR APPROVAL
SEND MODMSG TO MODERATORS TO ADD TO MODERATED LIST
FORWARDED GRAPHICAL MULTIMEDIA
54 DOES USER HAVE GRAPHICAL MULTIMEDIA COMMUNICATION PRIVILEGES?
YES
58 SEND GRAPHICAL MULTIMEDIA INFORMATION TO ALL APPROVED USERS
NO
56 SEND DENIAL OF ACCESS MESSAGE

FIG. 4

CENTRAL CONTROLLER LOOP COMMUNICATIONS

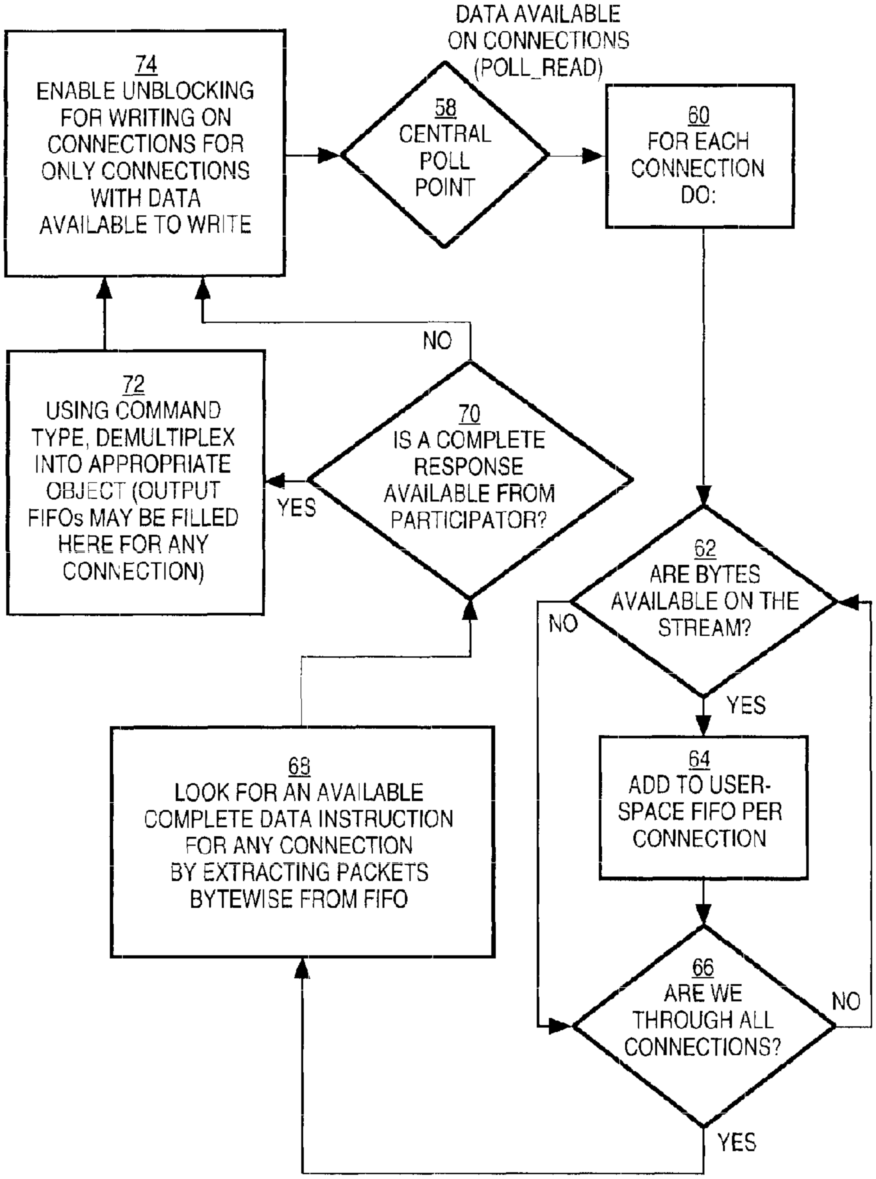

DATA AVAILABLE
ON CONNECTIONS
(POLL_READ)
74
ENABLE UNBLOCKING FOR WRITING ON CONNECTIONS FOR ONLY CONNECTIONS WITH DATA AVAILABLE TO WRITE
58
CENTRAL POLL POINT
60
FOR EACH CONNECTION DO:
NO
72
USING COMMAND TYPE, DEMULTIPLEX INTO APPROPRIATE OBJECT (OUTPUT FIFOs MAY BE FILLED HERE FOR ANY CONNECTION)
70
IS A COMPLETE RESPONSE AVAILABLE FROM PARTICIPATOR?
YES
62
ARE BYTES AVAILABLE ON THE STREAM?
NO
YES
68
LOOK FOR AN AVAILABLE COMPLETE DATA INSTRUCTION FOR ANY CONNECTION BY EXTRACTING PACKETS BYTEWISE FROM FIFO
64
ADD TO USER-SPACE FIFO PER CONNECTION
66
ARE WE THROUGH ALL CONNECTIONS?
NO
YES

FIG. 5

CLIENT CHANNEL DATA STRUCTURE AND INFORMATION FLOW DIAGRAM

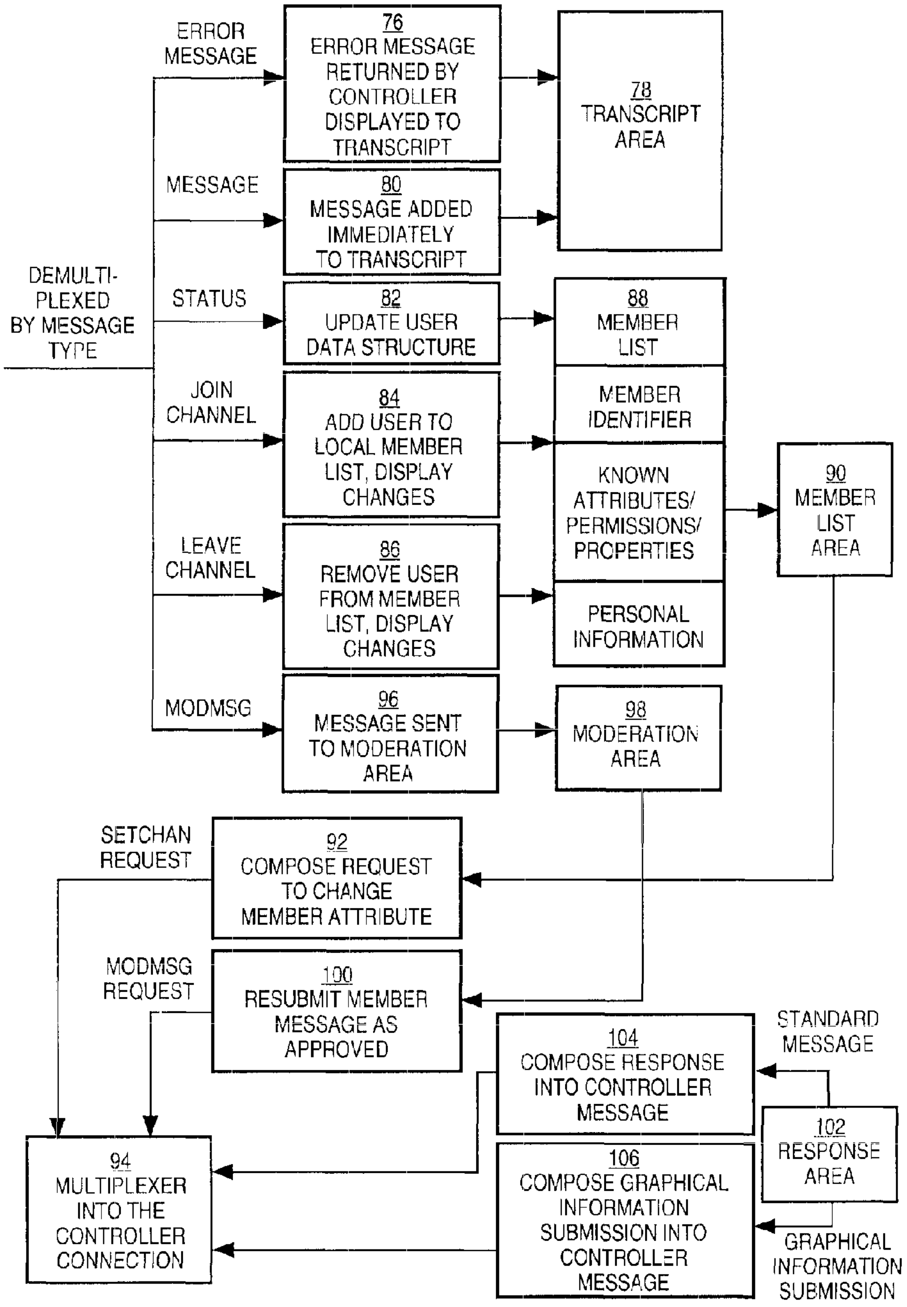

ERROR MESSAGE
76 ERROR MESSAGE RETURNED BY CONTROLLER DISPLAYED TO TRANSCRIPT
78 TRANSCRIPT AREA
MESSAGE
80 MESSAGE ADDED IMMEDIATELY TO TRANSCRIPT
DEMULTI-PLEXED BY MESSAGE TYPE
STATUS
82 UPDATE USER DATA STRUCTURE
88 MEMBER LIST
MEMBER IDENTIFIER
JOIN CHANNEL
84 ADD USER TO LOCAL MEMBER LIST, DISPLAY CHANGES
KNOWN ATTRIBUTES/ PERMISSIONS/ PROPERTIES
90 MEMBER LIST AREA
LEAVE CHANNEL
86 REMOVE USER FROM MEMBER LIST, DISPLAY CHANGES
PERSONAL INFORMATION
MODMSG
96 MESSAGE SENT TO MODERATION AREA
98 MODERATION AREA
SETCHAN REQUEST
92 COMPOSE REQUEST TO CHANGE MEMBER ATTRIBUTE
MODMSG REQUEST
100 RESUBMIT MEMBER MESSAGE AS APPROVED
104 COMPOSE RESPONSE INTO CONTROLLER MESSAGE
STANDARD MESSAGE
102 RESPONSE AREA
94 MULTIPLEXER INTO THE CONTROLLER CONNECTION
106 COMPOSE GRAPHICAL INFORMATION SUBMISSION INTO CONTROLLER MESSAGE
GRAPHICAL INFORMATION SUBMISSION

FIG. 6

PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM

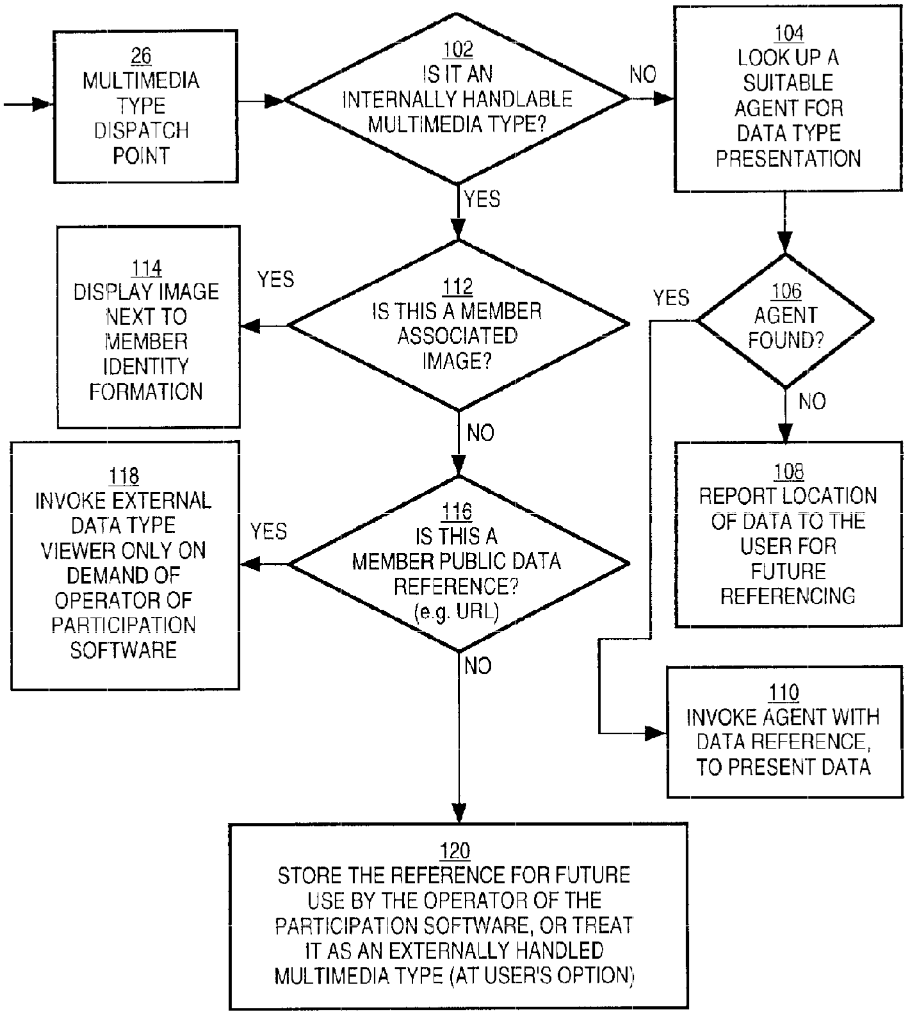
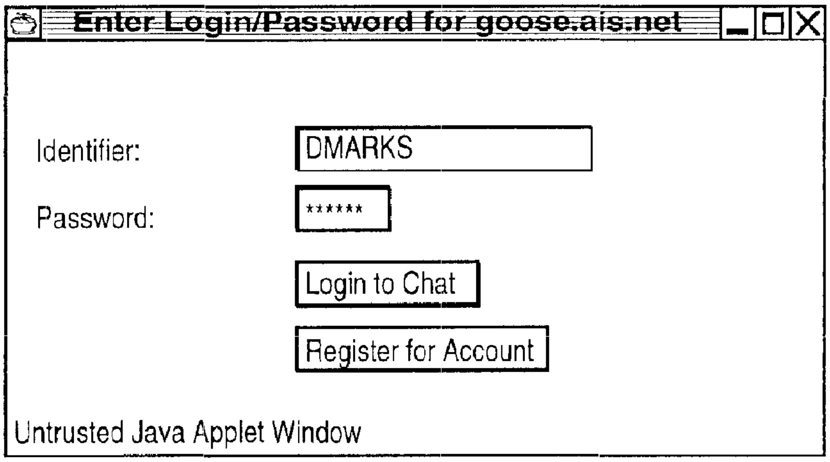

26 MULTIMEDIA TYPE DISPATCH POINT
102 IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104 LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114 DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112 IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106 AGENT FOUND?
NO
NO
118 INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116 IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
108 REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
NO
110 INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120 STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

FIG. 7



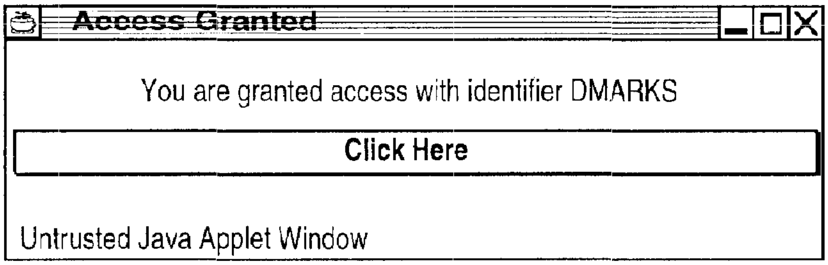
Enter Login/Password for goose.ais.net

Identifier: DMARKS

Password: ******

Untrusted Java Applet Window

FIG. 8

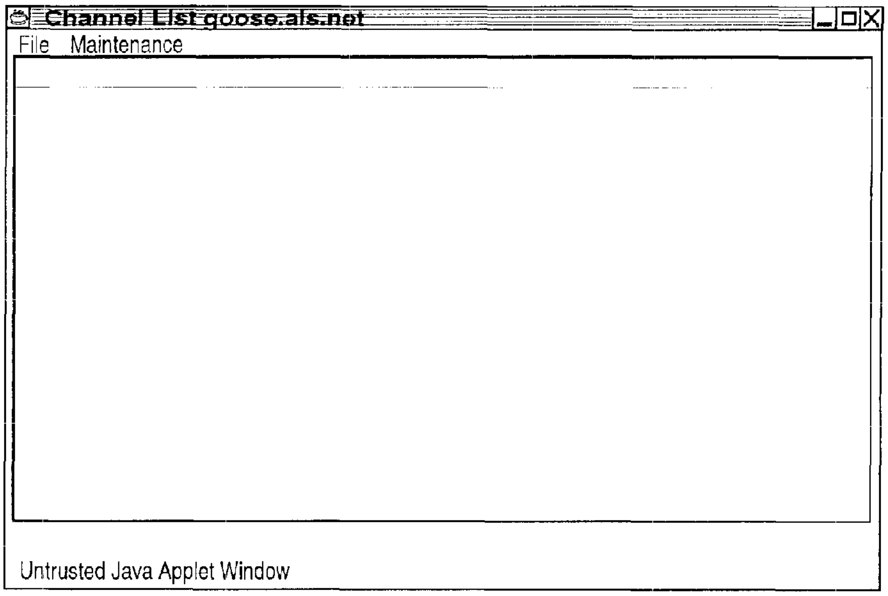


Access Granted

You are granted access with identifier DMARKS

Untrusted Java Applet Window

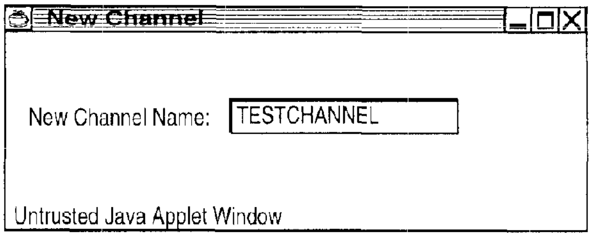
FIG. 9



Channel List goose.als.net

Untrusted Java Applet Window

FIG. 10

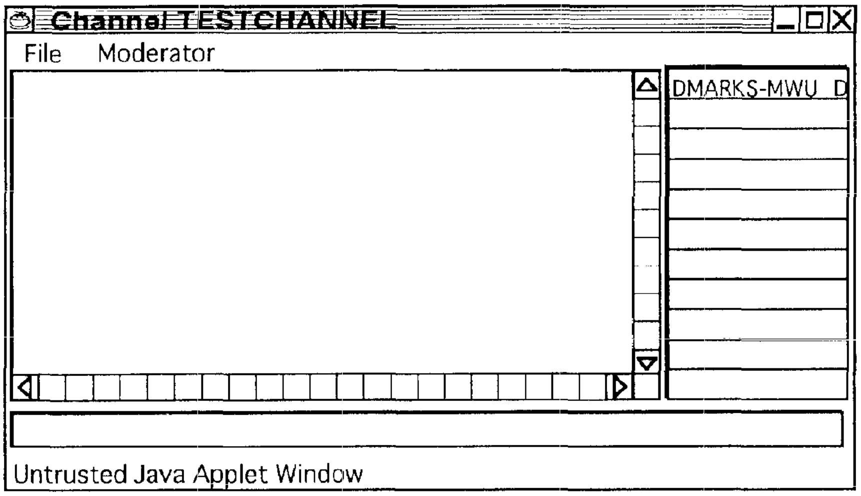


New Channel

New Channel Name: TESTCHANNEL

Untrusted Java Applet Window

FIG. 11



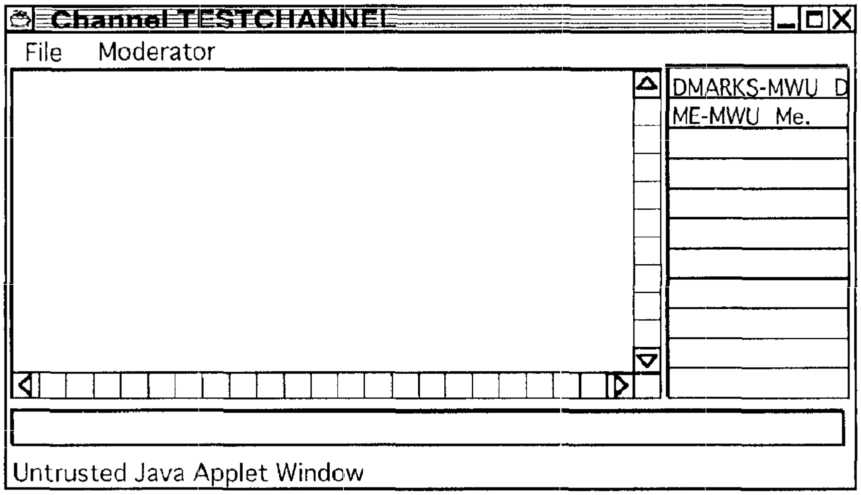
Channel TESTCHANNEL

File Moderator

DMARKS-MWU D

Untrusted Java Applet Window

FIG. 12



Channel TESTCHANNEL

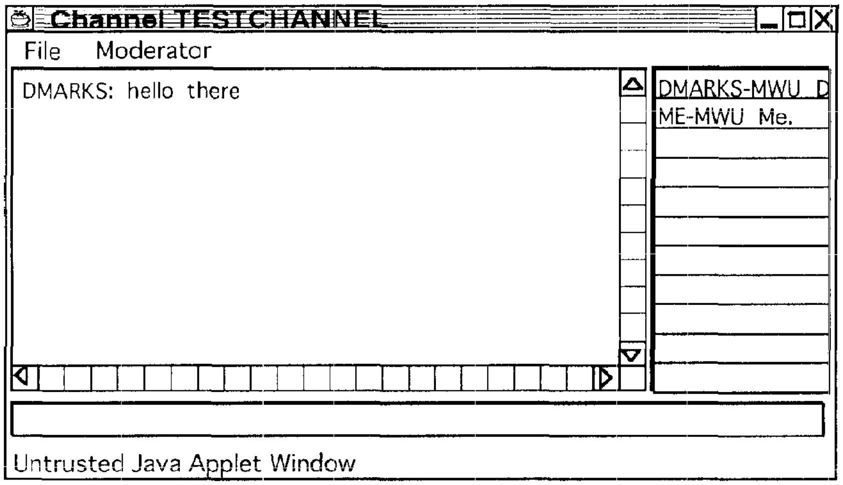
File Moderator

DMARKS-MWU D

ME-MWU Me.

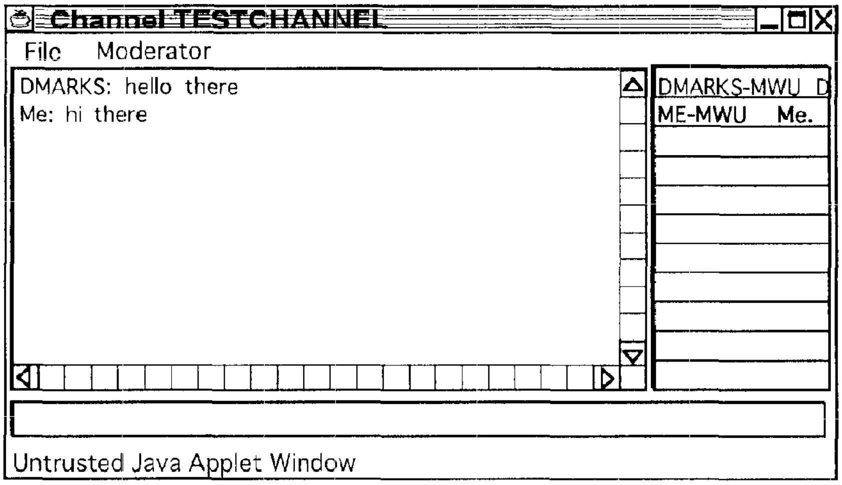
Untrusted Java Applet Window

FIG. 13



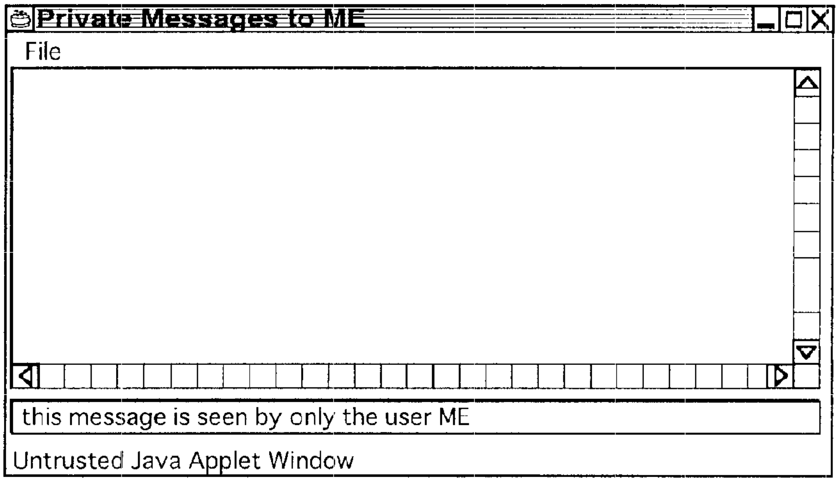
DMARKS: hello there

FIG. 14



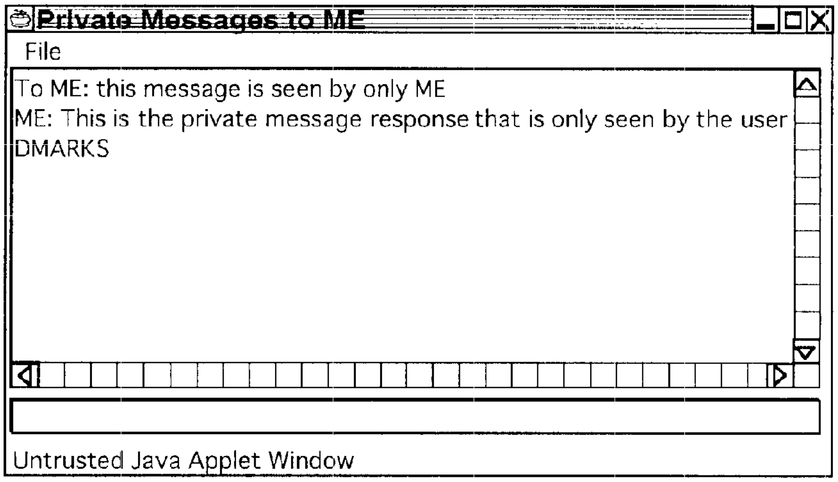
DMARKS: hello there
Me: hi there

FIG. 15



this message is seen by only the user ME

FIG. 16



To ME: this message is seen by only ME
ME: This is the private message response that is only seen by the user DMARKS

FIG. 17

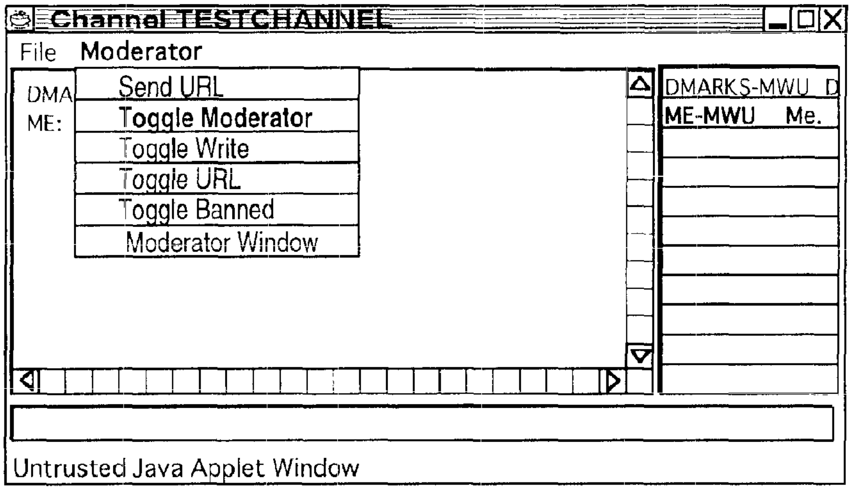
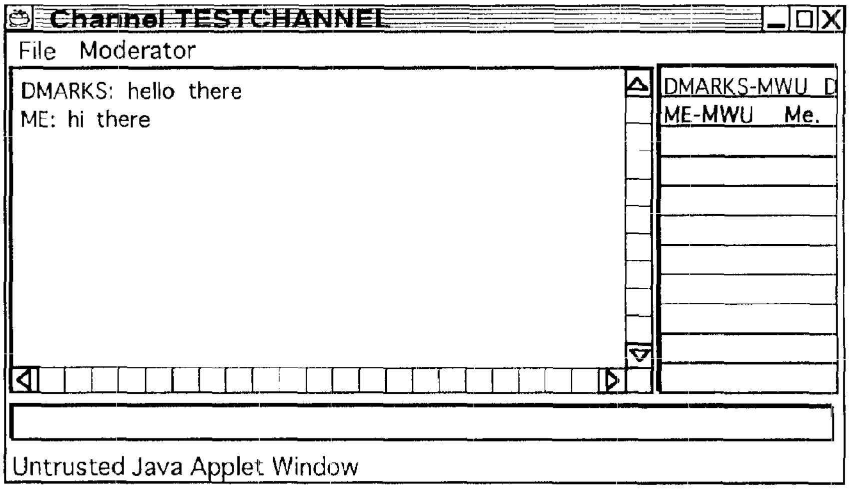
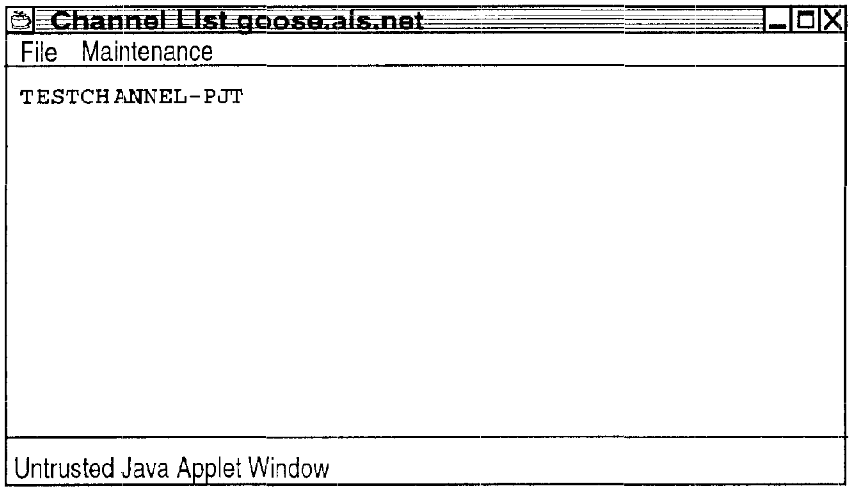


FIG. 18



DMARKS: hello there
ME: hi there

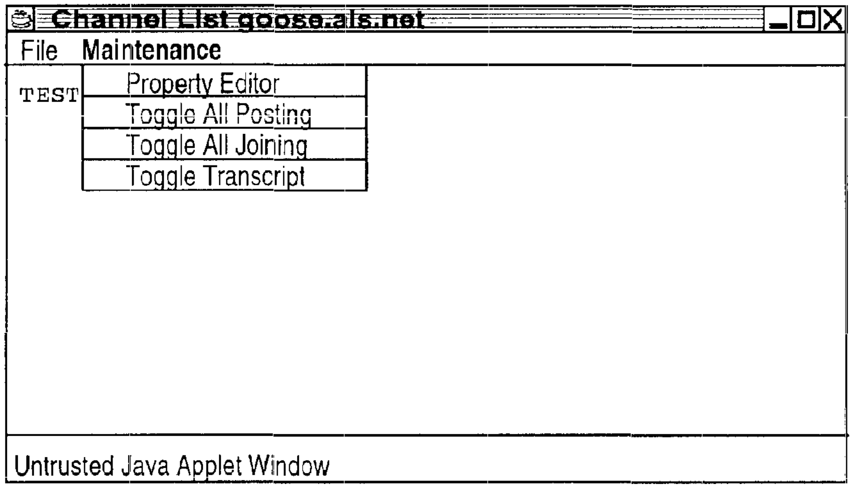
FIG. 19



TESTCH ANNEL-PJT

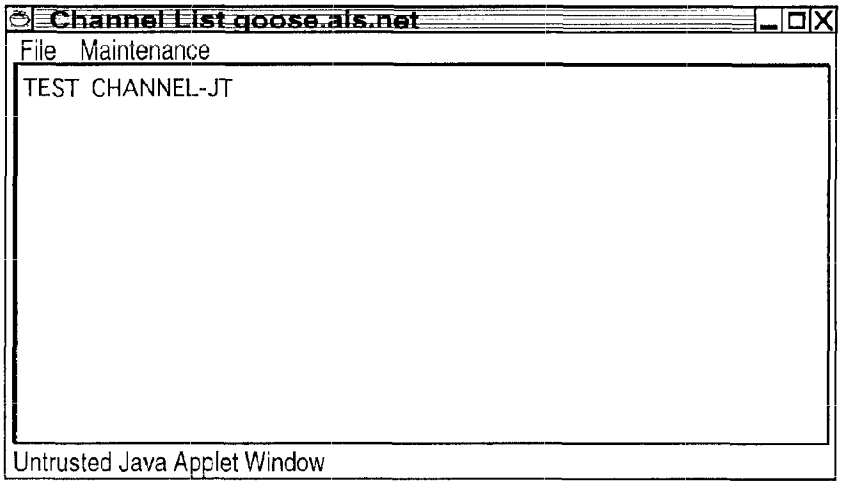
Untrusted Java Applet Window

FIG. 20



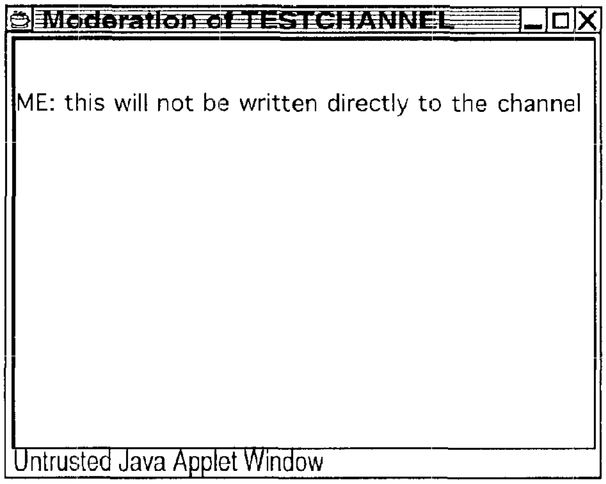
Untrusted Java Applet Window

FIG. 21



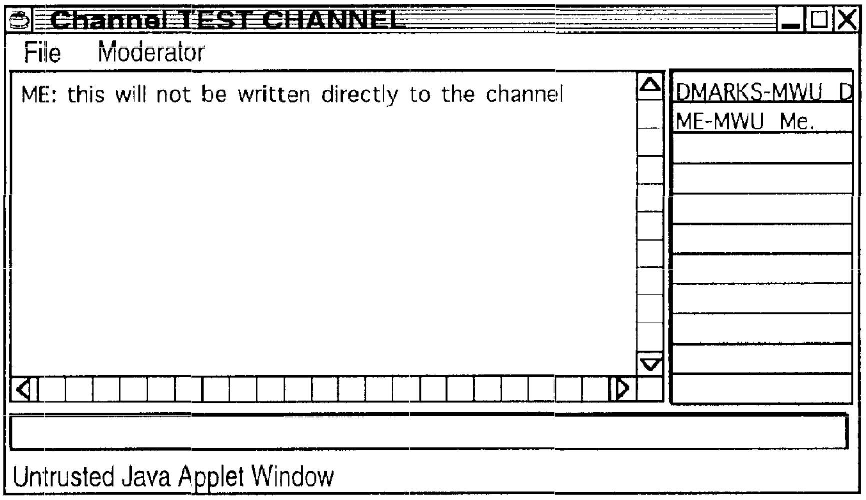
TEST CHANNEL-JT

FIG. 22



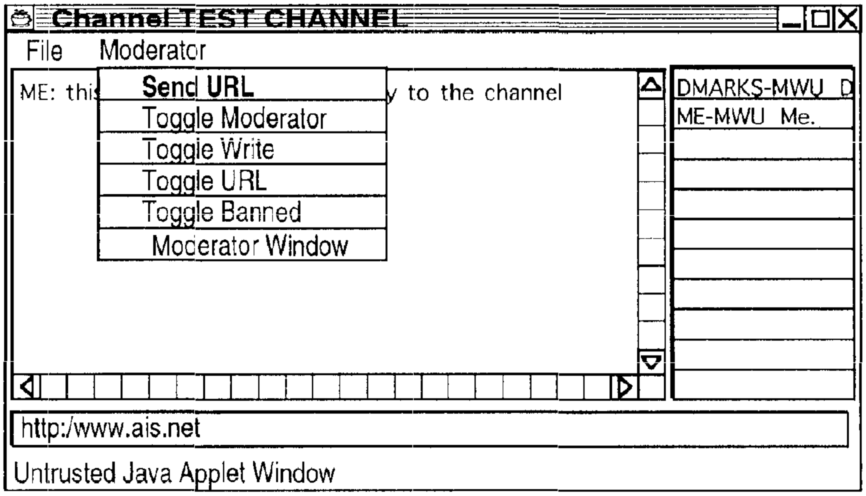
ME: this will not be written directly to the channel

FIG. 23



ME: this will not be written directly to the channel

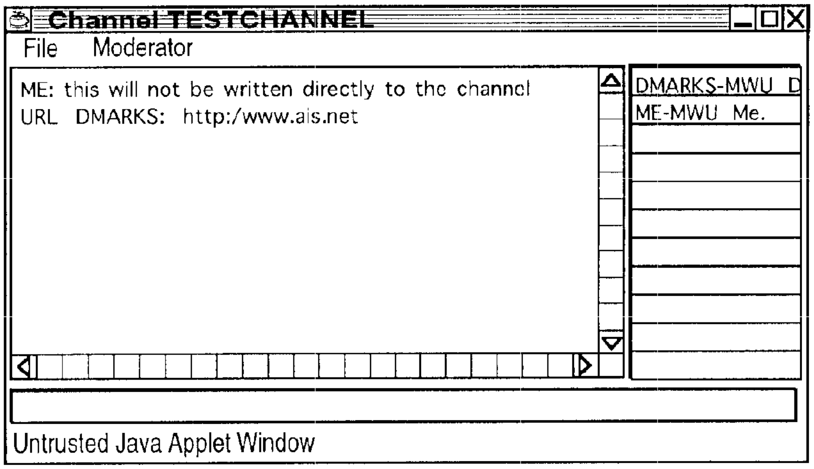
FIG. 24



ME: thi y to the channel

http:/www.ais.net

FIG. 25



ME: this will not be written directly to the channel
URL DMARKS: http:/www.ais.net

FIG. 26

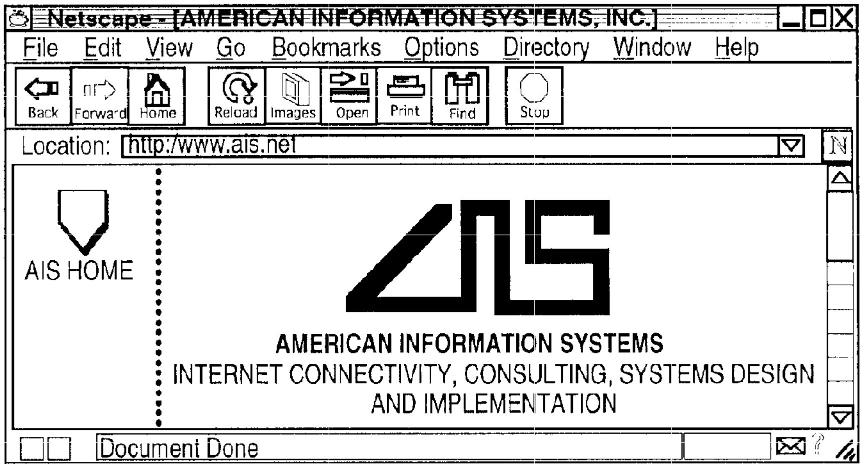
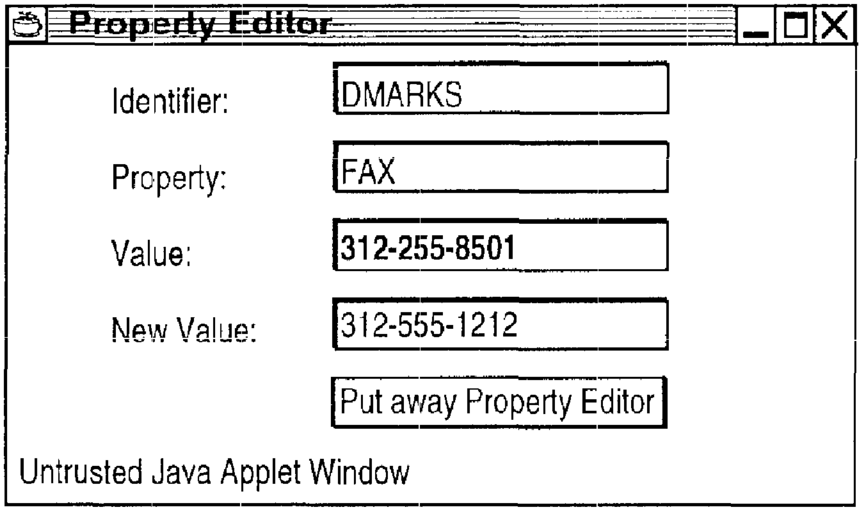

Netscape - [AMERICAN INFORMATION SYSTEMS, INC.]
File
Edit
View
Go
Bookmarks
Options
Directory
Window
Help
Back
Forward
Home
Reload
Images
Open
Print
Find
Stop
Location: http:/www.ais.net
AIS HOME
AIS
AMERICAN INFORMATION SYSTEMS
INTERNET CONNECTIVITY, CONSULTING, SYSTEMS DESIGN AND IMPLEMENTATION
Document Done

FIG. 27



Property Editor

Identifier: DMARKS

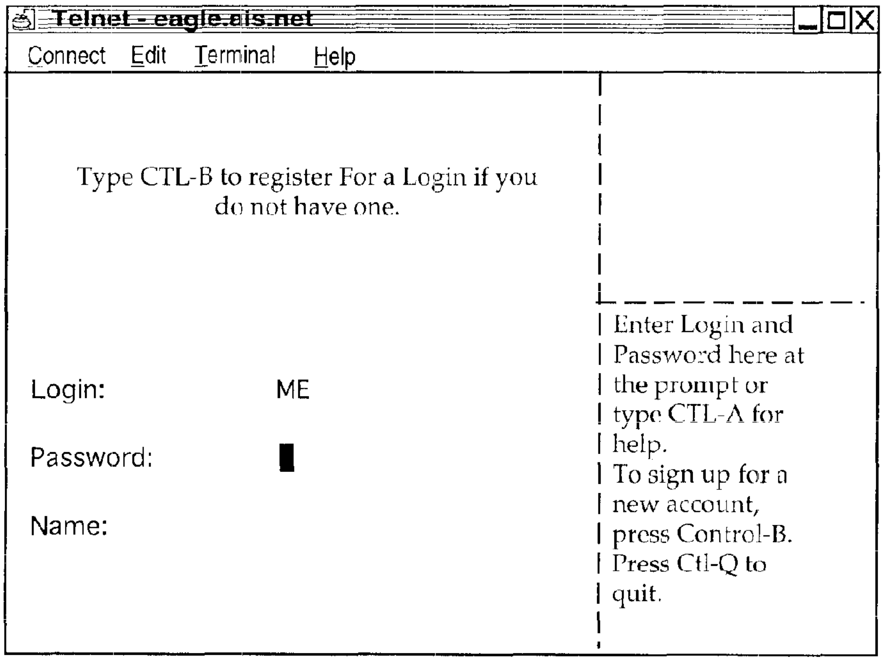
Property: FAX

Value: 312-255-8501

New Value: 312-555-1212

Untrusted Java Applet Window

FIG. 28



Type CTL-B to register For a Login if you do not have one.

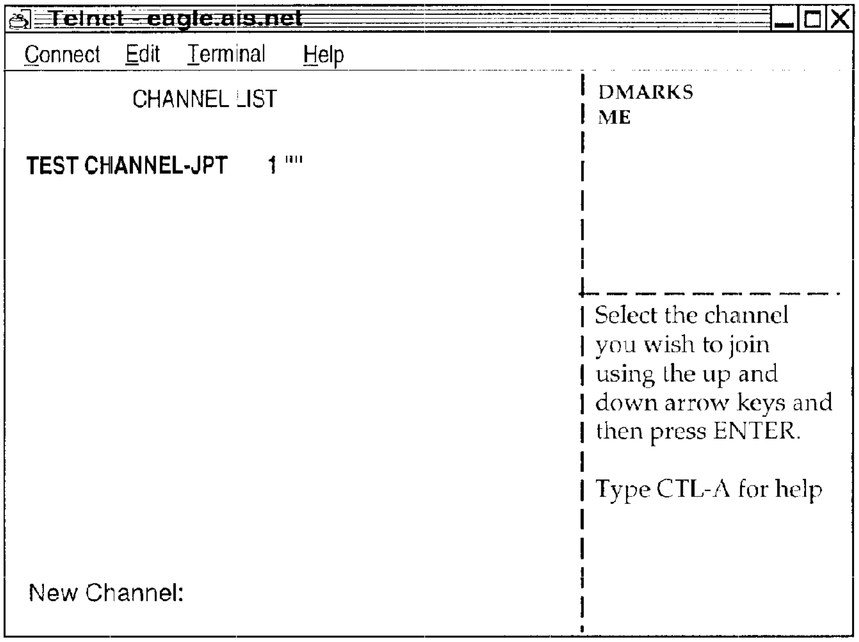
Login: ME

Password: █

Name:

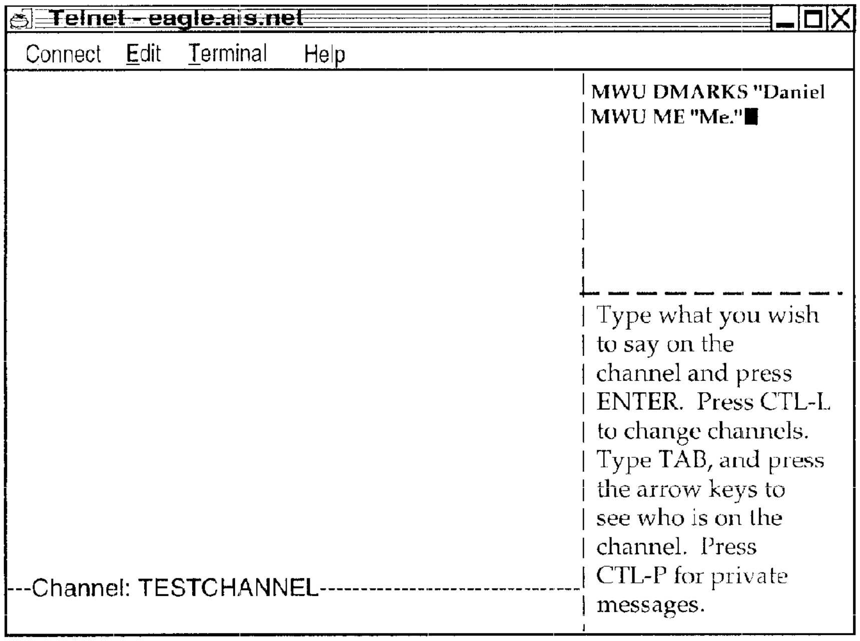
Enter Login and Password here at the prompt or type CTL-A for help.
To sign up for a new account, press Control-B.
Press Ctl-Q to quit.

FIG. 29



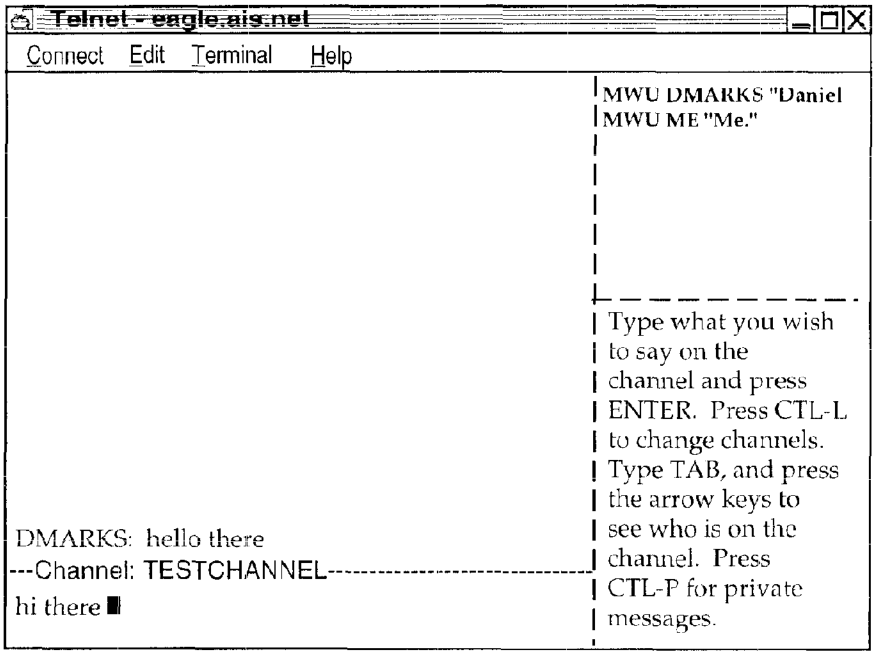
```
          CHANNEL LIST                               | DMARKS
                                                     | ME
TEST CHANNEL-JPT      1 ""                           |
                                                     |
                                                     |
                                                     |
                                                     |
                                                     L_ _ _ _ _ _ _ _ _ _ _
                                                     | Select the channel
                                                     | you wish to join
                                                     | using the up and
                                                     | down arrow keys and
                                                     | then press ENTER.
                                                     |
                                                     | Type CTL-A for help
                                                     |
                                                     |
 New Channel:                                        |
                                                     |
```

FIG. 30



```
                                                     | MWU DMARKS "Daniel
                                                     | MWU ME "Me."■
                                                     |
                                                     |
                                                     |
                                                     |
                                                     |
                                                     L_ _ _ _ _ _ _ _ _ _ _
                                                     | Type what you wish
                                                     | to say on the
                                                     | channel and press
                                                     | ENTER.  Press CTL-L
                                                     | to change channels.
                                                     | Type TAB, and press
                                                     | the arrow keys to
                                                     | see who is on the
                                                     | channel.  Press
---Channel: TESTCHANNEL------------------------------| CTL-P for private
                                                     | messages.
```

FIG. 31

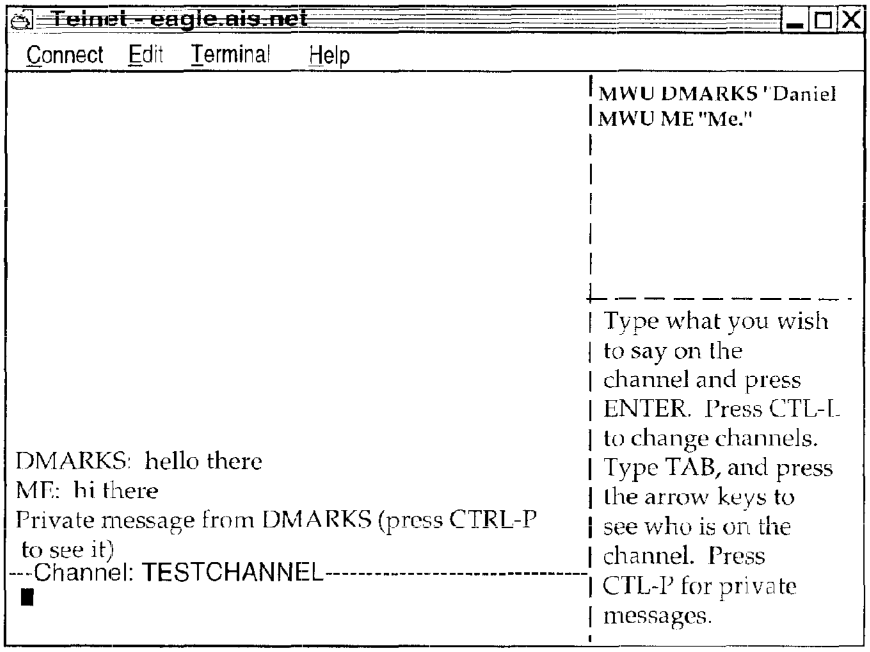


MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

DMARKS: hello there
---Channel: TESTCHANNEL--------------------------------
hi there █

FIG. 32

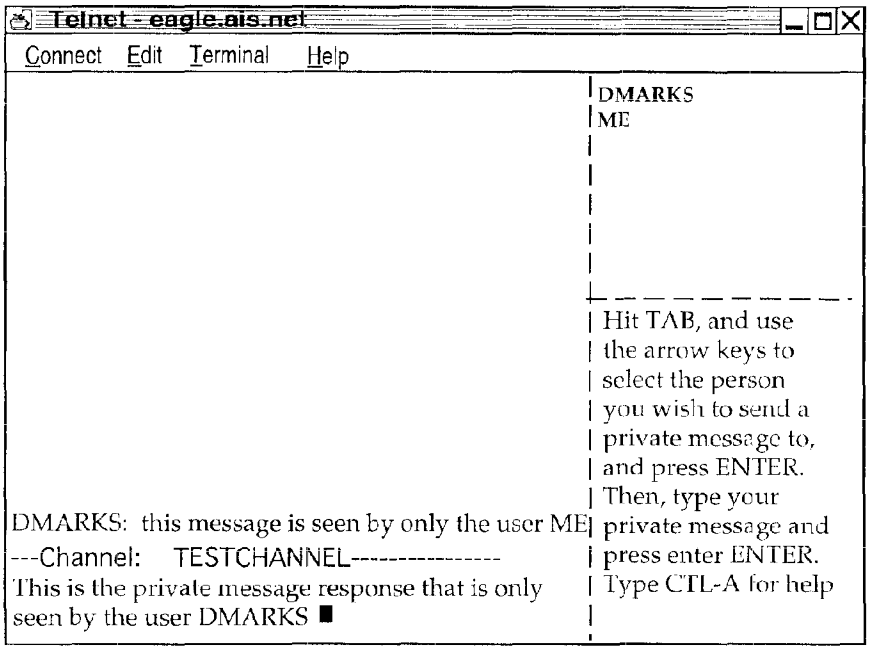


```
MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish
to say on the
channel and press
ENTER. Press CTL-L
to change channels.
Type TAB, and press
the arrow keys to
see who is on the
channel. Press
CTL-P for private
messages.

DMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P
 to see it)
---Channel: TESTCHANNEL--------------------------------
■
```

FIG. 33

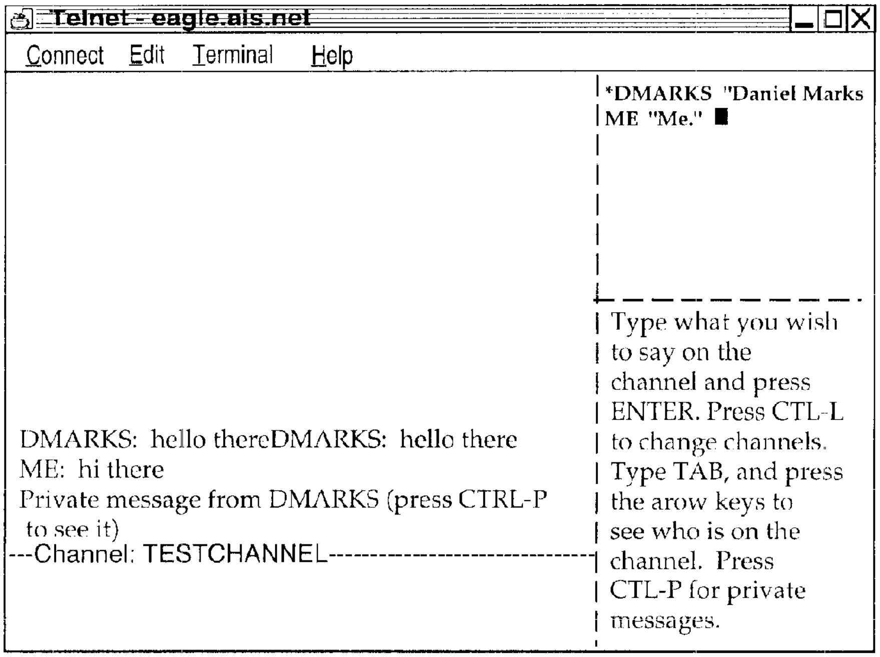


```
DMARKS
ME

Hit TAB, and use
the arrow keys to
select the person
you wish to send a
private message to,
and press ENTER.
Then, type your
private message and
press enter ENTER.
Type CTL-A for help

DMARKS: this message is seen by only the user ME
---Channel:   TESTCHANNEL----------------
This is the private message response that is only
seen by the user DMARKS ■
```

FIG. 34



*DMARKS "Daniel Marks
ME "Me." ■

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arow keys to see who is on the channel. Press CTL-P for private messages.

DMARKS: hello thereDMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P to see it)
---Channel: TESTCHANNEL------------------------------

## REAL TIME COMMUNICATIONS SYSTEM

### I. PRIORITY DATA

The present patent application is a continuation of and incorporates by reference U.S. patent application Ser. No. 09/399,578 filed by the same inventor on Sep. 20, 1999, and incorporates by reference U.S. patent application Ser. No. 08/617,658, now U.S. Pat. No. 5,956,491, titled Group Communications Multiplexing System that was filed by the same inventor on Apr. 1, 1996; and U.S. patent application Ser. No. 11/780,352 filed by the same inventor on Jul. 19, 2007, abandoned. U.S. patent application Ser. No. 09/399,578, filed Sep. 20, 1999, is a continuation of U.S. patent application Ser. No. 08/617,658, filed Apr. 1, 1996, issuing as U.S. Pat. No. 5,956,491, on Sep. 21, 1999.

### II. FIELD OF INVENTION

This invention is directed to an apparatus, a manufacture, and methods for making and using the same, in a field of digital electrical computer systems. More particularly, the present invention is directed to a digital electrical computer system involving a plurality of participator computers linked by a network to at least one of a plurality of participator computers, the participator computers operating in conjunction with the controller computer to handle multiplexing operations for communications involving groups of some of the participator computers.

### III. BACKGROUND OF THE INVENTION

Multiplexing group communications among computers ranges from very simple to very complex communications systems. At a simple level, group communications among computers involves electronic mail sent in a one way transmission to all those in a group or subgroup using, say, a local area network. Arbitrating which computers receive electronic mail is a rather well understood undertaking.

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

Even more complex is linking of computers to communicate in what has become known as a "chat room." Chat room communications can be mere text, such as that offered locally on a file server, or can involve graphics and certain multimedia capability, as exemplified by such Internet service providers as America On Line. Multiplexing in multimedia is more complex for this electronic environment.

On the Internet, "chat room" communications analogous to America On Line have not been developed, at least in part because Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications. Further, unlike the an Internet service provider, which has control over both the hardware platform and the computer program running on the platform to create the "chat room", there is no particular control over the platform that would be encountered on the Internet. Therefore, development of multiplexing technology for such an environment has been minimal.

Even with an emergence of the World Wide Web, which does have certain graphical multimedia capability, sophisticated chat room communication multiplexing has been the domain of the Internet service providers. Users therefore have a choice between the limited audience of a particular Internet Service provider or the limited chat capability of the Internet.

### IV. SUMMARY OF THE INVENTION

It is an object of the present invention to overcome such limitations of the prior art and to advance and improve the technology of group computer multiplexing to enable better computerized group communications.

It is another object of the present invention to provide a computerized human communication arbitrating and distributing system.

It is yet another object of the present invention to provide a group communication multiplexing system involving a controller digital computer linked to a plurality of participator computers to organize communications by groups of the participator computers.

It is still another object of the present invention to link the controller computer and the plurality of computers with respective software coordinated to arbitrate multiplexing activities.

It is still a further object of the present invention to provide a chat capability suitable for handling graphical, textual, and multimedia information in a platform independent manner.

These and other objects and utilities of the invention, which apparent from the discussion herein, are addressed by a computerized human communication arbitrating and distributing system. The system includes a controller digital electrical computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information and an output device for presenting information to a user having a user identity. A connection such as the Internet links the controller computer with each of the participator computers.

Controller software runs on the controller computer, programming the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups communicating through the controller computer and to distribute real time data to the respective ones of the groups.

Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message. The controller computer also conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

Therefore, for a computer system involving a plurality of programmed participator computers running the participator computer program can interact through a programmed controller computer with the controller computer multiplexing the communications for groups formed from the plurality, as well as arbitrating communications behavior.

### V. BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a depiction of hardware suitable for performing the present invention;

FIG. **2** is a communications overview of the present invention.

FIG. **3** is a data and communications dependency diagram for the controller group channel structure of the present invention.

FIG. **4** is a flow chart of the central controller loop communications for the controller computer.

FIG. **5** is a client channel data structure and information flow diagram of the present invention.

FIG. **6** is a participator software out-of-band multimedia information flow diagram of the present invention.

FIG. **7** is an illustration of a login/password screen of the present invention.

FIG. **8** is an illustration of a confirmation screen of the present invention.

FIG. **9** is an illustration of a channel list area screen of the present invention.

FIG. **10** is an illustration of a New Channel option pull-down menu screen of the present invention.

FIG. **11** is an illustration of a member on a new channel screen of the present invention.

FIG. **12** is an illustration of a second member on the new channel screen of the present invention.

FIG. **13** is an illustration of a communication on the new channel screen of the present invention.

FIG. **14** is an illustration of a private message window on the new channel screen of the present invention.

FIG. **15** is an illustration of a private message displayed on the private message window on the new channel screen of the present invention.

FIG. **16** is a further illustration of the private message on the private message window on new channel screen of the present invention.

FIG. **17** is an illustration of an attribute revocation on the new channel screen of the present invention.

FIG. **18** is a further illustration of the new channel screen of the present invention.

FIG. **19** is an illustration of the channel list window screen of the present invention.

FIG. **20** is an illustration of the toggle posting option on a screen of the present invention.

FIG. **21** is an illustration of a moderated version of the new channel screen of the present invention.

FIG. **22** is an illustration of a communication on a moderation window screen of the present invention.

FIG. **23** is an illustration of the communication passed on to the moderated version of the new channel screen of the present invention.

FIG. **24** is an illustration of a communication, for sending a graphical multimedia message, on to the moderated version of the new channel screen of the present invention

FIG. **25** is an illustration of a communication, for passing a URL (Uniform Resource Locator) to channel members, on a moderator pull-down menu screen of the present invention.

FIG. **25** is an illustration, showing the name of the URL, on a moderated version of the new channel screen of the present invention.

FIG. **26** is an illustration of data associated with the graphical multimedia message on a moderated version of the new channel screen of the present invention.

FIG. **27** is an illustration of a proprietary editor, suitable for a dialog to change tokens, on a screen of the present invention.

FIG. **28** is an illustration of a text-based interface login/password screen of the present invention.

FIG. **29** is an illustration of a text-based interface group screen of the present invention.

FIG. **30** is another illustration of a text-based interface group screen of the present invention.

FIG. **31** is another illustration of a text-based interface group screen of the present invention.

FIG. **32** is an illustration of a text-based interface private message screen of the present invention.

FIG. **33** is another illustration of a text-based interface private message screen of the present invention.

FIG. **34** is another illustration of a text-based interface group with moderator screen of the present invention.

## VI. DETAILED DESCRIPTION OF THE DRAWINGS

In providing a detailed description of a preferred embodiment of the present invention, reference is made to an appendix hereto, including the following items.

Appendix Contents

ALLUSER C
ALLUSER H
CHANNEL C
CHANNEL H
CHANNEL HLP
CLIST C
CLIST H
CLIST HLP
EDITUSER C
EDITUSER H
ENTRYFRM C
ENTRYFRM H
ENTRYFRM HLP
HELP C
HELP H
HELPSCR C
HELPSCR H
LINEEDIT C
LINEEDIT H
LIST C
LIST H
LOGIN HLP
MAIN C
MAKEFILE
MESSAGE C
MESSAGE H
MODERAT HLP
PRIVATE C
PRIVATE H
PRIVATE HLP
SOCKIO C
SOCKIO H
STR C
STR H
UCCLIENT
USER C
USER H
WINDOW C
WINDOW H

Note that the appendix includes code for two different embodiments: a Tellnet embodiment and a JAVA embodiment. Documentation and error messages, help files, log files, are also included in the appendix. While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled.

Referring now to FIG. **1**, the overall functioning of a computerized human communication arbitrating and distributing System **1** of the present invention is shown with odd numbers designating hardware or programmed hardware, and even numbers designating computer program logic and data flow. The System **1** includes a digital Controller Computer **3**, such as an Internet service provider-type computer. The Controller Computer **3** is operating with an operating system.

System **1** also includes a plurality of digital Participator Computers **5**, each of which may be an IBM-compatible personal computer with a processor and a DOS operating system. Each of the Participator Computers **5** includes an Input Device **7** for receiving human-input information from a respective human user. The Input Device **7** can be, for example, a keyboard, mouse or the like. Each of the Participator Computers **5** also includes an Output Device **9** for presenting information to the respective user. The Output Device **9** can be a monitor, printer (such as a dot-matrix or laser printer), or preferably both are used. Each of the Participator Computers **5** also includes a Memory **11**, such as a disk storage means.

The System **1** includes a Connection **13** located between, so as to link, the Controller Computer **3** with each of the Participator Computers **5**. The Connection **13** can be an Internet or more particularly, a World Wide Web connection.

The Controller Computer **3** is running and under the control of Controller Software **2**, which directs the Controller Computer **3** to arbitrate in accordance with predefined rules including a user identity, which ones of the Participator Computers **5** can interact in one of a plurality of groups through the Controller Computer **3** and to distribute real time data to the respective ones of the groups.

The Participator Computers **5** are each running and under the control of Participator Software **4**, which directs each of the Participator Computers **5** to handle a user Interface **6** permitting one said user to send a multimedia information Message **8** to the Controller Computer **3**, which arbitrates which of the Participator Computers **5** receives the multimedia information Message **8** and which conveys the multimedia information Message **8** to the selected participator computers **5** to present the multimedia information Message **8** to the respective user.

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**.

Turning now to FIG. **2**, there is shown a communications overview of the present invention. Beginning with the Controller Computer Software **2**, reference is made to Block **10**, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **10** links to Block **12**, which is illustrative of channel A . . . . Block **10** also links to Block **14**, which illustrates handling private message A. Block **10** also links to Block **16**, illustrative of handling out-of-band media. Block **10** additionally links to Block **18**, which illustrates asynchronous status messages.

Multiple connections between the controller computer **3** and a plurality of participator computers **5** permit communication implemented via the interplay of controller software **2** and participator software **4**. With particular regard to the participator software **4** illustrated in FIG. **2**, Block **20** is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **20** links to Block **22**, which is illustrative of channel A . . . . Block **20** also links to Block **24**, which illustrates handling private message A. Block **20** also links to Block **26**, illustrative of handling out-of-band media via Block **28**, which is illustrative of a Web browser or auxiliary computer program. Block **20** also links to Block **30**, which illustrates asynchronous status message handling via Block **32**, illustrative of user interface objects windows and screens.

De/multiplexing via API provides a "virtual connection" between Channel, Private Message, and Multimedia objects in the controller computer **3** and each participator computer **5**. An alternate architecture is to allow for a separate connection between each object so that multiplexing/demultiplexing is not necessary and each object handles its own connection. This would influence system performance, however.

Turning now to FIG. **3**, a data and communications dependency diagram controller group channel structure is illustrated. Beginning from what is designated as a portion of Block **10** the logic flows to Block **34** to consider JOIN, LEAVE, STATUS, SETCHAN API instructions. Block **34** examines member list maintenance instructions, accessing Block **36** to check permissions, list users, and change attributes. Note the exploded window **38** shows a display of member information including a user's name, personal information, and attributes/properties/permissions (operations involving the subsequently discussed tokens), i.e., stored per channel attributes under each member. In any case, confirmation or denial of access is communicated via Block **40** for multiplexing return of status messages to a target object.

From the portion of Block **10**, the logic flows to Block **42** for MESSAGE and MODMSG API instructions. Block **42** tests which of the two instructions were received, and for MODMSG, the logic flows to Block **44**, which tests whether the user is a moderator. If the user is not a moderator, the logic flows to Block **46**, which sends a denial message through Block **40**. If, however, the in Block **44** the user is a moderator, the logic flows to Block **48** for a repeat to all list members who are permitted to see the message, via Block **40**.

Returning to Block **42**, if MESSAGE is detected, the logic flows to Block **50**, which tests whether a user has post permission. If the user has post permission, the logic flows to Block **48**, etc. If the user does not have post permission, the logic flows to Block **52** to forward the message to moderators for approval, via Block **40**.

Additionally, the logic flows from Block **10** to Block **54** for a URL API instruction. Block **54** tests whether the user has graphical multimedia communication privileges, and if not, the logic flows via Block **56**, which sends a denial message via Block **40**. Otherwise, if the user does have graphical multimedia communications privileges in Block **54**, Block **58** sends graphical multimedia information to all approved users via Block **40**.

Turning now to FIG. **4**, central controller loop communications is illustrated. For the data on central poll point **58** (see Appendix POLL_POINT), a "do" loop begins at Block **60** for each connection. Block **62** tests whether bytes are available on the data stream. If they are, the bytes are added to user space FIFO per connection at Block **64**, leading to Block **66**, which tests whether there are any more connections. Note that in FIG. **4**, if there are no more bytes available in Block **62**, the logic skips to Block **66**, and if Block **66** is not finished with all connections, the loop returns to Block **62**. When all connections have been completed in Block **62**, the logic flows to Block **68**, which looks for an available complete data instruction for any connection by extracting packets byte-wise from the FIFO. Thereafter, Block **70** tests whether there is a complete response available from the participator computer. If the response is complete, the logic flows to Block **72** which, using a command type, demultiplexes into an appropriate object (output FIFOs may be filled here for any connection). The logic from Block **72** joins the "no" branch from Block **70** at

Block **74**, which enables unblocking for writing connections for only connections with data available to write, looping back to Block **58**.

FIG. **5** shows a client channel data structure and information flow diagram. From a message that is demultiplexed by message type, there are six possibilities: ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG. ERROR MESSAGE is communicated to Block **76**, where the error message is displayed to the transcript in the transcript area of Block **80**. MESSAGE is communicated to Block **78** where the message is immediately added to the transcript in transcript area **78**. STATUS is communicated to Block **82** to update user data structure; JOINCHANNEL is communicated to Block **84** to remove a user from the member list and display the change; and LEAVECHANNEL is communicated to Block **86**. From Block **82**, Block **84**, and Block **88**, the logic flows to Block **88**, which includes a member list, a member identifier, known attributes/permissions/properties, and personal information. From Block **88**, the logic proceeds to Block **90**, a member list area, and on to Block **92** to compose a request to change a member attribute. This "SETCHAN request is then communicated to Block **94**, which is the multiplexer leading to the controller computer connection.

MODMSG is communicated to Block **96**, which sends the message to the moderation area of Block **98**, and then to Block **100** to resubmit a member message as approved, thereby conveying a MODMSG request to Block **94**.

Note that a response is prepared in the response area of Block **102**. If the response is a standard message, it is conveyed to Block **104** to compose the response into a controller message, thereby sending a MESSAGE request to box **94**. If, however, the message is a graphical information submission, the logic flows from Block **102** to Block **106** to compose the graphical information submission into a controller message, thereby sending a URL request to Block **94**.

FIG. **6** is a participator software out-of-band multimedia information flow diagram, which begins with Block **26**, the multimedia type patch point. Block **26** leads to Block **102**, which tests whether there is an internally handlable multimedia type. If not, Block **104** looks up a suitable agent for data type presentation, which leads to Block **106**, which tests whether an agent was found. If not, Block **108** reports location of data to the user for future referencing. If the agent is found in Block **106**, the logic flows to Block **110**, which invokes the agent with a data reference to present the data.

If the multimedia type is internally handlable from Block **102**, the logic flows to Block **112**, which tests whether this is a member associated image. If it is a member associated image, Block **114** displays the image next to member identity information, and if it is not, the logic flows to Block **116**, which tests if this is a member public data reference (e.g., a URL). 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).

With further regard to the manner of interaction between the controller computer **3** and the participator computers **5**, and their respective computer programs **2** and **4**, includes a moderation capability that is controlled, or arbitrated, pursuant to system **1** recognizing user identity. Note that using the user identity for moderation purposes is a use additional to the use of the user identity for security purposes.

One embodiment of the present invention is to bring chat capability to the internet and World Wide Web. However, another embodiment involves non-internet relay chat. In either embodiment, System **1** is state driven such that synchronous and asynchronous messages can be communicated. For an asynchronous notification, each message is sent through the system **1** (API), which updates the information on the output device of the participator computers **5**. For a synchronous notification, a participator computer **5** must interrogate the system **1** for a message.

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. The control computer database serves as a repository of tokens for other programs to access, thereby affording information to otherwise independent computer systems. In the database, the storage of tokens can be by user, group, and content, and distribution controls can also be placed on the user's tokens as well as the database.

Each token is used to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process. The arbitration also includes controlling a user's ability to moderate communications involving a group or subgroup of the participator computers **5**. Once in a group, temporary tokens are assigned for priority to moderate/submoderate groups (a group is sometimes known as a channel in multiplexing terminology).

Accordingly, tokens are used by the controller computer **5** to control a user's group priority and moderation privileges, as well as controlling who joins the group, who leaves the group, and the visibility of members in the group. Visibility refers to whether a user is allowed to know another user is in the chat group.

Tokens are also used 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.

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

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

With regard to controlling communications in a group (which is in essence a collection of user identities), control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages.

Note that tokens for members in group can involve multiples formed in real time, say, within the span of a conversation. For example, for private communication, tokens are immediately formed to define a group of 2 users. Hierarchical groups within groups can also be formed, with each inheriting the properties of the group before it. Thus, a subgroup can include up to all members or more by adding any surplus to the former group.

With further regard to the controller computer **3**, e.g., a server, information is controlled for distribution to the user interfaces at selected ones of the participator computers **5**. The controller computer program, in one embodiment, can be a resident program interface (such as a JAVA application). There can be a token editor object (window/tear down, etc.)

per group, private communication, user, channel listings, user listings, etc. Each can link up in a token hierarchy for arbitration control.

The controller computer **5**, by means of the controller computer program **2**, keeps track of states and asynchronous messages as well as generating a synchronous message as a user logs in or interrogates system **1**.

With regard to multimedia information messages **8**, such messages are of independent data types, e.g., audio/video data types. The content of the message (e.g., a URL) permits the System **1** to automatically determine the handling of the message: either the Controller Computer **3** passes the content of Message **8** directly, or the Controller Computer **3** determines from the Message **8** how to find the content, say via Netscape. Accordingly, Message **8** can communicate video and sound (or other multimedia, e.g., a URL) to users, subject only to the server arbitration controls over what can be sent.

Turning now to an illustration of using the invention, the session starts with verifying the user's identity (at FIG. **7**). The login/password screen is shown, and the user enters his/her assigned login/password combination and clicks the "Login To Chat" button. If the password was entered correctly, a confirmation box appears on the screen.

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

To create a new group, the "New Channel" option is selected from a pull-down menu (at FIG. **9**). The name of the channel is entered by the input device **7**.

If the user has permission (this one does), a new channel is created for the group (at FIG. **10**). The window that displays the channel area has three regions: the bottom region, where responses are entered; the largest region, where a transcript of the communication is followed; and the rightmost region, which lists the group's current members. This list is continuously updated with asynchronously generated status messages received immediately when a new member joins the group. Only "DMARKS" is currently in this group. The "MWU" is the properties currently associated with DMARKS—the ability to moderate, write to the channel, and send multimedia messages.

A new member has joined the channel, and the member list status area is updated right away (at FIG. **11**). This new member has a login of "ME."

The user DMARKS now types "hello there" into the response area and presses RETURN (at FIG. **12**). This message is passed to the controller computer **5**, which sends the message to all channel members, i.e., those using participator computers **5**, including DMARKS.

The user ME now sends a message to the controller: "hi there" (at FIG. **13**). This message is also sent to all members by the controller computer **5**. Now user DMARKS clicks (using input device **7**, a mouse) on the name of the user "ME" in the member list window. The participator software **4** will now create a private message window, so that the users ME and DMARKS can exchange private messages. Private messages are only sent to the intended recipient by the controller, and no one else.

A private message window appears in response to DMARKS's request to open private communications with ME (at FIG. **14**). Now DMARKS types a message into the private message window's response area to ME: "this message is seen only by the user ME." When complete, the participator software **4** will forward this message to the controller computer **3**.

In response, the user ME has entered "This is the private message response that is only seen by the user DMARKS," which has been forwarded to user DMARKS (at FIG. **15**). This message is displayed immediately on DMARKS's window.

DMARKS now returns to the channel window for the group "TESTCHANNEL" (at FIG. **16**). To modify the permission attributes associated with user ME on the channel TEST CHANNEL, DMARKS (who is a moderator of the channel), clicks on the user ME in the member list to select ME, pulls down the Moderator menu, and selects "Toggle Moderator." This removes the moderator privileges from ME.

As a result of the attribute revocation, the "M" has disappeared from next to ME's name in the member list (at FIG. **17**), indicating that the property is no longer associated with the user ME.

Now DMARKS returns to the Channel List window (at FIG. **18**). DMARKS wishes to fully moderate the contents of the channel TESTCHANNEL, censoring all unwanted communications to the channel. DMARKS returns to the channel list, and selects the channel TESTCHANNEL by clicking on its name in the channel list.

Now DMARKS selects the "Toggle All Posting" option in the Maintenance pull-down menu (at FIG. **19**). This will turn off the channel property "posting," (or sending communications to the channel without moderator approval) which will be indicated by the removal of the letter "P" from next to the name TESTCHANNEL (at FIG. **20**).

Now the letter "P" is removed from after the name TESTCHANNEL in the Channel List window (at FIG. **21**), indicating that this channel is now moderated and will only have free posting ability by designated members.

Now, type user ME (who is also on channel TESTCHANNEL) wishes to send communications: "this will not be written directly to the channel" (at FIG. **22**). The controller, instead of sending it immediately to the channel to be seen by all members, will instead forward the message to the moderators for approval. The moderator, DMARKS, will then see the message on the Moderation Window, which provides a preview of any messages to be sent. To approve a message for general viewing, DMARKS now clicks on the message.

Now that DMARKS has clicked directly on the message, it is displayed inside the group's Channel window for all members to see (at FIG. **23**).

DMARKS now wishes to send a graphical multimedia message. This implementation sends graphical multimedia images by allowing a channel member to specify an Internet URL of a graphical multimedia resource to be presented to the group members. In this example, DMARKS wishes to send the URL "http://www.ais.net" (corresponding to the World Wide Web home page of American Information Systems, Inc.) to the channel members. DMARKS enters the URL into the response window, and selects "Send URL" from the Moderator pull-down menu (at FIG. **24**).

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.

Finally, DMARKS wishes to manually modify the attribute tokens associated with the user (at FIG. **27**). The user invokes the Property Editor dialog, which allows the user to view and change the tokens associated with a user. A property of a given user is determined by the Identifier and Property names. An old value of the property is shown, and a token value can be changed in the "New Value" field. With this property editor, a user with sufficient permissions (tokens) can change any of the tokens or security parameters of any user, or a user's ability to change security parameters can be restricted.

To start with an alternate embodiment using a text-based interface, a user is presented by the login/password screen (at FIG. **28**). This screen is where a user enters the information that proves his/her identity. The user must now enter his/her login and password to identify themselves.

After the user has been identified by the controller the Channel List screen appears (at FIG. **29**). The names of channels and their associated properties are shown on this screen. By using the arrow keys and highlighting the desired channel, ME may enter any publicly joinable group. Currently, there is only one group TESTCHANNEL, which ME will join.

Now the screen for the channel TESTCHANNEL appears (at FIG. **29**). The screen is split into four regions. The bottom left region is the response line, where messages users wish to enter appear. The upper left region is the transcript area where the communications of the group's channel appear as they occur. The upper right region is the Member List region, where a continuously updated list of members' names appear, with their attributes.

A message appears in the transcript area. The controller has forwarded a message to the group from DMARKS, "hello there" (at FIG. **31**), which is seen by all members of the group, including ME. Now ME will respond, by entering "hi there" into the response area.

When ME is finished entering his response, the participator software forwards the response to the controller, which sends it to the members of the channel. In the transcript area, the participator software notifies the user that it has received a private message from DMARKS, which is waiting inside the private message screen. To see the private message, ME presses the private message screen hot key.

A private message screen appears (at FIG. **32**), and the private message from DMARKS is at the bottom of the transcript area. Now to reply, ME types his response into the response area.

Now ME will return to the screen for the channel TESTCHANNEL. The member list area has changed because DMARKS has revoked ME's moderator permission. ME is no longer permitted to see the permissions of other users, so this information has been removed from his display (at FIG. **33**). The only information he can see now is who is moderator (at FIG. **34**). A "*" next to the identifier of a member of the group indicates the member is a moderator of the group. ME is no longer a moderator, and therefore a "*" does not appear the identifier ME.

To further exemplify the use of the present invention, the following is a transcript of communications produced in accordance herewith.

POWERQUALITY JOHNMUNG: unclear about meaning of "first contingency"

POWERQUALITY SAM: mike, that is correct on IEEE 519

POWERQUALITY SKLEIN: In assessing network security (against outage) the first contingencies are tested to see how the power system should be reconfigured to avoid getting a second contingency and cascading into an outage.

POWERQUALITY MSTEARS: These outages point out the need for reliability as part of the overall customer picture of PQ

POWERQUALITY BRIAN: Hi Jennifer, hit crt-p for private messagae

POWERQUALITY SKLEIN: In simpler terms, a single point failure shouldn't crash the system.

POWERQUALITY SKLEIN: Are we all chatted out?

POWERQUALITY ANDYV: brian, johnmung has been banned!!! why?

POWERQUALITY BRIAN: no way, new subject

POWERQUALITY BRIAN: just a sec, andy

POWERQUALITY BRIAN: No banning on this channel, John is back on

POWERQUALITY TKEY: ieee 519 limits the harmonic current a customer can inject back into the pcc and limit the vthd the utility provides at the PCC

POWERQUALITY JOHNMUNG: thanks guys, for unbanning me—i've been thrown out of better places than this!

POWERQUALITY BRIAN: New subject . . . now . . .

POWERQUALITY BRIAN: good one john . . . :)

POWERQUALITY MSTEARS: For critical facilities dual feeds or other backup capability need to be economically evaluated to keep the facility in operation

POWERQUALITY SAM: John, I remember that club very well

POWERQUALITY JOHNMUNG: question: please comment on frequency of complaints involving spikes, sags or harmonics

POWERQUALITY WARD: Problems caused by sags is the main complaint.

POWERQUALITY BRIAN: What subject does anyone want to see the next chat

POWERQUALITY WARD: Surges is probably next; harmonics really don't cause that many problems, although they are certainly there.

POWERQUALITY ANDYV: what is the solution ward?

POWERQUALITY TKEY: Agree they are the most frequent (sags) and the panel sesion on the cost of voltage sags at PES drew **110** people

POWERQUALITY SAM: harmonics tend to be an interior problem within a facility, rather than on the distribution system

POWERQUALITY WARD: The best solution is making the equipment less susceptible to sags. This requires working with the manufacturers.

POWERQUALITY ANDYV: won't that cost more

POWERQUALITY MSTEARS: The complaint of surges covers many things in the customers eyes sags have become a real problem because they are harder to resolve

POWERQUALITY GRAVELY: John—The latest EPRI results confirms the 90+% of the time SGS are the problem and short term ones.

POWERQUALITY WINDSONG: What is the topic for the 25??

POWERQUALITY WARD: Each problem can be dealt with as it occurs, but the time involved gets very expensive.

POWERQUALITY JOHNMUNG: making equipment less susceptible causes legal problems for manufacturers—as each improvemnt can be cited by compinant as example of malfeasance

POWERQUALITY WARD: AndyV: The cost to the manufacturer increases. The overall cost to everyone involved decreases.

POWERQUALITY TKEY: customer pays any way you cut it, if the eqpt is more immune customers pay only once instead of every time the process fails

POWERQUALITY BRIAN: The topic is regarding Power Quality

POWERQUALITY BRIAN: This chat is available for everyone 24 hours a day

POWERQUALITY ANDYV: ddorr>>will the manufacturer spend more to produce a better product

POWERQUALITY WARD: And as Tom says, the cost to the customer is far less.

POWERQUALITY BRIAN: This chat will be functioning 24 hrs/day

POWERQUALITY BRIAN: please usae it

POWERQUALITY BRIAN: The next panel discussion is Nov 15th

POWERQUALITY WARD: Andy, that's where standards come in.

POWERQUALITY SKLEIN: Is the customer capable of resolving the fingerpointing among the manufacturers and utilities?

POWERQUALITY DDORR: andy, only if the end userss create a market for pq compatible eqpt by demanding better products

POWERQUALITY MSTEARS: The manufacturers problems in including fixes is being competative with some who doesn't provide the fix

POWERQUALITY ANDYV: how will we educate the general consumer?

POWERQUALITY GRAVELY: Is it possible to have a basic theme topic or some core questions for 15 Nov chat?

POWERQUALITY WARD: Stan, the customer cannot be expected to resolve the fingerpointing. The manufacturers and utilities need to work together.

POWERQUALITY ANDYV: about power quality and reliability?

POWERQUALITY SKLEIN: If electric power is going to be treated as a fungible commodity, there has to be a definition. Like, everyone knows what number 2 heating oil is.

POWERQUALITY SAM: Ideally a manufacturer would not be able to compete if they don't add the protective function in their products, but alot more public education is required before we get to this point.

POWERQUALITY WARD: Andy, there are many ways to educate the customers, but they require a lot of contact between the utility and the customers. The Western Resources Power Technology Center in Wichita is doing it, just as an example.

POWERQUALITY DDORR: standard power vs premium power is one solution as is std qpt vs Pq compatible eqpt

POWERQUALITY SKLEIN: I want to buy number 2 electric power and to be able to check the nameplates of my appliances to be sure they can take it. Just like I buy regular gasoline.

POWERQUALITY MSTEARS: Sam—I agree, that is partly the utilities responsibilitysince we serve the customers

POWERQUALITY BBOYER: What differentiates number 2 from number 1?

POWERQUALITY SKLEIN: I used the analogy of number 2 heating oil. I don't know what number 1 heating oil is.

POWERQUALITY DDORR: Number two has cap switching and all the normal utility operational events while number one is much better

POWERQUALITY SKLEIN: Perhaps we can just say regular vs high test.

POWERQUALITY SAM: mike, yes a joint effort between the utiliy, manufacturer and standards juristictions is a goal for utilicorp as we move forward with offering from our strategic marketing partners, and bring PQ technologies to the public

POWERQUALITY TKEY: We are finding that many mfgrs want to produce pq compatible equipment, but they have no clue as to what to test for

POWERQUALITY ANDYV: Tom>>will the IEC standards help?

POWERQUALITY TKEY: Its up to the utility to help define normal events IEC will take time

POWERQUALITY SKLEIN: You can't have a commodity product with all the variation in specifications we have been discussing. It has to be regular, premium, and super premium or it won't work.

POWERQUALITY JOHNMUNG: Tom as a former manufacturer i sympathize—your work at PEAC is invaluable but anecdotal knowledge from utility people on the firing line is equally important

POWERQUALITY TKEY: Super premium, does that mean a UPS?

POWERQUALITY ANDYV: how do you stop a facility from affecting you super-premium power?

POWERQUALITY TKEY: John, Good Point

POWERQUALITY SAM: Tkey, a ups, local generation or redundant service

POWERQUALITY SKLEIN: This is what I meant earlier by electricity being a non-virtualizable service. You can't make each customer see the power system as though they had their own dedicated generating plant.

POWERQUALITY BRIAN: THE CHAT CHANNEL WILL BE OPEN 24/HRS/DAY 7 DAYS A WEEK

POWERQUALITY TKEY: I must sign out for about 5 minutes but I'll be back

POWERQUALITY BRIAN: OK TOM

POWERQUALITY MSTEARS: PQ for facilities need to be done with a system perspective to to get the right resolution

POWERQUALITY BBOYER: Andy's question is still relevant—how do stop a facility from downgrading utility service to other customers?

POWERQUALITY BRIAN: MIKE>>LETS SWITCH BACK TO RETAIL WHEELING

POWERQUALITY WARD: You work with that customer to do whatever is needed to correct their disturbances.

POWERQUALITY BBOYER: Be more specific

POWERQUALITY MSTEARS: Interaction between facilites can be evaluated and designed for

POWERQUALITY JOHNMUNG: as a key to hardening it helps to identify the most sensitive circuits, i.e. microprocessor logic, test for vulnerability under common surges, sags, rfi, and then notify users that their equipment contains these subsystems—for a start

POWERQUALITY BRIAN: hI DOUG

POWERQUALITY GRAVELY: Brian: Are you saving this session as a file? Can we get a list of chat session participants?

POWERQUALITY BRIAN: s, we may

POWERQUALITY DMARKS: gravely: hit TAB and use the arrow keys to page through the list of participants

POWERQUALITY SKLEIN: Will the session be available for downloading?

POWERQUALITY BRIAN: yes, Mike we will publish in PQ Magazine

POWERQUALITY WARD: Part of the agreement for high quality power should be that the customer receiving the power will not disturb the utility system.

POWERQUALITY BRIAN: if john let's us . . . .

POWERQUALITY GRAVELY: I tried that, however, netcruiser has a software problem and I cannot see all of the names.

POWERQUALITY SAM: most utilities rules and regulations already require that a customer not put anything back out on the utility system

POWERQUALITY BRIAN: MIKE G.>>WE WILL PUBLISH THIS IN PQ MAG NEXT MONTH IF ASNDY US

POWERQUALITY BRIAN: HOW ABOUT IT ANDY?

POWERQUALITY ANDYV: ok

POWERQUALITY BRIAN: COOL

POWERQUALITY WARD: Standards will have to be set for what constitutes a disturbance, and then the utility should work with customers, install filters, etc., to be sure they stay within the rules.

POWERQUALITY BRIAN: THANKS ANDY

POWERQUALITY ANDYV: a meeting review or a sumary of events

POWERQUALITY GRAVELY: It would be good to take a few minutes to recommend how the 15 Nov session could be more effective.

POWERQUALITY BRIAN: A SYNAPSE OF THIS CHAT WILL BE IN NEXT MONTHS PQ MAG

POWERQUALITY WINDSONG:

POWERQUALITY SKLEIN: I don't get PQ mag. Will it be on the Net?

POWERQUALITY BRIAN: STAN SIGN UP FOR IT ON OUR HOME PAGE

POWERQUALITY DOUGC: the transcript of this conference will be available on the EnergyOne pages.

POWERQUALITY BRIAN: YOU CAN SIGN UP ON LINE

POWERQUALITY BRIAN: HTTP://WWW.UTILICORP.COM

POWERQUALITY WINDSONG: Good comment Gravely Comments from the users would be greatly appreciated!!

POWERQUALITY SAM: PQ magazine is available online on the UCU Internet bulletin board, http://www.utilicorp.com

POWERQUALITY ANDYV: or link from powerquality.com

POWERQUALITY BRIAN: YOU CAN GET A FREE MAG SUBSCRIPTION FROM UTILICORP'S HOME PAGE

POWERQUALITY SKLEIN: Thanks

POWERQUALITY BRIAN: ALSO, THERE IS A PQ FORUM ON OUR HOME PAGE

POWERQUALITY JOHNMUNG: for nov 15 shall we pick five key topics? suggest health care, energy storage rfi/emc as a few topics—also new gas turbine 25 kw generator just announce today—just some suggestions

POWERQUALITY BRIAN: GOOD SUGGESTION JOHN

POWERQUALITY ANDYV: lets develop an outline of topics for next time.

POWERQUALITY BRIAN: OK

POWERQUALITY GRAVELY: One suggestion for 15 Nov—Have participants place a list of desired topics on your other chat box and prioritize by interest level.

POWERQUALITY SKLEIN: How about deregulation and retail wheeling.

POWERQUALITY BRIAN: COMMENTS SHOULD BE SENT TO ME BY EMAIL

POWERQUALITY BRIAN: BSPENCER@UTILICORP.COM

POWERQUALITY BRIAN: 15 minutes remaining

POWERQUALITY ANDYZYREK: Let's discuss the new standard IEEE 1159.

POWERQUALITY ANDYV: may be we could generate an online questionaire to see what people are needing discussed.

POWERQUALITY BRIAN: but the chat is available for 24 hrs/day 7 days a week

POWERQUALITY ANDYV: what does IEEE1159 address?

POWERQUALITY BRIAN: Please send all suggestion to me for our next chat

POWERQUALITY BRIAN: Bobbin is not banned now

POWERQUALITY BRIAN: my fault

POWERQUALITY ANDYZYREK: New PQ measuring techniques. We have not received our issue yet.

POWERQUALITY ANDYV: You should have it my now.

POWERQUALITY BRIAN: Bobbin is not banned anymore

POWERQUALITY ANDYV: you can e-mail me or john at: editors@powerquality.com

POWERQUALITY BRIAN: is two hours right fdo rhtis feature

POWERQUALITY JOHNMUNG: do i understand that many programmable logic controllers can be hardened by addition of simple CVT like a sola?

POWERQUALITY ANDYZYREK: Yes, but it is being delivered by snail mail.

POWERQUALITY ANDYV: no 2nd class

POWERQUALITY BRIAN: 15 minutes to go

POWERQUALITY ANDYV: Please e-mail me you complete name and addess and I will mail you one today 1st class . . . now is that serice or what?

POWERQUALITY BRIAN: Is two hours long enough for tthis chat?

POWERQUALITY TKEY: Im back

POWERQUALITY WARD: Brian, I think two hours is about right.

POWERQUALITY BRIAN: hi tom

POWERQUALITY BRIAN: good . . .

POWERQUALITY ANDYV: yes I agree 2 hrs

POWERQUALITY BRIAN: anyone else

POWERQUALITY ANDYV: it the time of day correct?

POWERQUALITY BRIAN: questions now . . . .

POWERQUALITY SKLEIN: The topic foremost in my mind right now is what to eat for lunch. I enjoyed the discussion, which I understand has been historic in some sense. But I think I will sign off now and go eat.

POWERQUALITY SAM: 2 hours seems to work very well

POWERQUALITY DANIELH: time of day is good

POWERQUALITY BILLMANN: 2 hrs is fine

POWERQUALITY MSTEARS: Two hours work well, the middle of the day allows east and west coast to be involved

POWERQUALITY BRIAN: good, Will everyone be back for the next chat

POWERQUALITY GRAVELY: Brian, I will forward my recommendations on email, thanks.

POWERQUALITY BILLMANN: yes i'll be back

POWERQUALITY ANDYZYREK: Brian, would it be possible to have a forum published on your home page prior to Nov 15.

POWERQUALITY BRIAN: I would like to do another chat before Nov 15th. any thoughts

POWERQUALITY ANDY: U bet

POWERQUALITY SAM: I believe that this chat may set an attendance record for most participants during a first session

POWERQUALITY JOHNMUNG: a parting thought—"harmonics make the music rich, they make the tone insprinng—harmonics in your power line WILL BLOW THE BUILDINGS WIRING" tIM MUNGENAST

POWERQUALITY BRIAN: Your're all invited to return

POWERQUALITY BRIAN: the next chat

POWERQUALITY BRIAN: This chat feature will help set standards of how we view our industry

POWERQUALITY WARD: For me this was two hours very well spent, and it was quite enjoyable.
POWERQUALITY BRIAN: Tell a colleague about our chat Nov 15th
POWERQUALITY BRIAN: Thanks Ward
POWERQUALITY BRIAN: I would like to do this on a weekly basis, any thoughts yet
POWERQUALITY GRAVELY: John: talk it up in Germany!!
POWERQUALITY ANDY: I would like to thank utilicorp and everyone envolved.
POWERQUALITY BRIAN: Thanks Andy for your help
POWERQUALITY WARD: Did this notice go out to the Power Globe mailing list?
POWERQUALITY BRIAN: No, but could help us Ward with that
POWERQUALITY BRIAN: Lets all get the word out about this chat
POWERQUALITY WARD: I'm on the list and will be glad to forward anything you wish to it.
POWERQUALITY BRIAN: Please use it whenver you wish, even schedule your own chats whenver
POWERQUALITY JOHNMUNG: MANY THANKS TO UTILICORP AND ALL INVOLVED—FROM AN OLD STEAM BOATER :-)
POWERQUALITY BRIAN: thanks ward
POWERQUALITY BRIAN: Hi duane
POWERQUALITY BRIAN: This chat is officially over, but do stick around for more chatting
POWERQUALITY BRIAN: Thanks to all, cya on Nov 15th
POWERQUALITY MSTEARS: Ward, Tom, and John I appreciate your participation
POWERQUALITY BRIAN: Thanks Guys and Ladies!!!!!!!!!!
POWERQUALITY SWPPD: WHAT IS HAPPENING ON NOV. 15
POWERQUALITY BRIAN: our next chat with a panel of experts
POWERQUALITY BRIAN: topic yet to be decided
POWERQUALITY DPSWOBO: Hi Brian, Sorry I was on the phone and could not respond right away. Did I get the time incorrectly for the chat?
POWERQUALITY BRIAN: please send us a suggestions
POWERQUALITY ANDY: good bye ;-)
POWERQUALITY BRIAN: Yeah, but stick around to chat with some friends
POWERQUALITY BRIAN: We had a total of 50 people and avg of 20 people at one time
POWERQUALITY BRIAN: Thanks everyone!!!Lunch Time
POWERQUALITY BRIAN: Next Chat Nov 15th at 10-12 ct
POWERQUALITY BRIAN: But this chat line is available 24 hrs/day/7 days a week
POWERQUALITY BRIAN: Please use it whenever
POWERQUALITY GRAVELY: Thanks to the panel and Utilicorp for the session!
POWERQUALITY BRIAN: Talk to your collegues and friends about any particular topic
POWERQUALITY BRIAN: Come see our home page for new topics and chats
POWERQUALITY BRIAN: http://www.utilicorp.com
POWERQUALITY BRIAN: Thanks Power Quality Assurance Magazine and All our panel members
POWERQUALITY BRIAN: :)
POWERQUALITY SWPPD: MISSED THIS SESSION. ICAN WE GET HARD COPY INFO?
POWERQUALITY BRIAN: yes swwp, it will be published in pq mag and our home page
POWERQUALITY BRIAN: catch our next session on nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY SWPPD: THANKS A BUNCH!!
POWERQUALITY SWPPD: GOOD BYE!
POWERQUALITY BRIAN: no prob
POWERQUALITY BRIAN: cya
POWERQUALITY DESWETT:
POWERQUALITY TKEY: Good session brian, ddorr and I will be signing off now. look forward to the next session
POWERQUALITY DPSWOBO: Thanks for the info on the next session, we will get on next time
POWERQUALITY DMARKS: I hope everyone enjoyed this session.
POWERQUALITY MSTEARS: I am logging off Thanks
POWERQUALITY SAM: This is Tony and I am watching the action . . . we made history. Great work guys.
POWERQUALITY BRIAN: Lunch time
POWERQUALITY BRIAN: Next chat is nov 15th
POWERQUALITY BRIAN: 10-12ct
POWERQUALITY BRIAN: please continuie to look at utilicorp's hp
POWERQUALITY BRIAN: for more info
POWERQUALITY BRIAN: email if you have any questions regarding the chat
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: later
SUPPORT BRIAN: hi guys
SUPPORT BRIAN: success
SUPPORT BRIAN: yess!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
SUPPORT BRIAN: thanks for the help
SUPPORT BRIAN: cya
POWERQUALITY BRIAN: next chat on Nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: any suggestion on topics please contact me by email
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: hi chuck
POWERQUALITY BRIAN: hi randy
POWERQUALITY CPREECS: hello brian
POWERQUALITY BRIAN: How are you chuck
POWERQUALITY CPREECS: how has the participation been?
POWERQUALITY BRIAN: I am sorry you missed the offical chat, but do come back at any time for some chatting
POWERQUALITY BRIAN: great 20 people avg. 50 total people
POWERQUALITY CPREECS: ?yes, i got some conflicting info
POWERQUALITY BRIAN: transcripts will be in PQ mag next month and on utilicorp's home page
POWERQUALITY CPREECS: what were the topics discussed?
POWERQUALITY BRIAN: how is that chuck
POWERQUALITY BRIAN: power quality, standards,
POWERQUALITY BRIAN: retail wheeling
POWERQUALITY BRIAN: cya, lunch time
POWERQUALITY CPREECS: later
POWERQUALITY BRIAN: bye all
POWERQUALITY BRIAN: email me chuck
POWERQUALITY RB: sorry I missed it. I got 12-2 est off the net. bye.
POWERQUALITY BRIAN: sorry RB
POWERQUALITY BRIAN: miss information

POWERQUALITY BRIAN: next chat is 10-12
POWERQUALITY BRIAN: ct
POWERQUALITY BRIAN: nov 15th
POWERQUALITY BRIAN: bye
POWERQUALITY RB: thanks
POWERQUALITY BRIAN: no prob, tell all
POWERQUALITY ANDY: Is anyone still here talking about power quality?
POWERQUALITY DAVE: Just signed on that is what I was trying to find out
POWERQUALITY ANDY: the PQ chat was running from 11:00-1:00est
POWERQUALITY ANDY: Were you involved then?
POWERQUALITY DAVE: No I just got a chance to sign on now
POWERQUALITY ANDY: there were some great discussions.
POWERQUALITY ANDY: The transcripts will be available to down load at utilicorp.com Brian Spencer says.
POWERQUALITY ANDY: What is your experience in PQ
POWERQUALITY DAVE: That is what I was looking for, are they available to down load now, I work in a data center and have worked with UPS systems for about 12 years
POWERQUALITY DAVE: I did field service for Exide
POWERQUALITY ANDY: Brian just went to Lunch in KS I don/t know when it will availalbe.
POWERQUALITY DAVE: Thanks for the Info on the downloads, I hope they do this again
POWERQUALITY ANDY: so do I.
POWERQUALITY DAVE: What is your experience on PQ
POWERQUALITY ANDY: I am the editor or Power quality mag.
POWERQUALITY DAVE: Good mag., I pick up alot in it
POWERQUALITY ANDY: do your receive power quality assurance magazine?
POWERQUALITY ANDY: great glad to hear it.
POWERQUALITY DAVE: We get it at work but I have asked to have it sent to my home
POWERQUALITY ANDY: did you get the latest issue witht the lighting on the cover?
POWERQUALITY DAVE: Not yet, have seen it on line though
POWERQUALITY ANDY: great.
POWERQUALITY ANDY: any suggestion for editorial?
POWERQUALITY DAVE:
POWERQUALITY DAVE: no it is good
POWERQUALITY ANDY: ok.
POWERQUALITY ANDY: I am currently editing an article about VRLA battery charging.
POWERQUALITY DAVE: I am working on a resonant problem with Utility and was looking for info
POWERQUALITY ANDY: explain
POWERQUALITY ANDY: by the way my e-mail is andy@powerquality.com
POWERQUALITY DAVE: we are running a lot of 5th har. across our system in a large data center
POWERQUALITY ANDY: I see
POWERQUALITY ANDY: I will try to address this in an upcomming issue. may be march/april or even sooner.
POWERQUALITY DAVE: we have 4800 kw of UPS cap on two transformers and we have alot of 5th on our other boards
POWERQUALITY ANDY: If you are interested in writing up a case history including you solutions I would like to review it and poss. publish
POWERQUALITY MSTONEHAM: Is this chat session still active?
POWERQUALITY ANDY: YES
POWERQUALITY ANDY: We can'nt get enough! ! !
POWERQUALITY DAVE: when we can get it fixed, It looks like we have a problem with input filtering on a couple of UPS,s
POWERQUALITY ANDY: input fro the utility or a generator?
POWERQUALITY DAVE: utility
POWERQUALITY MSTONEHAM: I understand there was a chat session earlier today with some guest "chatters". Is there an archive of the discussion since I missed it?
POWERQUALITY DAVE: we have 66 kv to 12 kv then to 480 v by 4 trans on property
POWERQUALITY ANDY: What are you leaning towards in a solution dave
POWERQUALITY ANDY: MTONEHAM>>yes but I don't know when. contact BSPENCER@utilicorp.com
POWERQUALITY DAVE: the computer seem to have no problem, but we have alot of motor heating/bad PF
POWERQUALITY MSTONEHAM: Thanks!
POWERQUALITY DAVE: we currently are working with a consultant but I am looking for more info
POWERQUALITY ANDY: will capacitors solve your problem
POWERQUALITY ANDY:
POWERQUALITY ANDY: there also is a forum under utilicorp.com where you can post you questions.
POWERQUALITY DAVE: Each 600 kw UPS has Input filtering/may need trap for 5th
POWERQUALITY ANDY: or you can access it form powerquality.com
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: Talk to ya later dave
POWERQUALITY DAVE: is PQ.com your Mag
POWERQUALITY ANDY: bye
POWERQUALITY DAVE: bye
POWERQUALITY ANDY: yes
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: :-)
POWERQUALITY MSTONEHAM:
POWERQUALITY MSTONEHAM: Is anyone else hear? There doesn't seem to be much traffic.
POWERQUALITY MSTONEHAM:
POWERQUALITY CILCOJRG: Hello—is the conference over?
POWERQUALITY CILCOJRG:
POWERQUALITY CILCOJRG: hello
POWERQUALITY BRIAN: yes
POWERQUALITY BRIAN: the conference was from 10-12 ct
POWERQUALITY BRIAN: someone gave out the wrong information
POWERQUALITY BRIAN: hello cilco
POWERQUALITY BRIAN: anyone still there
SUPPORT BRIAN: hi all
SUPPORT BRIAN: anyone there
POWERQUALITY BRIAN: jenny>>are you there
POWERQUALITY CJBOUTCHER: is anyone here a utility employee?
POWERQUALITY BRIAN: Hi chris
POWERQUALITY BRIAN: how are you?
POWERQUALITY CJBOUTCHER: hi brian it is quiet in here
POWERQUALITY BRIAN: the conference was at 10:00ct
POWERQUALITY CJBOUTCHER: ah I see
POWERQUALITY CJBOUTCHER: when is the next one?
POWERQUALITY BRIAN: nov 15th
POWERQUALITY BRIAN: 10-12

POWERQUALITY BRIAN: ct
POWERQUALITY CJBOUTCHER: is the channel open at other times?
POWERQUALITY BRIAN: yes 24 hours a day
POWERQUALITY CJBOUTCHER: but not much discussion?
POWERQUALITY BRIAN: not right now,
POWERQUALITY BRIAN: cya
POWERQUALITY CJBOUTCHER: bye
POWERQUALITY BRIAN: hi jenny
POWERQUALITY JOSH: hello?
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: are you awake yet?
POWERQUALITY BRIAN: just giving present this a.m.
POWERQUALITY BRIAN: :)
POWERQUALITY BRIAN: who is guest96
POWERQUALITY GUEST96: test

While a particular embodiment of the present invention has been disclosed, it is to be understood that various different modifications are possible and are within the true spirit of the invention, the scope of which is to be determined with reference to the claims set forth below. There is no intention, therefore, to limit the invention to the exact disclosure presented herein as a teaching of one embodiment of the invention.

The invention claimed is:

1. A method of communicating content among users using of a computer system including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the method comprising:

authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database;

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;

running controller software on the controller computer, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers;

providing an API on the controller computer, the API multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers; and

communicating real-time messages within the group of the interactively connected said participator computers.

2. The method of claim **1**, wherein the communicating content includes communicating at least one of sound, video, graphic, pointer, and multimedia content.

3. The method of claim **2**, wherein said at least one comprises at least two.

4. The method of claim **2**, wherein said at least one comprises at least three.

5. The method of claim **2**, wherein said at least one comprises at least four.

6. The method of claim **2**, wherein said at least one comprises at least five.

7. The method of claim **1**, wherein the communicating content includes communicating a pointer that allows the content to be produced on demand.

8. The method of claim **1**, wherein the API includes API messages.

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

10. The method of claim **9**, wherein the API messages include JOIN, LEAVE, STATUS, SETCHAN, and MODMSG instructions.

11. The method of claim **9**, wherein the API messages include MESSAGE and MODMSG instructions.

12. The method of claim **1**, wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages.

13. The method of claim **12**, wherein the message type includes ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG.

14. The method of claim **1**, further including determining censorship of the content.

15. The method of claim **1**, wherein the controller computer determines censorship.

16. The method of claim **1**, wherein the communicating is conducted over the network, including the Internet.

17. The method of claim **1**, wherein the communicating content includes communicating content invoked with a URL.

18. The method of claim **1**, wherein the controller software comprises a JAVA™ application.

19. An apparatus to communicate content among users of a computer system, the computer system comprising:

a controller computer system, including a controller computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, in communication with each of the participator computers by authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database, wherein the controller computer is running controller software, in accordance with predefined rules, to direct arbitration of which ones of the participator computers interactively connect within a group of the participator computers, to provide an API on the controller computer, whereby the API multiplexes and demultiplexes API messages by type, to create a virtual connection and provide the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers, and to allow communication of real-time messages within the group of the interactively connected said participator computers.

20. The apparatus of claim **19**, wherein the content includes at least one of sound, video, graphic, pointer, and multimedia content.

21. The apparatus of claim **20**, wherein said at least one comprises at least two.

22. The apparatus of claim **20**, wherein said at least one comprises at least three.

23. The apparatus of claim **20**, wherein said at least one comprises at least three.

24. The apparatus of claim **20**, wherein said at least one comprises at least four.

25. The apparatus of claim **19**, wherein the controller software comprises a JAVA™ application.

**26**. The apparatus of claim **19**, wherein the content includes a pointer which allows the content to be produced on demand.

**27**. The apparatus of claim **19**, wherein the API includes API messages.

**28**. The apparatus of claim **19**, wherein communications among the controller computer and the participator computers are mediated via API messages.

**29**. The apparatus of claim **28**, wherein the API messages include at least one of JOIN, LEAVE, STATUS, SETCHAN, and MODMSG instructions.

**30**. The apparatus of claim **28**, wherein the message type includes at least one of ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG.

**31**. The apparatus of claim **19**, wherein the controller software includes multiplexing and de-multiplexing operations carried out as a message type on API messages.

**32**. The apparatus of claim **31**, wherein the API messages include at least one of MESSAGE and MODMSG instructions.

**33**. The apparatus of claim **19**, wherein the computer system determines censorship of the content.

**34**. The apparatus of claim **19**, wherein the controller computer determines censorship.

**35**. The apparatus of claim **19**, wherein the content is communicated over a network, including the Internet.

**36**. The apparatus of claim **19**, wherein the content is communicated by invoking a URL.

**37**. An apparatus comprising:

a computer system, the 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 independent participator computers which are otherwise independent of each other, via the Internet network, communicating with the participator computers by authenticating a first user identity and a second user identity according to permissions retrieved from the repository of tokens of the database, the

controller computer running controller software, in accordance with predefined rules, directing arbitration of which ones of the participator computers interact within a group of the participator computers, providing an API on the controller computer, whereby the API is multiplexing and demultiplexing API messages by type, creating a virtual connection and providing the virtual connection between channels, private messages, and multimedia objects in the controller computer and the participator computers, and providing communication of real-time messages within the group of the interactively connected said participator computers.

* * * * *

US008473552B1

(12) **United States Patent**
**Marks**

(10) **Patent No.: US 8,473,552 B1**
(45) **Date of Patent: Jun. 25, 2013**

(54) **COMMUNICATIONS SYSTEM**

(76) Inventor: **Daniel L Marks**, Urbana, IL (US)

( * ) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 952 days.

(21) Appl. No.: **11/510,351**

(22) Filed: **Aug. 24, 2006**

**Related U.S. Application Data**

(63) Continuation of application No. 09/399,578, filed on Sep. 20, 1999, which is a continuation of application No. 08/617,658, filed on Apr. 1, 1996, now Pat. No. 5,956,491.

(51) **Int. Cl.**
***G06F 15/16*** (2006.01)

(52) **U.S. Cl.**
USPC .............................. **709/206**; 709/204; 709/225

(58) **Field of Classification Search**
USPC .......................................... 709/204–207, 225
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | | |
|---|---|---|---|---|---|
| 5,347,632 | A | | 9/1994 | Filepp et al. | |
| 5,408,470 | A | | 4/1995 | Rothrock et al. | |
| 5,440,624 | A | * | 8/1995 | Schoof, II | 379/202.01 |
| 5,452,299 | A | * | 9/1995 | Thessin et al. | 370/260 |
| 5,616,876 | A | | 4/1997 | Cluts | 84/609 |
| 5,689,553 | A | * | 11/1997 | Ahuja et al. | 379/202.01 |
| 5,771,355 | A | * | 6/1998 | Kuzma | 709/232 |
| 5,774,668 | A | | 6/1998 | Choquier et al. | |
| 5,793,365 | A | | 8/1998 | Tang et al. | 345/329 |
| 5,880,731 | A | | 3/1999 | Liles et al. | 345/349 |
| 5,941,947 | A | * | 8/1999 | Brown et al. | 709/225 |
| 6,560,707 | B2 | | 5/2003 | Curtis et al. | 713/163 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| EP | 336 552 A2 | 10/1989 |

OTHER PUBLICATIONS

Vinod Anupam et al., Shastra—An Architecture for development of collaborative applications, Proceedings Second Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Apr. 1993, pp. 155-163.*

Andreas Dieberger, Providing Spatial Navigation for the World Wide Web, Spatial Information theory a Theoretical Baisi for GIS, Lecture Notes in Computer Science, vol. 988, 1995, pp. 93-106.*

Lee Newberg et al., Integrating the Worl-Wide Web and Multi-User Domains to Support Advanced Network-Based Learning Experiments, Conference Proceedings of ED-MEDIA 1995, pp. 494-499.*

(Continued)

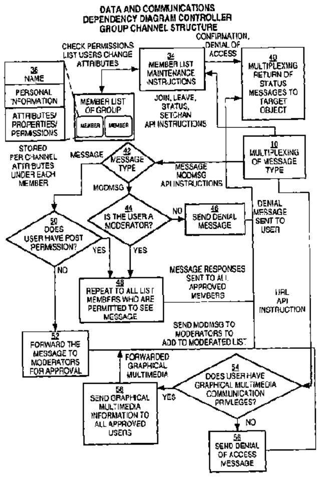
*Primary Examiner* — Patrice Winder

(74) *Attorney, Agent, or Firm* — Peter K. Trzyna, Esq.

(57) **ABSTRACT**

A computerized human communication arbitrating and distributing system, including a controller digital computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information from a human user and an output device for presenting information to the user, each said user having a user identity. A connection, such as Internet, links the controller computer with each of the participator computers. Controller software runs on the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups through the controller computer and to distribute real time data to the respective ones of the groups. Participator software runs on each of the participator computers to handle a user interface permitting one said user to send a multimedia information message to the controller computer, which arbitrates which of the participator computers receive the multimedia information message and conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

**64 Claims, 22 Drawing Sheets**


DATA AND COMMUNICATIONS DEPENDENCY DIAGRAM CONTROLLER GROUP CHANNEL STRUCTURE
CHECK PERMISSIONS LIST USERS CHANGE ATTRIBUTES
34 MEMBER LIST MAINTENANCE INSTRUCTIONS
CONFIRMATION, DENIAL OF ACCESS
40 MULTIPLEXING RETURN OF STATUS MESSAGES TO TARGET OBJECT
36 NAME
PERSONAL INFORMATION
ATTRIBUTES/ PROPERTIES/ PERMISSIONS
MEMBER LIST OF GROUP
MEMBER
MEMBER
JOIN, LEAVE, STATUS, SETCHAN API INSTRUCTIONS
STORED PER CHANNEL ATTRIBUTES UNDER EACH MEMBER
MESSAGE
42 MESSAGE TYPE
MESSAGE MODMSG API INSTRUCTIONS
10 MULTIPLEXING OF MESSAGE TYPE
MODMSG
44 IS THE USER A MODERATOR?
NO
46 SEND DENIAL MESSAGE
DENIAL MESSAGE SENT TO USER
50 DOES USER HAVE POST PERMISSION?
YES
YES
NO
48 REPEAT TO ALL LIST MEMBERS WHO ARE PERMITTED TO SEE MESSAGE
MESSAGE RESPONSES SENT TO ALL APPROVED MEMBERS
URL API INSTRUCTION
SEND MODMSG TO MODERATORS TO ADD TO MODERATED LIST
52 FORWARD THE MESSAGE TO MODERATORS FOR APPROVAL
FORWARDED GRAPHICAL MULTIMEDIA
54 DOES USER HAVE GRAPHICAL MULTIMEDIA COMMUNICATION PRIVLEGES?
YES
58 SEND GRAPHICAL MULTIMEDIA INFORMATION TO ALL APPROVED USERS
NO
56 SEND DENIAL OF ACCESS MESSAGE

## OTHER PUBLICATIONS

TY Hou et al., An active multimedia System for Delayed Conferencing, Proceedings of the SPIE Conference on High-Speed Networking and Multimedia Computing, San Jose CA, 1994, pp. 97-104.*

Paul Tarau et al., LogiMOO: an Extensible Multi-User Virtual World with Natureal Language Control, The Journal of Logic Programming, 1993,col. 12, pp. 1-23.*

Office Action—Final Rejection Dated Apr. 8, 2004 from U.S. Appl. No. 09/399,578.

Meloan, Steve. CU-SeeMe. Tech Toys. 1995 Urban Desires. pp. 1-2 http://desires.com/1.6/Toys/Cuseeme/cuseeme.html.

"ITU-T: Telecommunication Standardization of Sector ITU: Series T: Terminal Equipments and Protocols for Telematic Services," International Telecommunication Union, T.120, (Jul. 1996) pp. 1-24.

"T.120 Whitepaper: A Primer on the T.120 Series Standard," DataBeam Corporation, 1995, pp. 1-15.

"Complaint: Brian Hollander vs. Peter K. Trzyna and PTK Technologies, LLC," Filed Nov. 13, 2007, pp. 1-18.

"Amendment and Response," for U.S. Appl. No. 11/510,473, filed Feb. 5, 2010, pp. 1-26.

"Preliminary Amendment," for U.S. Appl. No. 11/510,473, filed Nov. 30, 2007, pp. 1-21.

"Office Action" for U.S. Appl. No. 11/510,473, mailed on Oct. 5, 2009, pp. 1-49.

"Preliminary Amendment," for U.S. Appl. No. 11/510,463, filed Nov. 30, 2007, pp. 1-12.

"Office Action" for U.S. Appl. No. 11/510,463, mailed on Sep. 22, 2009, pp. 1-27.

Pavel Curtis et al., MUDS Grow Up: Social Virtual Reality in the Real World, Xerox PARC, Jan. 1993, 6 pages.

"Corrected Amendment and Response" for U.S. Appl. No. 11/510,463, filed Apr. 1, 2010. pp. 1-16.

"Amendment and Response" for U.S. Appl. No. 11/510,463, filed Mar. 22, 2010. pp. 1-16.

"Preliminary Amendment," for U.S. Appl. No. 11/836,633, filed Nov. 30, 2007. pp. 1-3.

Tim Meyer et al., A MOO-Based Collaboration Hypermedia System for WWW, Proceedings for Second International Conference for WWW, Oct. 1994.

Paul Kindberg et al., Mushroom: a framework for collaboration and interaction across the Internet, in the Proceedings of ERCIM Workshop on CSCW and the Web, Feb. 1996, 11 pages.

"Amendment and Response" filed on Feb. 5, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Oct. 5, 2009, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Sep. 22, 2009, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"MUDS Grow Up: Social Virtual Reality in the Real World". Curtis P. and Nichols, D.A. Xerox PARC. (Jan. 1993) pp. 1-6.

"Corrected Amendment and Response" filed on Apr. 1, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Mar. 22, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Fourth Preliminary Amendment" filed on May 25, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Third Preliminary Amendment" filed on May 7, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Apr. 14, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Office Action-Final Rejection" mailed on Jun. 28, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

Bentley et al., Supporting collaborative information sharing with the World Wide Web: The BSCW shared workspace system, Proceedings of the 4th International World Wide Web Conference, Dec. 1995, 12 pages.

Atul Prakash et al., DistiVew for Building Effiicient Collaborative Applications using Replicated Objects, Proceeding of the 1994 ACM conference on Computer supported cooperative work, 12 pages.

Kankanahalli Srinivas et al., MONET: A Multi-media System for Conferencing and Application Sharing in Distributed Systems. Feb. 1992, CERC Techinical Report Series Research Note, 19 pages.

"Office Action-Final Rejection" mailed on May 12, 2010, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

Atul Prakash et al., DistView for Building Efficient Collaborative Applications using Replicated Objects, Proceedings of the 1994 ACM conference on Computer supported cooperative work, pp. 153-164.

K.J. Maly et al., Mosaic + XTV = CoReview, Computer Networks and ISDN Systems, vol. 27 Issue 6, Apr. 1995, pp. 849-860, Proceedings of the Thrid International World Wide Web Conference.

Trzyna, Peter K., "Amendment After Final and Request for Reconsideration" filed Jan. 16, 2013, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007. pp. 1-14. USA.

Trzyna, Peter K., "Amendment After Final" filed Feb. 19, 2013, for U.S. Appl. No. 09/399,578, filed Sep. 20, 1999. pp. 1-177. USA.

T. Socolofsky et al., Request for Comments (RFC) 1180: A TCP/IP Tutorial, Network Working Group, Jan. 1991, pp. 1-29.

Anupam, Vinod "Collaborative Multimedia Environments for Problem Solving." A Thesis Submitted to Purdue University. (Aug. 1994), pp. 1-212, Ann Arbor, MI.

Bajaj, Chandrajit et al. "Collaborative Multimedia in Shastra." 3rd International Conference on Multimedia, San Francisco, CA (1995). pp. 365-366.

Anupam, Vinod et al. "Collaborative Multimedia in Scientific Design." Proceedings: First ACM Multimedia Conference. ACM Multimedia 93, Anaheim, California, ACM Press, (1993). pp. 447-456.

Anupam, Vinod et al. "Shastra—An Architecture for Development of Collaborative Applications." Proceedings: Second IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Morgantown, (1993). pp. 155-166.

Bajaj, Chandrajit et al. "Brokered Collaborative Infrastructure for CSCW." Proceedings: Fourth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Berkeley Springs. West Virginia, IEEE Computer Society Press, (1995), pp. 207-213.

Anupam, Vinod et al. "Shastra: Multimedia Collaborative Design Environment." IEEE Multimedia, 1, 2, (1994), pp. 39-49.

Anupam, Vinod et al. "Distributed and Collaborative Visualization." IEEE Computer, 27, 7, (Jul. 1994), pp. 37-43.

Bajaj, Chandrajit et al. "Web based Collaborative Visualization of Distributed and Parallel Simulation." In Proceedings of the 1999 IEEE Symposium on Parallel Visualization and Graphics, (Oct. 24-29, 1999), San Francisco, CA, pp. 47-54.

Bajaj, Chandrajit et al. "NLS: Collaborative Virtual Environment to Promote Shared Awareness." Proceedings: Workshop on New Paradigms in Information Visualization and Manipulation NPIV'96, In conjunction with Fifth ACM International Conference on Information and Knowledge Management (CIKM'96), (1996), pp. 41-45.

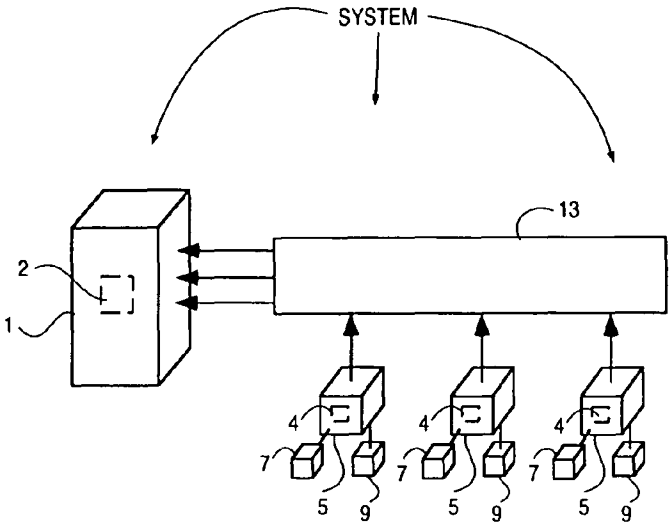
Bajaj, Chandrajit et al. "Web Based Collaboration-Aware Synthetic Environments" Proceedings of the 1997 GVU/NIST TEAMCAD workshop, Atlanta, GA, 1997. 143-150.

Oikarinen, J. & Reed, D. Internet Relay Chat Protocol. May 1993. pp. 1-69.

Expert Report of Bruce M. Maggs. pp. 1-134.

* cited by examiner

FIG. 1



COMMUNICATIONS OVERVIEW

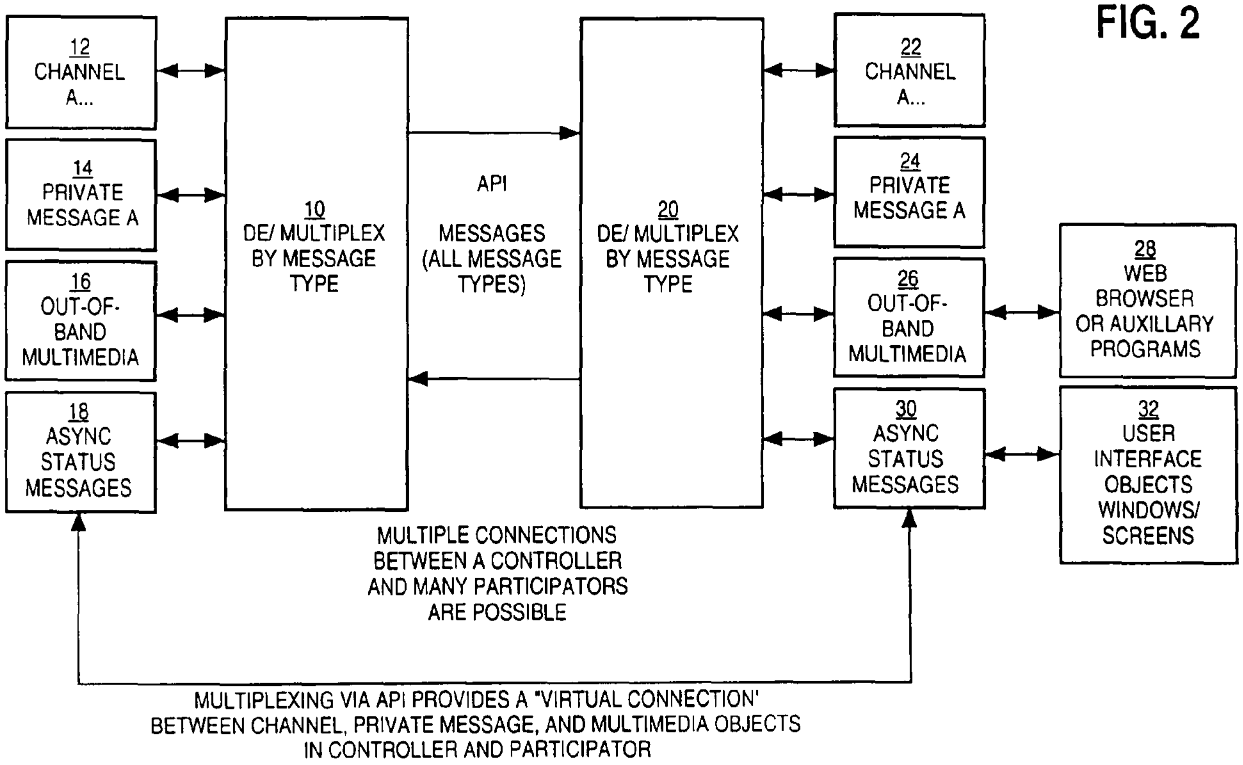

12 CHANNEL A...
14 PRIVATE MESSAGE A
16 OUT-OF-BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DE/ MULTIPLEX BY MESSAGE TYPE
API
MESSAGES (ALL MESSAGE TYPES)
20 DE/ MULTIPLEX BY MESSAGE TYPE
22 CHANNEL A...
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILLARY PROGRAMS
32 USER INTERFACE OBJECTS WINDOWS/ SCREENS
MULTIPLE CONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A "VIRTUAL CONNECTION' BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

FIG. 2

FIG. 3

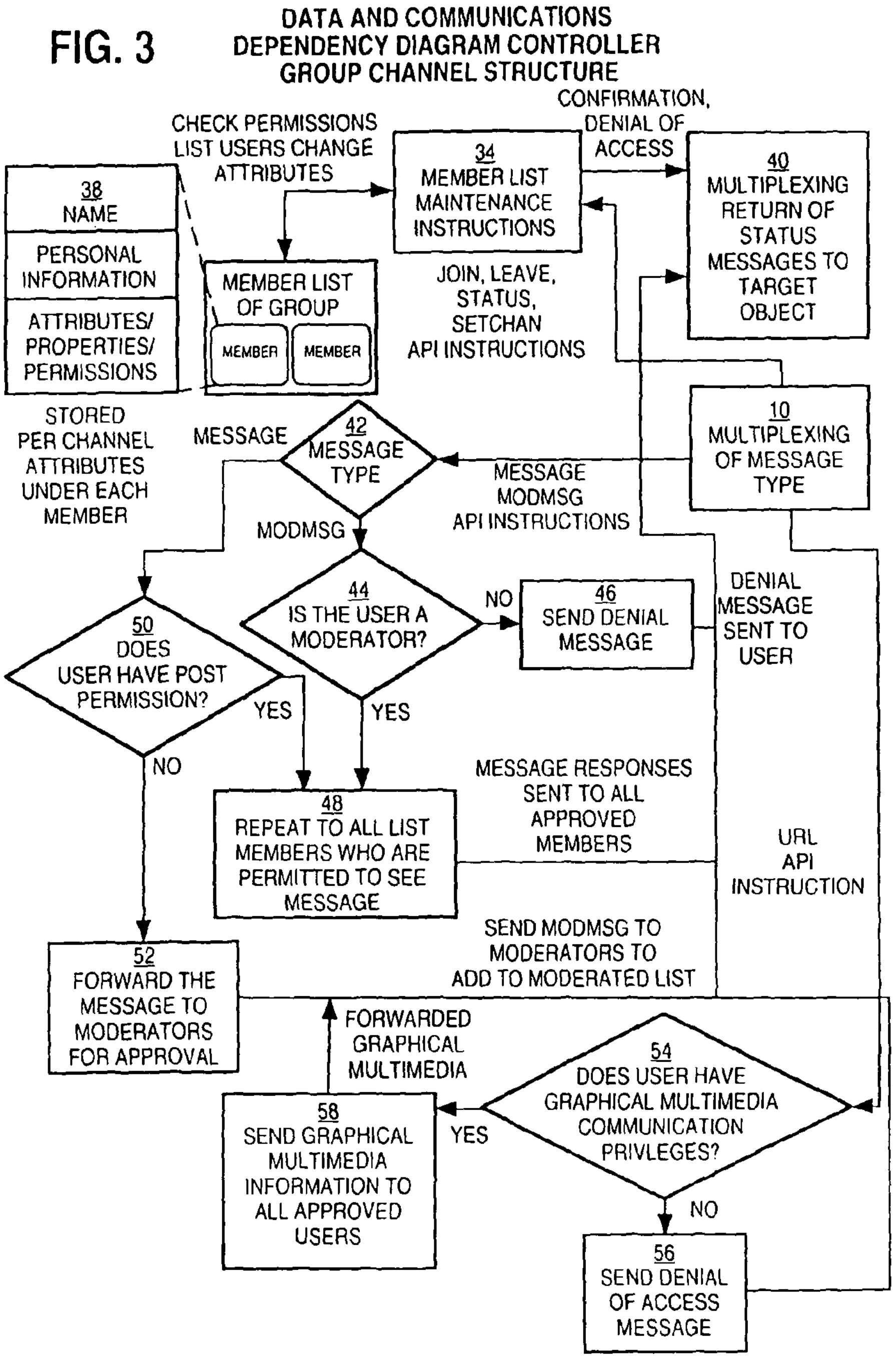

DATA AND COMMUNICATIONS DEPENDENCY DIAGRAM CONTROLLER GROUP CHANNEL STRUCTURE
CHECK PERMISSIONS LIST USERS CHANGE ATTRIBUTES
34 MEMBER LIST MAINTENANCE INSTRUCTIONS
CONFIRMATION, DENIAL OF ACCESS
40 MULTIPLEXING RETURN OF STATUS MESSAGES TO TARGET OBJECT
38 NAME
PERSONAL INFORMATION
ATTRIBUTES/ PROPERTIES/ PERMISSIONS
MEMBER LIST OF GROUP
MEMBER
MEMBER
JOIN, LEAVE, STATUS, SETCHAN API INSTRUCTIONS
STORED PER CHANNEL ATTRIBUTES UNDER EACH MEMBER
MESSAGE
42 MESSAGE TYPE
10 MULTIPLEXING OF MESSAGE TYPE
MESSAGE MODMSG API INSTRUCTIONS
MODMSG
44 IS THE USER A MODERATOR?
NO
46 SEND DENIAL MESSAGE
DENIAL MESSAGE SENT TO USER
50 DOES USER HAVE POST PERMISSION?
YES
YES
NO
48 REPEAT TO ALL LIST MEMBERS WHO ARE PERMITTED TO SEE MESSAGE
MESSAGE RESPONSES SENT TO ALL APPROVED MEMBERS
URL API INSTRUCTION
SEND MODMSG TO MODERATORS TO ADD TO MODERATED LIST
52 FORWARD THE MESSAGE TO MODERATORS FOR APPROVAL
FORWARDED GRAPHICAL MULTIMEDIA
54 DOES USER HAVE GRAPHICAL MULTIMEDIA COMMUNICATION PRIVLEGES?
YES
NO
58 SEND GRAPHICAL MULTIMEDIA INFORMATION TO ALL APPROVED USERS
56 SEND DENIAL OF ACCESS MESSAGE

FIG. 4

CENTRAL CONTROLLER LOOP COMMUNICATIONS

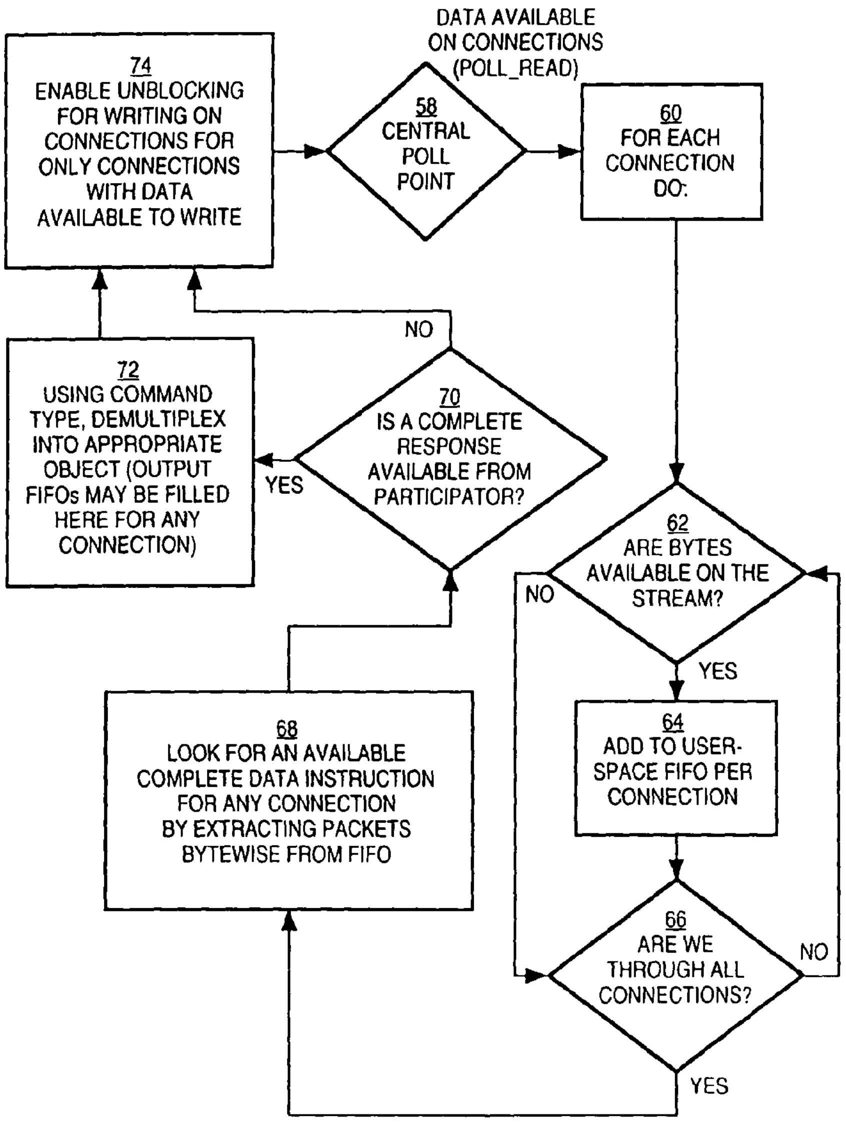

74
ENABLE UNBLOCKING FOR WRITING ON CONNECTIONS FOR ONLY CONNECTIONS WITH DATA AVAILABLE TO WRITE
DATA AVAILABLE ON CONNECTIONS (POLL_READ)
58
CENTRAL POLL POINT
60
FOR EACH CONNECTION DO:
NO
72
USING COMMAND TYPE, DEMULTIPLEX INTO APPROPRIATE OBJECT (OUTPUT FIFOs MAY BE FILLED HERE FOR ANY CONNECTION)
YES
70
IS A COMPLETE RESPONSE AVAILABLE FROM PARTICIPATOR?
62
ARE BYTES AVAILABLE ON THE STREAM?
NO
YES
64
ADD TO USER-SPACE FIFO PER CONNECTION
68
LOOK FOR AN AVAILABLE COMPLETE DATA INSTRUCTION FOR ANY CONNECTION BY EXTRACTING PACKETS BYTEWISE FROM FIFO
66
ARE WE THROUGH ALL CONNECTIONS?
NO
YES

FIG. 5

CLIENT CHANNEL DATA STRUCTURE AND INFORMATION FLOW DIAGRAM

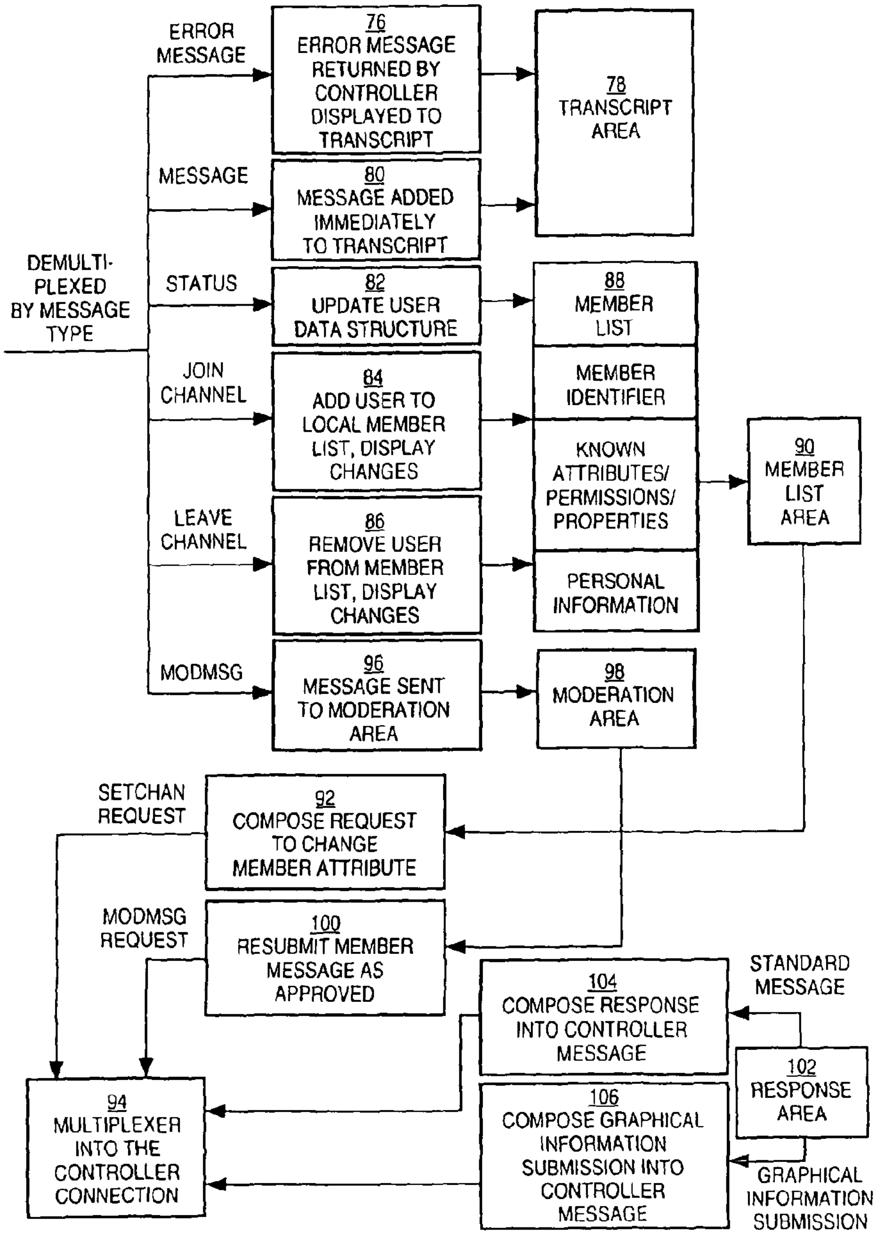

ERROR MESSAGE
76 ERROR MESSAGE RETURNED BY CONTROLLER DISPLAYED TO TRANSCRIPT
78 TRANSCRIPT AREA
MESSAGE
80 MESSAGE ADDED IMMEDIATELY TO TRANSCRIPT
DEMULTI-PLEXED BY MESSAGE TYPE
STATUS
82 UPDATE USER DATA STRUCTURE
88 MEMBER LIST
JOIN CHANNEL
84 ADD USER TO LOCAL MEMBER LIST, DISPLAY CHANGES
MEMBER IDENTIFIER
KNOWN ATTRIBUTES/ PERMISSIONS/ PROPERTIES
90 MEMBER LIST AREA
LEAVE CHANNEL
86 REMOVE USER FROM MEMBER LIST, DISPLAY CHANGES
PERSONAL INFORMATION
MODMSG
96 MESSAGE SENT TO MODERATION AREA
98 MODERATION AREA
SETCHAN REQUEST
92 COMPOSE REQUEST TO CHANGE MEMBER ATTRIBUTE
MODMSG REQUEST
100 RESUBMIT MEMBER MESSAGE AS APPROVED
104 COMPOSE RESPONSE INTO CONTROLLER MESSAGE
STANDARD MESSAGE
102 RESPONSE AREA
94 MULTIPLEXER INTO THE CONTROLLER CONNECTION
106 COMPOSE GRAPHICAL INFORMATION SUBMISSION INTO CONTROLLER MESSAGE
GRAPHICAL INFORMATION SUBMISSION

FIG. 6

PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM

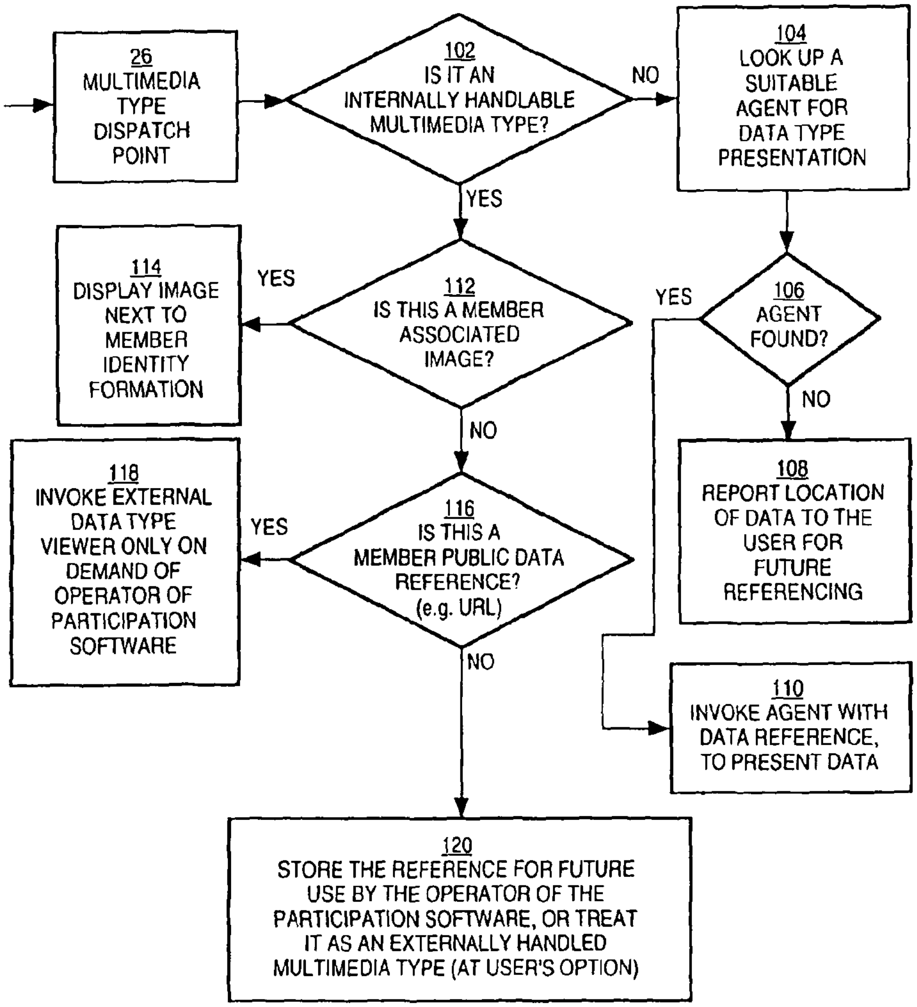
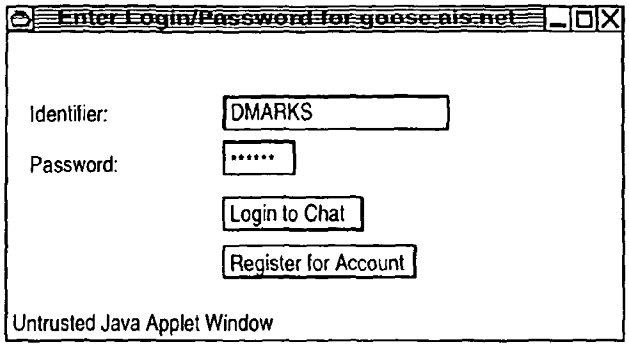

26
MULTIMEDIA TYPE DISPATCH POINT
102
IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104
LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114
DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112
IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106
AGENT FOUND?
NO
NO
108
REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
118
INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116
IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
NO
110
INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120
STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

FIG. 7

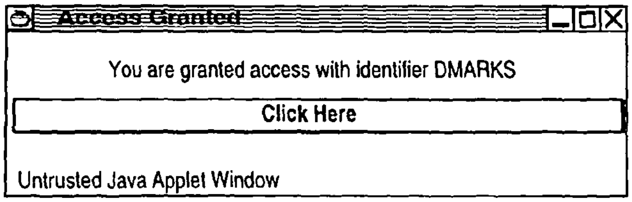

Enter Login/Password for goose.ais.net

Identifier: DMARKS

Password: ••••••

Untrusted Java Applet Window

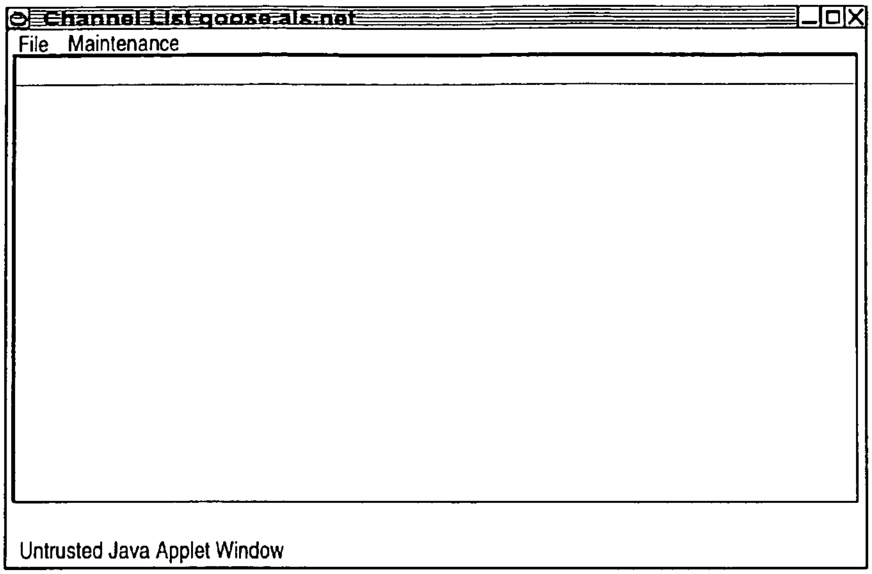
FIG. 8


Access Granted

You are granted access with identifier DMARKS

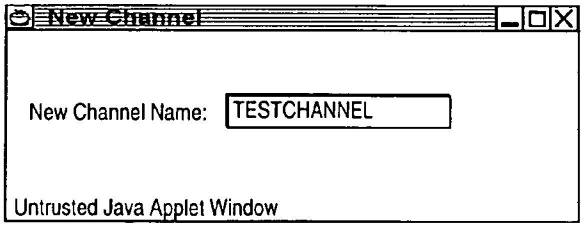
Untrusted Java Applet Window

FIG. 9



Untrusted Java Applet Window

FIG. 10



New Channel Name: TESTCHANNEL

Untrusted Java Applet Window

FIG. 11

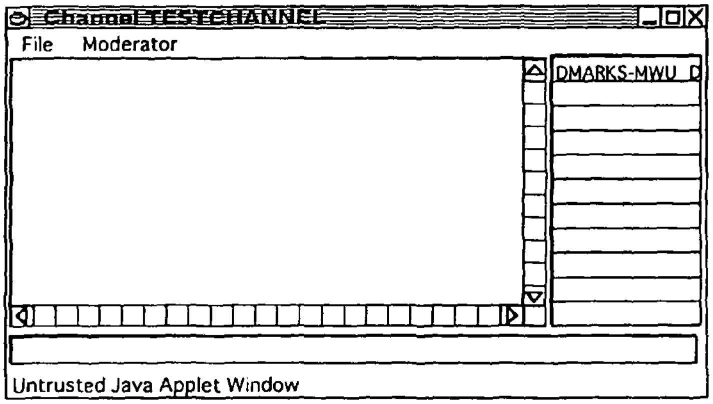

Channel TESTCHANNEL
File
Moderator
DMARKS-MWU D
Untrusted Java Applet Window

FIG. 12

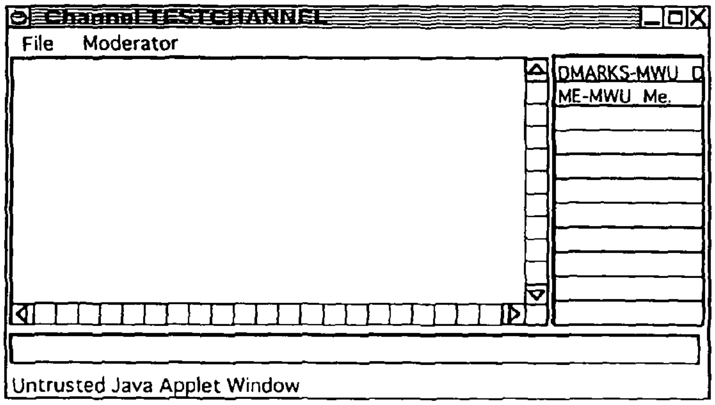
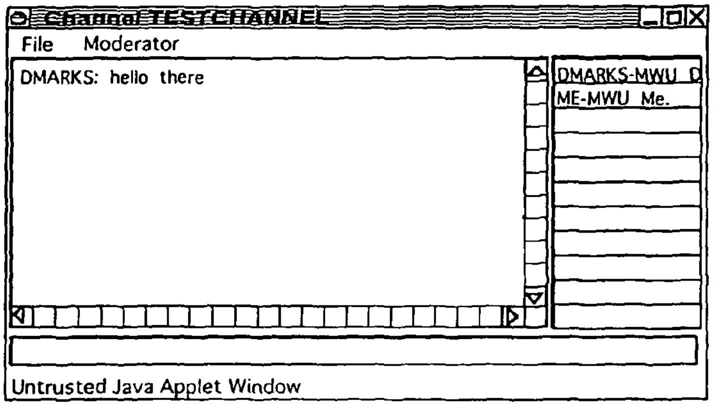

Channel TESTCHANNEL
File
Moderator
DMARKS-MWU D
ME-MWU Me.
Untrusted Java Applet Window

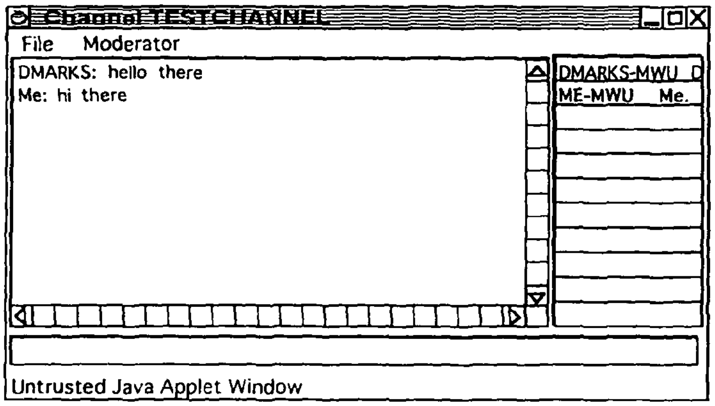
FIG. 13



DMARKS: hello there

DMARKS-MWU D
ME-MWU Me.

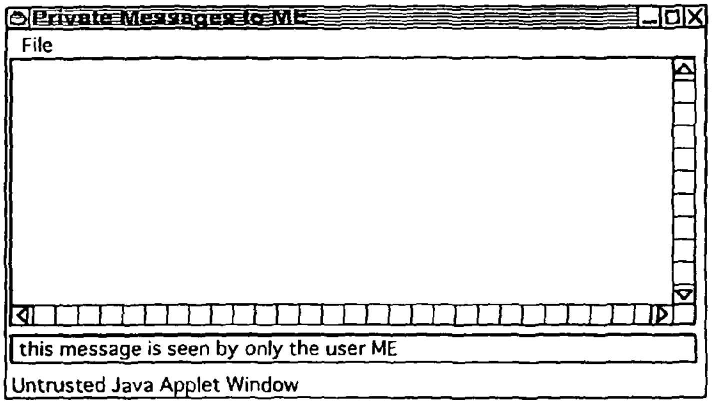
FIG. 14



DMARKS: hello there
Me: hi there

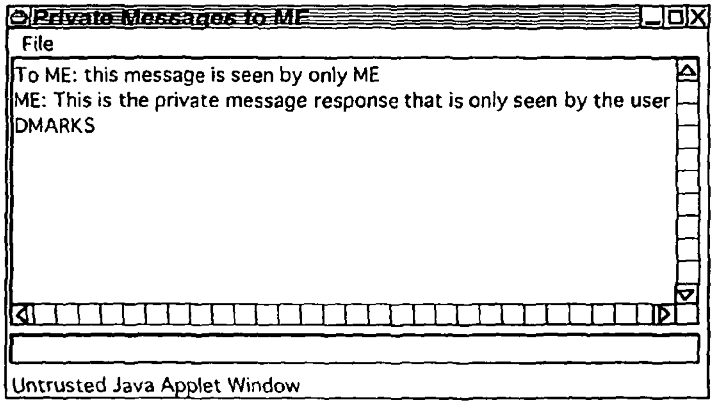
DMARKS-MWU D
ME-MWU Me.

FIG. 15



this message is seen by only the user ME

FIG. 16



To ME: this message is seen by only ME
ME: This is the private message response that is only seen by the user DMARKS

FIG. 17

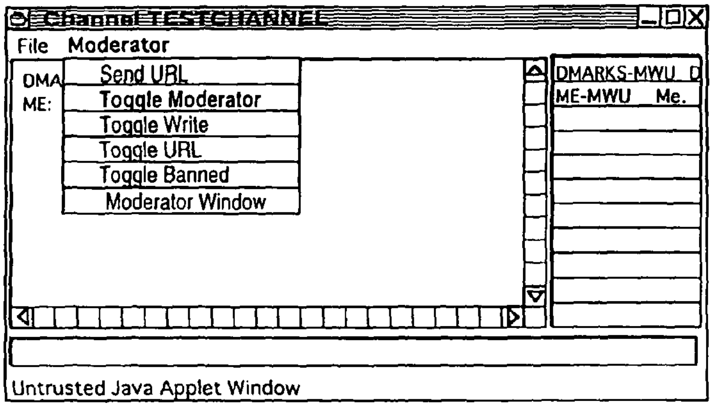
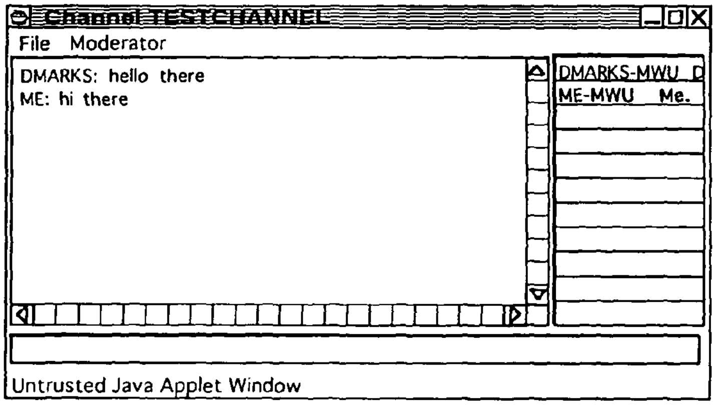


FIG. 18



DMARKS: hello there
ME: hi there

FIG. 19

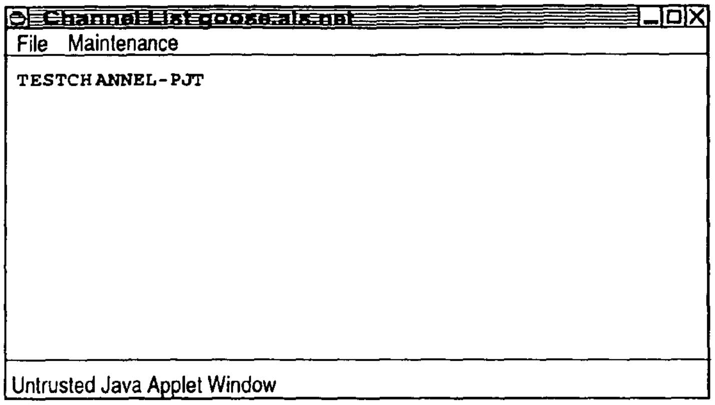

Channel List goose.als.net
File
Maintenance
TESTCHANNEL-PJT
Untrusted Java Applet Window

FIG. 20

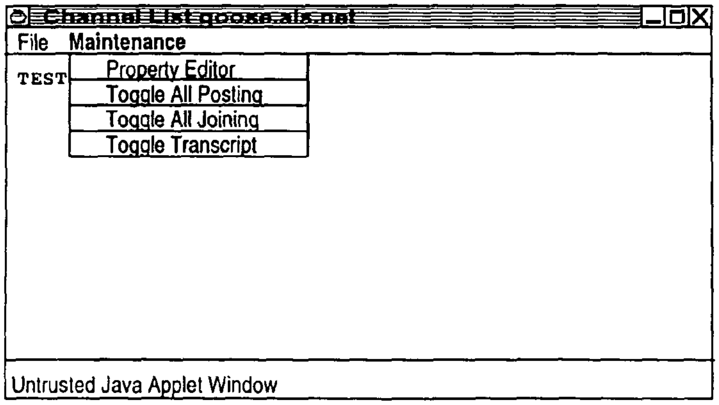
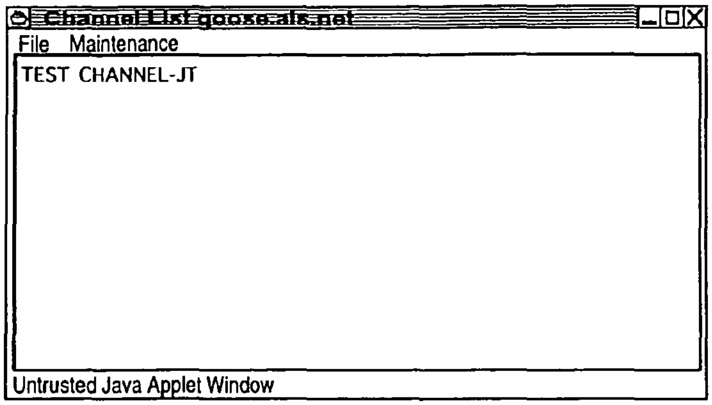
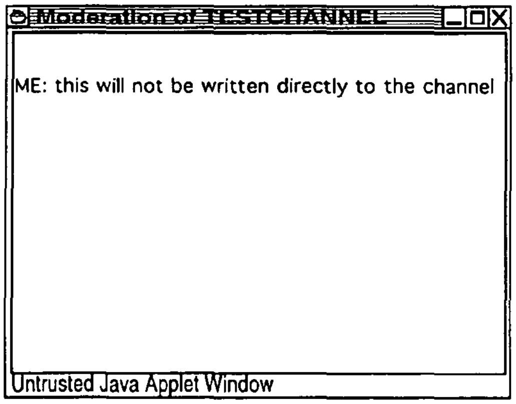

Channel List goose.als.net
File
Maintenance
TEST
Property Editor
Toggle All Posting
Toggle All Joining
Toggle Transcript
Untrusted Java Applet Window

FIG. 21



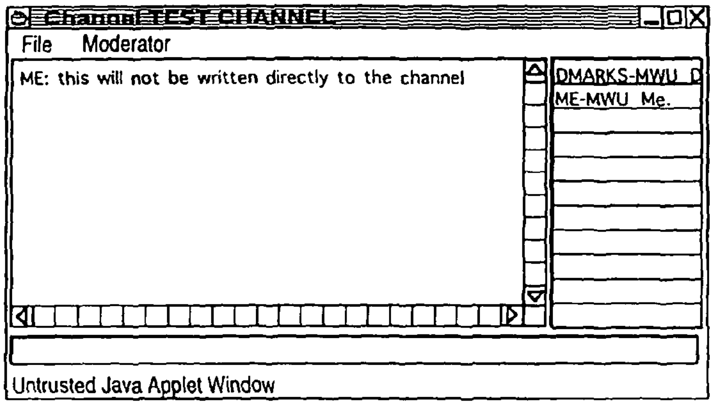
TEST CHANNEL-JT

FIG. 22



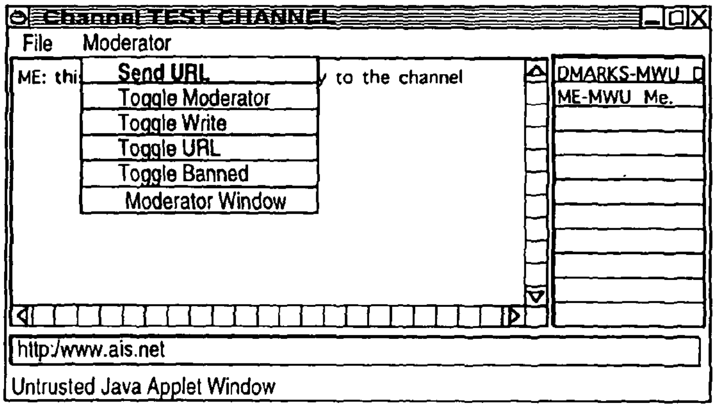
ME: this will not be written directly to the channel

FIG. 23



ME: this will not be written directly to the channel

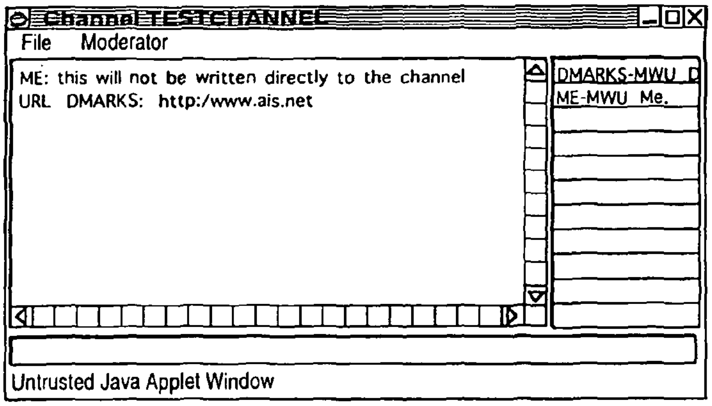
FIG. 24



ME: thi y to the channel

http:/www.ais.net

FIG. 25



ME: this will not be written directly to the channel
URL DMARKS: http:/www.ais.net

FIG. 26

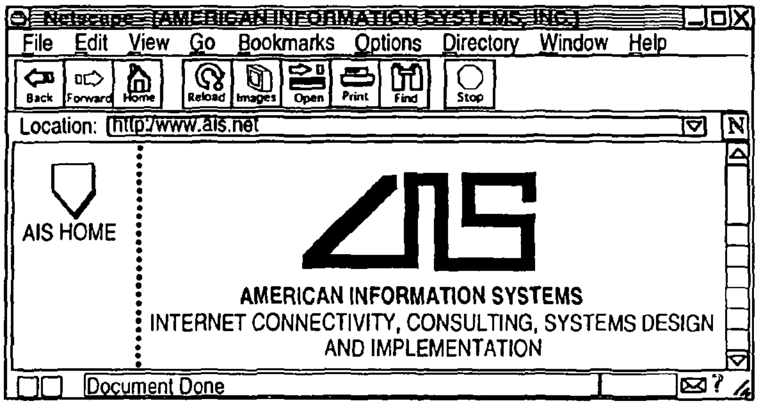
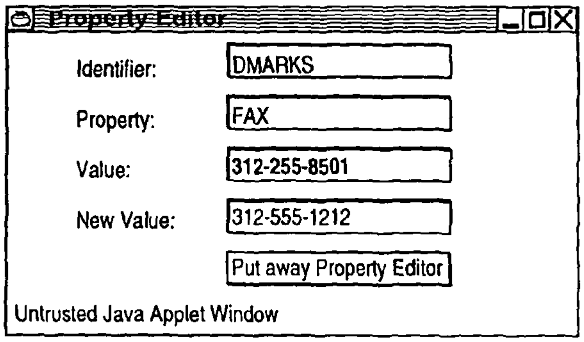


FIG. 27



Identifier: DMARKS

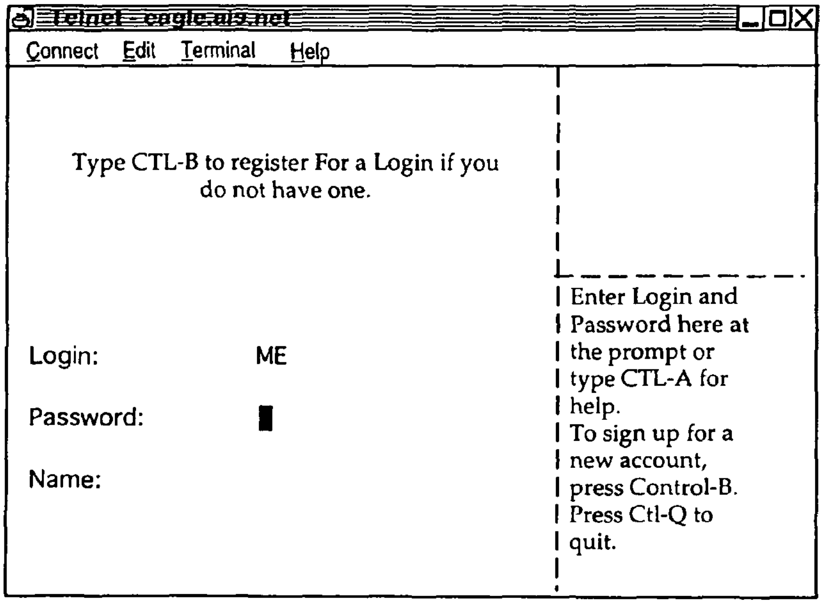
Property: FAX

Value: 312-255-8501

New Value: 312-555-1212

Untrusted Java Applet Window

FIG. 28



Type CTL-B to register For a Login if you do not have one.

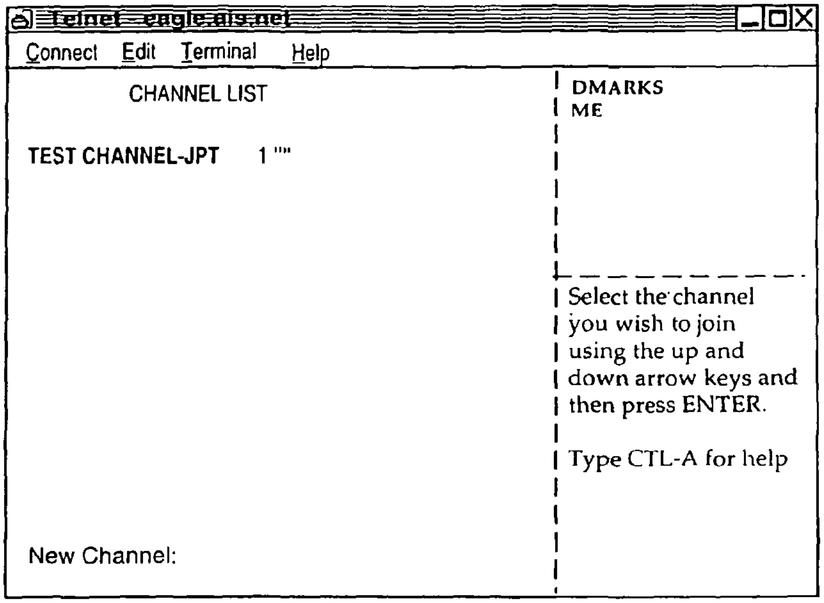
Login: ME

Password:

Name:

Enter Login and Password here at the prompt or type CTL-A for help.
To sign up for a new account, press Control-B.
Press Ctl-Q to quit.

FIG. 29



CHANNEL LIST

TEST CHANNEL-JPT 1 ""

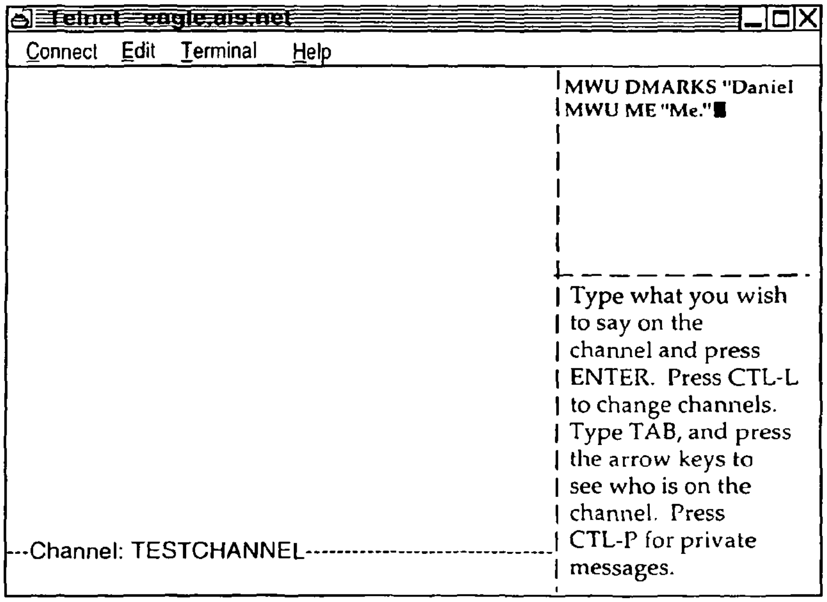
New Channel:

DMARKS
ME

Select the channel you wish to join using the up and down arrow keys and then press ENTER.

Type CTL-A for help

FIG. 30

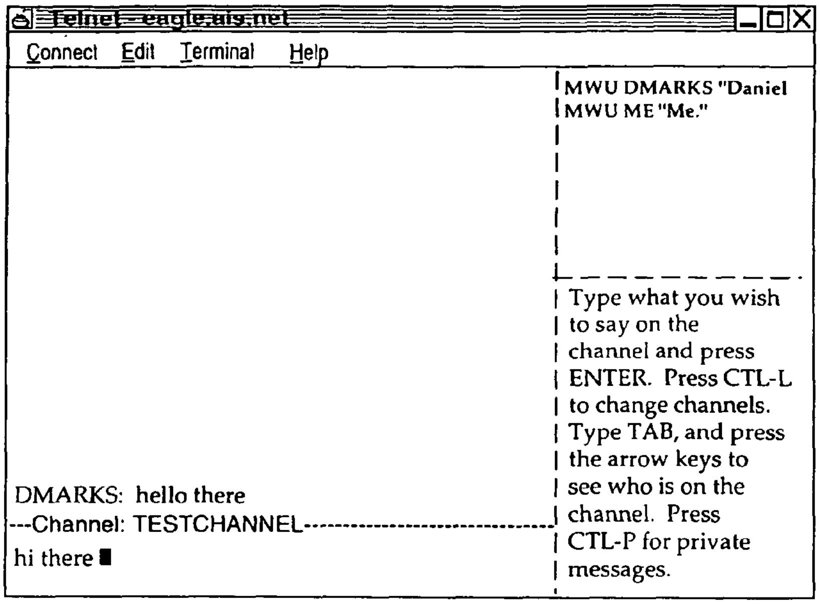


MWU DMARKS "Daniel
MWU ME "Me."■

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

---Channel: TESTCHANNEL---------------------------------

FIG. 31

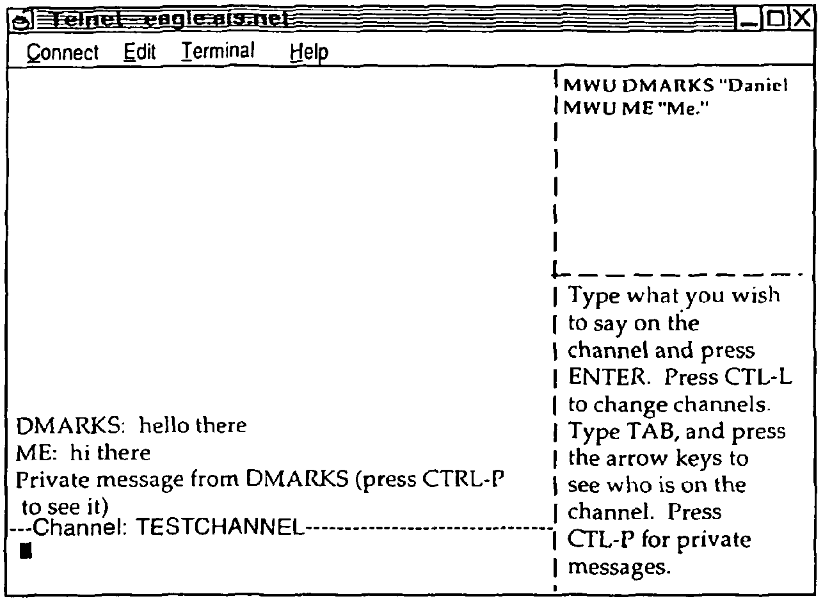


MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

DMARKS: hello there
---Channel: TESTCHANNEL--------------------------------
hi there ▮

FIG. 32

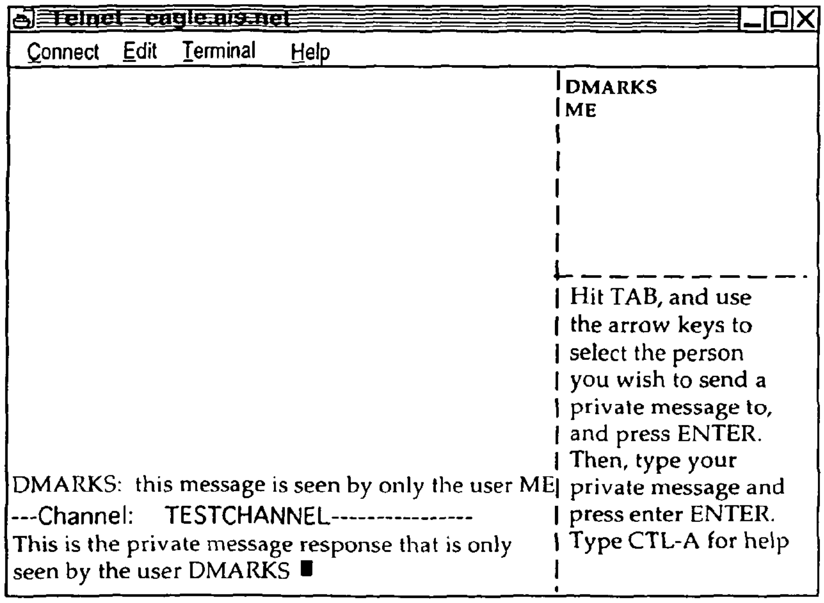


```
MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish
to say on the
channel and press
ENTER. Press CTL-L
to change channels.
Type TAB, and press
the arrow keys to
see who is on the
channel. Press
CTL-P for private
messages.

DMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P
 to see it)
---Channel: TESTCHANNEL--------------------------------
■
```

FIG. 33

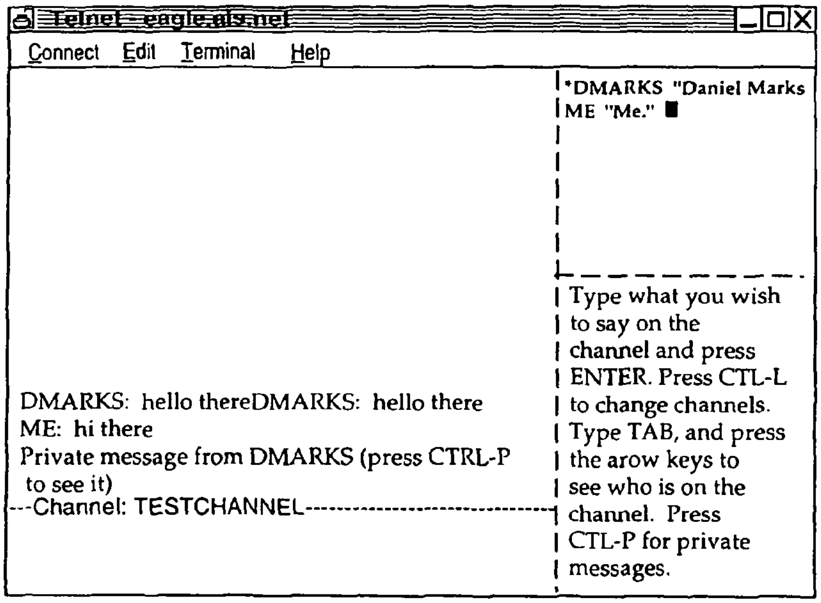


```
DMARKS
ME

Hit TAB, and use
the arrow keys to
select the person
you wish to send a
private message to,
and press ENTER.
Then, type your
private message and
press enter ENTER.
Type CTL-A for help

DMARKS: this message is seen by only the user ME
---Channel:    TESTCHANNEL----------------
This is the private message response that is only
seen by the user DMARKS ■
```

FIG. 34



```
*DMARKS "Daniel Marks
ME "Me."
```

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arow keys to see who is on the channel. Press CTL-P for private messages.

```
DMARKS: hello thereDMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P
 to see it)
---Channel: TESTCHANNEL------------------------------
```

# COMMUNICATIONS SYSTEM

## I. PRIORITY DATA

The present patent application is a continuation of and incorporates by reference U.S. patent application Ser. No. 09/399,578 filed by the same inventor on Sep. 20, 1999, as well as U.S. patent application Ser. No. 08/617,658, issuing as U.S. Pat. No. 5,956,491, on Sep. 21, 1999, titled Group Communications Multiplexing System that was filed by the same inventor on Apr. 1, 1996. U.S. patent application Ser. No. 09/399,578, filed Sep. 20, 1999, is a continuation of U.S. patent application Ser. No. 08/617,658, filed Apr. 1, 1996, issuing as U.S. Pat. No. 5,956,491, on Sep. 21, 1999.

## II. FIELD OF INVENTION

This invention is directed to an apparatus, a manufacture, and methods for making and using the same, in a field of digital electrical computer systems. More particularly, the present invention is directed to a digital electrical computer system involving a plurality of participator computers linked by a network to at least one of a plurality of participator computers, the participator computers operating in conjunction with the controller computer to handle multiplexing operations for communications involving groups of some of the participator computers.

## III. BACKGROUND OF THE INVENTION

Multiplexing group communications among computers ranges from very simple to very complex communications systems. At a simple level, group communications among computers involves electronic mail sent in a one way transmission to all those in a group or subgroup using, say, a local area network. Arbitrating which computers receive electronic mail is a rather well understood undertaking.

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

Even more complex is linking of computers to communicate in what has become known as a "chat room." Chat room communications can be mere text, such as that offered locally on a file server, or can involve graphics and certain multimedia capability, as exemplified by such Internet service providers as America On Line. Multiplexing in multimedia is more complex for this electronic environment.

On the Internet, "chat room" communications analogous to America On Line have not been developed, at least in part because Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications. Further, unlike the an Internet service provider, which has control over both the hardware platform and the computer program running on the platform to create the "chat room", there is no particular control over the platform that would be encountered on the Internet. Therefore, development of multiplexing technology for such an environment has been minimal.

Even with an emergence of the World Wide Web, which does have certain graphical multimedia capability, sophisticated chat room communication multiplexing has been the domain of the Internet service providers. Users therefore have a choice between the limited audience of a particular Internet Service provider or the limited chat capability of the Internet.

## IV. SUMMARY OF THE INVENTION

It is an object of the present invention to overcome such limitations of the prior art and to advance and improve the technology of group computer multiplexing to enable better computerized group communications.

It is another object of the present invention to provide a computerized human communication arbitrating and distributing system.

It is yet another object of the present invention to provide a group communication multiplexing system involving a controller digital computer linked to a plurality of participator computers to organize communications by groups of the participator computers.

It is still another object of the present invention to link the controller computer and the plurality of computers with respective software coordinated to arbitrate multiplexing activities.

It is still a further object of the present invention to provide a chat capability suitable for handling graphical, textual, and multimedia information in a platform independent manner.

These and other objects and utilities of the invention, which apparent from the discussion herein, are addressed by a computerized human communication arbitrating and distributing system. The system includes a controller digital electrical computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information and an output device for presenting information to a user having a user identity. A connection such as the Internet links the controller computer with each of the participator computers.

Controller software runs on the controller computer, programming the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups communicating through the controller computer and to distribute real time data to the respective ones of the groups.

Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message. The controller computer also conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

Therefore, for a computer system involving a plurality of programmed participator computers running the participator computer program can interact through a programmed controller computer with the controller computer multiplexing the communications for groups formed from the plurality, as well as arbitrating communications behavior.

## V. BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a depiction of hardware suitable for performing the present invention;

FIG. **2** is a communications overview of the present invention.

FIG. **3** is a data and communications dependency diagram for the controller group channel structure of the present invention.

FIG. **4** is a flow chart of the central controller loop communications for the controller computer.

FIG. **5** is a client channel data structure and information flow diagram of the present invention.

FIG. **6** is a participator software out-of-band multimedia information flow diagram of the present invention.

FIG. **7** is an illustration of a login/password screen of the present invention.

FIG. **8** is an illustration of a confirmation screen of the present invention.

FIG. **9** is an illustration of a channel list area screen of the present invention.

FIG. **10** is an illustration of a New Channel option pull-down menu screen of the present invention.

FIG. **11** is an illustration of a member on a new channel screen of the present invention.

FIG. **12** is an illustration of a second member on the new channel screen of the present invention.

FIG. **13** is an illustration of a communication on the new channel screen of the present invention.

FIG. **14** is an illustration of a private message window on the new channel screen of the present invention.

FIG. **15** is an illustration of a private message displayed on the private message window on the new channel screen of the present invention.

FIG. **16** is a further illustration of the private message on the private message window on new channel screen of the present invention.

FIG. **17** is an illustration of an attribute revocation on the new channel screen of the present invention.

FIG. **18** is a further illustration of the new channel screen of the present invention.

FIG. **19** is an illustration of the channel list window screen of the present invention.

FIG. **20** is an illustration of the toggle posting option on a screen of the present invention.

FIG. **21** is an illustration of a moderated version of the new channel screen of the present invention.

FIG. **22** is an illustration of a communication on a moderation window screen of the present invention.

FIG. **23** is an illustration of the communication passed on to the moderated version of the new channel screen of the present invention.

FIG. **24** is an illustration of a communication, for sending a graphical multimedia message, on to the moderated version of the new channel screen of the present invention.

FIG. **25** is an illustration, showing the name of the URL, on a moderated version of the new channel screen of the present invention.

FIG. **26** is an illustration of data associated with the graphical multimedia message on a moderated version of the new channel screen of the present invention.

FIG. **27** is an illustration of a proprietary editor, suitable for a dialog to change tokens, on a screen of the present invention.

FIG. **28** is an illustration of a text-based interface login/password screen of the present invention.

FIG. **29** is an illustration of a text-based interface group screen of the present invention.

FIG. **30** is another illustration of a text-based interface group screen of the present invention.

FIG. **31** is another illustration of a text-based interface group screen of the present invention.

FIG. **32** is an illustration of a text-based interface private message screen of the present invention.

FIG. **33** is another illustration of a text-based interface private message screen of the present invention.

FIG. **34** is another illustration of a text-based interface group with moderator screen of the present invention.

## VI. DETAILED DESCRIPTION OF THE DRAWINGS

In providing a detailed description of a preferred embodiment of the present invention, reference is made to an appendix hereto, including the following items.

Appendix Contents

ALLUSER C
ALLUSER H
CHANNEL C
CHANNEL H
CHANNEL HLP
CLIST C
CLIST H
CLIST HLP
EDITUSER C
EDITUSER H
ENTRYFRM C
ENTRYFRM H
ENTRYFRM HLP
HELP C
HELP H
HELPSCR C
HELPSCR H
LINEEDIT C
LINEEDIT H
LIST C
LIST H
LOGIN HLP
MAIN C
MAKEFILE
MESSAGE C
MESSAGE H
MODERAT HLP
PRIVATE C
PRIVATE H
PRIVATE HLP
SOCKIO C
SOCKIO H
STR C
STR H
UCCLIENT
USER C
USER H
WINDOW C
WINDOW H

Note that the appendix includes code for two different embodiments: a Tellnet embodiment and a JAVA embodiment. Documentation and error messages, help files, log files, are also included in the appendix. While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled.

Referring now to FIG. **1**, the overall functioning of a computerized human communication arbitrating and distributing System **1** of the present invention is shown with odd numbers designating hardware or programmed hardware, and even numbers designating computer program logic and data flow. The System **1** includes a digital Controller Computer **3**, such as an Internet service provider-type computer. The Controller Computer **3** is operating with an operating system.

System **1** also includes a plurality of digital Participator Computers **5**, each of which may be an IBM-compatible personal computer with a processor and a DOS operating system. Each of the Participator Computers **5** includes an Input Device **7** for receiving human-input information from a respective human user. The Input Device **7** can be, for example, a keyboard, mouse or the like. Each of the Participator Computers **5** also includes an Output Device **9** for presenting information to the respective user. The Output Device **9** can be a monitor, printer (such as a dot-matrix or laser printer), or preferably both are used. Each of the Participator Computers 5 also includes a Memory 11, such as a disk storage means.

The System 1 includes a Connection 13 located between, so as to link, the Controller Computer 3 with each of the Participator Computers 5. The Connection 13 can be an Internet or more particularly, a World Wide Web connection.

The Controller Computer 3 is running and under the control of Controller Software 2, which directs the Controller Computer 3 to arbitrate in accordance with predefined rules including a user identity, which ones of the Participator Computers 5 can interact in one of a plurality of groups through the Controller Computer 3 and to distribute real time data to the respective ones of the groups.

The Participator Computers 5 are each running and under the control of Participator Software 4, which directs each of the Participator Computers 5 to handle a user Interface 6 permitting one said user to send a multimedia information Message 8 to the Controller Computer 3, which arbitrates which of the Participator Computers 5 receives the multimedia information Message 8 and which conveys the multimedia information Message 8 to the selected participator computers 5 to present the multimedia information Message 8 to the respective user.

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.

Turning now to FIG. 2, there is shown a communications overview of the present invention. Beginning with the Controller Computer Software 2, reference is made to Block 10, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block 10 links to Block 12, which is illustrative of channel A . . . . Block 10 also links to Block 14, which illustrates handling private message A. Block 10 also links to Block 16, illustrative of handling out-of-band media. Block 10 additionally links to Block 18, which illustrates asynchronous status messages.

Multiple connections between the controller computer 3 and a plurality of participator computers 5 permit communication implemented via the interplay of controller software 2 and participator software 4. With particular regard to the participator software 4 illustrated in FIG. 2, Block 20 is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block 20 links to Block 22, which is illustrative of channel A . . . . Block 20 also links to Block 24, which illustrates handling private message A. Block 20 also links to Block 26, illustrative of handling out-of-band media via Block 28, which is illustrative of a Web browser or auxiliary computer program. Block 20 also links to Block 30, which illustrates asynchronous status message handling via Block 32, illustrative of user interface objects windows and screens.

De/multiplexing via API provides a "virtual connection" between Channel, Private Message, and Multimedia objects in the controller computer 3 and each participator computer 5. An alternate architecture is to allow for a separate connection between each object so that multiplexing/demultiplexing is not necessary and each object handles its own connection. This would influence system performance, however.

Turning now to FIG. 3, a data and communications dependency diagram controller group channel structure is illustrated. Beginning from what is designated as a portion of Block 10 the logic flows to Block 34 to consider JOIN, LEAVE, STATUS, SETCHAN API instructions. Block 34 examines member list maintenance instructions, accessing Block 36 to check permissions, list users, and change attributes. Note the exploded window 38 shows a display of member information including a user's name, personal information, and attributes/properties/permissions (operations involving the subsequently discussed tokens), i.e., stored per channel attributes under each member. In any case, confirmation or denial of access is communicated via Block 40 for multiplexing return of status messages to a target object.

From the portion of Block 10, the logic flows to Block 42 for MESSAGE and MODMSG API instructions. Block 42 tests which of the two instructions were received, and for MODMSG, the logic flows to Block 44, which tests whether the user is a moderator. If the user is not a moderator, the logic flows to Block 46, which sends a denial message through Block 40. If, however, the in Block 44 the user is a moderator, the logic flows to Block 48 for a repeat to all list members who are permitted to see the message, via Block 40.

Returning to Block 42, if MESSAGE is detected, the logic flows to Block 50, which tests whether a user has post permission. If the user has post permission, the logic flows to Block 48, etc. If the user does not have post permission, the logic flows to Block 52 to forward the message to moderators for approval, via Block 40.

Additionally, the logic flows from Block 10 to Block 54 for a URL API instruction. Block 54 tests whether the user has graphical multimedia communication privileges, and if not, the logic flows via Block 56, which sends a denial message via Block 40. Otherwise, if the user does have graphical multimedia communications privileges in Block 54, Block 58 sends graphical multimedia information to all approved users via Block 40.

Turning now to FIG. 4, central controller loop communications is illustrated. For the data on central poll point 58 (see Appendix POLL_POINT), a "do" loop begins at Block 60 for each connection. Block 62 tests whether bytes are available on the data stream. If they are, the bytes are added to user space FIFO per connection at Block 64, leading to Block 66, which tests whether there are any more connections. Note that in FIG. 4, if there are no more bytes available in Block 62, the logic skips to Block 66, and if Block 66 is not finished with all connections, the loop returns to Block 62. When all connections have been completed in Block 62, the logic flows to Block 68, which looks for an available complete data instruction for any connection by extracting packets byte-wise from the FIFO. Thereafter, Block 70 tests whether there is a complete response available from the participator computer. If the response is complete, the logic flows to Block 72 which, using a command type, demultiplexes into an appropriate object (output FIFOs may be filled here for any connection). The logic from Block 72 joins the "no" branch from Block 70 at Block 74, which enables unblocking for writing connections for only connections with data available to write, looping back to Block 58.

FIG. 5 shows a client channel data structure and information flow diagram. From a message that is demultiplexed by message type, there are six possibilities: ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG. ERROR MESSAGE is communicated to Block 76, where the error message is displayed to the transcript in the transcript area of Block 80. MESSAGE is communicated to Block 78 where the message is immediately added to the transcript in transcript area 78. STATUS is communicated to Block 82 to update user data structure; JOINCHANNEL is communicated to Block 84 to remove a user from the member list and display the change;

and LEAVECHANNEL is communicated to Block **86**. From Block **82**, Block **84**, and Block **88**, the logic flows to Block **88**, which includes a member list, a member identifier, known attributes/permissions/properties, and personal information. From Block **88**, the logic proceeds to Block **90**, a member list area, and on to Block **92** to compose a request to change a member attribute. This "SETCHAN request is then communicated to Block **94**, which is the multiplexer leading to the controller computer connection.

MODMSG is communicated to Block **96**, which sends the message to the moderation area of Block **98**, and then to Block **100** to resubmit a member message as approved, thereby conveying a MODMSG request to Block **94**.

Note that a response is prepared in the response area of Block **102**. If the response is a standard message, it is conveyed to Block **104** to compose the response into a controller message, thereby sending a MESSAGE request to box **94**. If, however, the message is a graphical information submission, the logic flows from Block **102** to Block **106** to compose the graphical information submission into a controller message, thereby sending a URL request to Block **94**.

FIG. **6** is a participator software out-of-band multimedia information flow diagram, which begins with Block **26**, the multimedia type patch point. Block **26** leads to Block **102**, which tests whether there is an internally handlable multimedia type. If not, Block **104** looks up a suitable agent for data type presentation, which leads to Block **106**, which tests whether an agent was found. If not, Block **108** reports location of data to the user for future referencing. If the agent is found in Block **106**, the logic flows to Block **110**, which invokes the agent with a data reference to present the data.

If the multimedia type is internally handlable from Block **102**, the logic flows to Block **112**, which tests whether this is a member associated image. If it is a member associated image, Block **114** displays the image next to member identity information, and if it is not, the logic flows to Block **116**, which tests if this is a member public data reference (e.g., a URL). 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).

With further regard to the manner of interaction between the controller computer **3** and the participator computers **5**, and their respective computer programs **2** and **4**, includes a moderation capability that is controlled, or arbitrated, pursuant to system **1** recognizing user identity. Note that using the user identity for moderation purposes is a use additional to the use of the user identity for security purposes.

One embodiment of the present invention is to bring chat capability to the internet and World Wide Web. However, another embodiment involves non-internet relay chat. In either embodiment, System **1** is state driven such that synchronous and asynchronous messages can be communicated. For an asynchronous notification, each message is sent through the system **1** (API), which updates the information on the output device of the participator computers **5**. For a synchronous notification, a participator computer **5** must interrogate the system **1** for a message.

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. The control computer database serves as a repository of tokens for other programs to access, thereby affording information to otherwise independent computer systems. In the database, the storage of tokens can be by user, group, and content, and distribution controls can also be placed on the user's tokens as well as the database.

Each token is used to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process. The arbitration also includes controlling a user's ability to moderate communications involving a group or subgroup of the participator computers **5**. Once in a group, temporary tokens are assigned for priority to moderate/submoderate groups (a group is sometimes known as a channel in multiplexing terminology).

Accordingly, tokens are used by the controller computer **5** to control a user's group priority and moderation privileges, as well as controlling who joins the group, who leaves the group, and the visibility of members in the group. Visibility refers to whether a user is allowed to know another user is in the chat group.

Tokens are also used 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.

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

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

With regard to controlling communications in a group (which is in essence a collection of user identities), control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages.

Note that tokens for members in group can involve multiples formed in real time, say, within the span of a conversation. For example, for private communication, tokens are immediately formed to define a group of 2 users. Hierarchical groups within groups can also be formed, with each inheriting the properties of the group before it. Thus, a subgroup can include up to all members or more by adding any surplus to the former group.

With further regard to the controller computer **3**, e.g., a server, information is controlled for distribution to the user interfaces at selected ones of the participator computers **5**. The controller computer program, in one embodiment, can be a resident program interface (such as a JAVA application). There can be a token editor object (window/tear down, etc.) per group, private communication, user, channel listings, user listings, etc. Each can link up in a token hierarchy for arbitration control.

The controller computer **5**, by means of the controller computer program **2**, keeps track of states and asynchronous messages as well as generating a synchronous message as a user logs in or interrogates system **1**.

With regard to multimedia information messages **8**, such messages are of independent data types, e.g., audio/video data types. The content of the message (e.g., a URL) permits the System **1** to automatically determine the handling of the message: either the Controller Computer **3** passes the content of Message **8** directly, or the Controller Computer **3** determines from the Message **8** how to find the content, say via Netscape. Accordingly, Message **8** can communicate video and sound (or other multimedia, e.g., a URL) to users, subject only to the server arbitration controls over what can be sent.

Turning now to an illustration of using the invention, the session starts with verifying the user's identity (at FIG. **7**). The login/password screen is shown, and the user enters his/her assigned login/password combination and clicks the "Login To Chat" button. If the password was entered correctly, a confirmation box appears on the screen.

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

To create a new group, the "New Channel" option is selected from a pull-down menu (at FIG. **9**). The name of the channel is entered by the input device **7**.

If the user has permission (this one does), a new channel is created for the group (at FIG. **10**). The window that displays the channel area has three regions: the bottom region, where responses are entered; the largest region, where a transcript of the communication is followed; and the rightmost region, which lists the group's current members. This list is continuously updated with asynchronously generated status messages received immediately when a new member joins the group. Only "DMARKS" is currently in this group. The "MWU" is the properties currently associated with DMARKS—the ability to moderate, write to the channel, and send multimedia messages.

A new member has joined the channel, and the member list status area is updated right away (at FIG. **11**). This new member has a login of "ME."

The user DMARKS now types "hello there" into the response area and presses RETURN (at FIG. **12**). This message is passed to the controller computer **5**, which sends the message to all channel members, i.e., those using participator computers **5**, including DMARKS.

The user ME now sends a message to the controller: "hi there" (at FIG. **13**). This message is also sent to all members by the controller computer **5**. Now user DMARKS clicks (using input device **7**, a mouse) on the name of the user "ME" in the member list window. The participator software **4** will now create a private message window, so that the users ME and DMARKS can exchange private messages. Private messages are only sent to the intended recipient by the controller, and no one else.

A private message window appears in response to DMARKS's request to open private communications with ME (at FIG. **14**). Now DMARKS types a message into the private message window's response area to ME: "this message is seen only by the user ME." When complete, the participator software **4** will forward this message to the controller computer **3**.

In response, the user ME has entered "This is the private message response that is only seen by the user DMARKS," which has been forwarded to user DMARKS (at FIG. **15**). This message is displayed immediately on DMARKS's window.

DMARKS now returns to the channel window for the group "TESTCHANNEL" (at FIG. **16**). To modify the permission attributes associated with user ME on the channel TEST CHANNEL, DMARKS (who is a moderator of the channel), clicks on the user ME in the member list to select ME, pulls down the Moderator menu, and selects "Toggle Moderator." This removes the moderator privileges from ME.

As a result of the attribute revocation, the "M" has disappeared from next to ME's name in the member list (at FIG. **17**), indicating that the property is no longer associated with the user ME.

Now DMARKS returns to the Channel List window (at FIG. **18**). DMARKS wishes to fully moderate the contents of the channel TESTCHANNEL, censoring all unwanted communications to the channel. DMARKS returns to the channel list, and selects the channel TESTCHANNEL by clicking on its name in the channel list.

Now DMARKS selects the "Toggle All Posting" option in the Maintenance pull-down menu (at FIG. **19**). This will turn off the channel property "posting," (or sending communications to the channel without moderator approval) which will be indicated by the removal of the letter "P" from next to the name TESTCHANNEL (at FIG. **20**).

Now the letter "P" is removed from after the name TESTCHANNEL in the Channel List window (at FIG. **21**), indicating that this channel is now moderated and will only have free posting ability by designated members.

Now, type user ME (who is also on channel TESTCHANNEL) wishes to send communications: "this will not be written directly to the channel" (at FIG. **22**). The controller, instead of sending it immediately to the channel to be seen by all members, will instead forward the message to the moderators for approval. The moderator, DMARKS, will then see the message on the Moderation Window, which provides a preview of any messages to be sent. To approve a message for general viewing, DMARKS now clicks on the message.

Now that DMARKS has clicked directly on the message, it is displayed inside the group's Channel window for all members to see (at FIG. **23**).

DMARKS now wishes to send a graphical multimedia message. This implementation sends graphical multimedia images by allowing a channel member to specify an Internet URL of a graphical multimedia resource to be presented to the group members. In this example, DMARKS wishes to send the URL "http://www.ais.net" (corresponding to the World Wide Web home page of American Information Systems, Inc.) to the channel members. DMARKS enters the URL into the response window, and selects "Send URL" from the Moderator pull-down menu (at FIG. **24**).

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.

Finally, DMARKS wishes to manually modify the attribute tokens associated with the user (at FIG. **27**). The user invokes the Property Editor dialog, which allows the user to view and change the tokens associated with a user. A property of a given user is determined by the Identifier and Property names. An old value of the property is shown, and a token value can be changed in the "New Value" field. With this property editor, a user with sufficient permissions (tokens) can change any of the tokens or security parameters of any user, or a user's ability to change security parameters can be restricted.

To start with an alternate embodiment using a text-based interface, a user is presented by the login/password screen (at FIG. **28**). This screen is where a user enters the information that proves his/her identity. The user must now enter his/her login and password to identify themselves.

After the user has been identified by the controller the Channel List screen appears (at FIG. **29**). The names of channels and their associated properties are shown on this screen. By using the arrow keys and highlighting the desired channel, ME may enter any publicly joinable group. Currently, there is only one group TESTCHANNEL, which ME will join.

Now the screen for the channel TESTCHANNEL appears (at FIG. **29**). The screen is split into four regions. The bottom left region is the response line, where messages users wish to enter appear. The upper left region is the transcript area where the communications of the group's channel appear as they occur. The upper right region is the Member List region, where a continuously updated list of members' names appear, with their attributes.

A message appears in the transcript area. The controller has forwarded a message to the group from DMARKS, "hello there" (at FIG. **31**), which is seen by all members of the group, including ME. Now ME will respond, by entering "hi there" into the response area.

When ME is finished entering his response, the participator software forwards the response to the controller, which sends it to the members of the channel. In the transcript area, the participator software notifies the user that it has received a private message from DMARKS, which is waiting inside the private message screen. To see the private message, ME presses the private message screen hot key.

A private message screen appears (at FIG. **32**), and the private message from DMARKS is at the bottom of the transcript area. Now to reply, ME types his response into the response area.

Now ME will return to the screen for the channel TESTCHANNEL. The member list area has changed because DMARKS has revoked ME's moderator permission. ME is no longer permitted to see the permissions of other users, so this information has been removed from his display (at FIG. **33**). The only information he can see now is who is moderator (at FIG. **34**). A "*" next to the identifier of a member of the group indicates the member is a moderator of the group. ME is no longer a moderator, and therefore a "*" does not appear the identifier ME.

To furthere exemplify the use of the present invention, the following is a transcript of communications produced in accordance herewith.

POWERQUALITY JOHNMUNG: unclear about meaning of "first contingency"

POWERQUALITY SAM: mike, that is correct on IEEE 519

POWERQUALITY SKLEIN: In assessing network security (against outage) the first contingencies are tested to see how the power system should be reconfigured to avoid getting a second contingency and cascading into an outage.

POWERQUALITY MSTEARS: These outages point out the need for reliability as part of the overall customer picture of PQ

POWERQUALITY BRIAN: Hi Jennifer, hit crt-p for private message

POWERQUALITY SKLEIN: In simpler terms, a single point failure shouldn't crash the system.

POWERQUALITY SKLEIN: Are we all chatted out?

POWERQUALITY ANDYV: brian, johnmung has been banned!!! why?

POWERQUALITY BRIAN: no way, new subject

POWERQUALITY BRIAN: just a sec, andy

POWERQUALITY BRIAN: No banning on this channel, John is back on

POWERQUALITY TKEY: ieee 519 limits the harmonic current a customer can inject back into the pcc and limit the vthd the utility provides at the PCC

POWERQUALITY JOHNMUNG: thanks guys, for unbanning me—i've been thrown out of better places than this!

POWERQUALITY BRIAN: New subject . . . now . . . .

POWERQUALITY BRIAN: good one john . . . :)

POWERQUALITY MSTEARS: For critical facilities dual feeds or other backup capability need to be economically evaluated to keep the facility in operation

POWERQUALITY SAM: John, I remember that club very well

POWERQUALITY JOHNMUNG: question: please comment on frequency of complaints involving spikes, sags or harmonics

POWERQUALITY WARD: Problems caused by sags is the main complaint.

POWERQUALITY BRIAN: What subject does anyone want to see the next chat

POWERQUALITY WARD: Surges is probably next; harmonics really don't cause that many problems, although they are certainly there.

POWERQUALITY ANDYV: what is the solution ward?

POWERQUALITY TKEY: Agree they are the most frequent (sags) and the panel session on the cost of voltage sags at PES drew 110 people

POWERQUALITY SAM: harmonics tend to be an interior problem within a facility, rather than on the distribution system

POWERQUALITY WARD: The best solution is making the equipment less susceptible to sags. This requires working with the manufacturers.

POWERQUALITY ANDYV: won't that cost more

POWERQUALITY MSTEARS: The complaint of surges covers many things in the customers eyes sags have become a real problem because they are harder to resolve

POWERQUALITY GRAVELY: John—The latest EPRI results confirms the 90+% of the time SGS are the problem and short term ones.

POWERQUALITY WINDSONG: What is the topic for the 25??

POWERQUALITY WARD: Each problem can be dealt with as it occurs, but the time involved gets very expensive.

POWERQUALITY JOHNMUNG: making equipment less susceptible causes legal problems for manufacturers-as each improvement can be cited by component as example of malfeasance

POWERQUALITY WARD: AndyV: The cost to the manufacturer increases. The overall cost to everyone involved decreases.

POWERQUALITY TKEY: customer pays any way you cut it, if the eqpt is more immune customers pay only once instead of every time the process fails

POWERQUALITY BRIAN: The topic is regarding Power Quality

POWERQUALITY BRIAN: This chat is available for everyone 24 hours a day

POWERQUALITY ANDYV: ddorr>>will the manufacturer spend more to produce a better product

POWERQUALITY WARD: And as Tom says, the cost to the customer is far less.

POWERQUALITY BRIAN: This chat will be functioning 24 hrs/day

POWERQUALITY BRIAN: please usae it
POWERQUALITY BRIAN: The next panel discussion is November 15th
POWERQUALITY WARD: Andy, that's where standards come in.
POWERQUALITY SKLEIN: Is the customer capable of resolving the fingerpointing among the manufacturers and utilities?
POWERQUALITY DDORR: andy, only if the end users create a market for pq compatible eqpt by demanding better products
POWERQUALITY MSTEARS: The manufacturers problems in including fixes is being competative with some who doesn't provide the fix
POWERQUALITY ANDYV: how will we educate the general consumer?
POWERQUALITY GRAVELY: Is it possible to have a basic theme topic or some core questions for 15 November chat?
POWERQUALITY WARD: Stan, the customer cannot be expected to resolve the fingerpointing. The manufacturers and utilities need to work together.
POWERQUALITY ANDYV: about power quality and reliability?
POWERQUALITY SKLEIN: If electric power is going to be treated as a fungible commodity, there has to be a definition. Like, everyone knows what number 2 heating oil is.
POWERQUALITY SAM: Ideally a manufacturer would not be able to compete if they don't add the protective function in their products, but alot more public education is required before we get to this point.
POWERQUALITY WARD: Andy, there are many ways to educate the customers, but they require a lot of contact between the utility and the customers. The Western Resources Power Technology Center in Wichita is doing it, just as an example.
POWERQUALITY DDORR: standard power vs premium power is one solution as is std qpt vs Pq compatible eqpt
POWERQUALITY SKLEIN: I want to buy number 2 electric power and to be able to check the nameplates of my appliances to be sure they can take it. Just like I buy regular gasoline.
POWERQUALITY MSTEARS: Sam—I agree, that is partly the utilities responsibility since we serve the customers
POWERQUALITY BBOYER: What differentiates number 2 from number 1?
POWERQUALITY SKLEIN: I used the analogy of number 2 heating oil. I don't know what number 1 heating oil is.
POWERQUALITY DDORR: Number two has cap switching and all the normal utility operational events while number one is much better
POWERQUALITY SKLEIN: Perhaps we can just say regular vs high test.
POWERQUALITY SAM: mike, yes a joint effort between the utility, manufacturer and standards juristictions is a goal for utilicorp as we move forward with offering from our strategic marketing partners, and bring PQ technologies to the public
POWERQUALITY TKEY: We are finding that many mfgrs want to produce pq compatible equipment, but they have no clue as to what to test for
POWERQUALITY ANDYV: Tom>>will the IEC standards help?
POWERQUALITY TKEY: Its up to the utility to help define normal events IEC will take time
POWERQUALITY SKLEIN: You can't have a commodity product with all the variation in specifications we have been discussing. It has to be regular, premium, and super premium or it won't work.
POWERQUALITY JOHNMUNG: Tom as a former manufacturer i sympathize—your work at PEAC is invaluable but anecdotal knowledge from utility people on the firing line is equally important
POWERQUALITY TKEY: Super premium, does that mean a UPS?
POWERQUALITY ANDYV: how do you stop a facility from affecting you super-premium power?
POWERQUALITY TKEY: John, Good Point
POWERQUALITY SAM: Tkey, a ups, local generation or redundant service
POWERQUALITY SKLEIN: This is what I meant earlier by electricity being a non-virtualizable service. You can't make each customer see the power system as though they had their own dedicated generating plant.
POWERQUALITY BRIAN: THE CHAT CHANNEL WILL BE OPEN 24/HRS/DAY 7 DAYS A WEEK POWERQUALITY TKEY: I must sign out for about 5 minutes but I'll be back
POWERQUALITY BRIAN: OK TOM
POWERQUALITY MSTEARS: PQ for facilities need to be done with a system perspective to get the right resolution
POWERQUALITY BBOYER: Andy's question is still relevant—how do stop a facility from downgrading utility service to other customers?
POWERQUALITY BRIAN: MIKE>>LETS SWITCH BACK TO RETAIL WHEELING
POWERQUALITY WARD: You work with that customer to do whatever is needed to correct their disturbances.
POWERQUALITY BBOYER: Be more specific
POWERQUALITY MSTEARS: Interaction between facilities can be evaluated and designed for
POWERQUALITY JOHNMUNG: as a key to hardening it helps to identify the most sensitive circuits, i.e. microprocessor logic, test for vulnerability under common surges, sags, rfi, and then notify users that their equipment contains these subsystems—for a start
POWERQUALITY BRIAN: hI DOUG
POWERQUALITY GRAVELY: Brian: Are you saving this session as a file? Can we get a list of chat session participants?
POWERQUALITY BRIAN: s, we may
POWERQUALITY DMARKS: gravely: hit TAB and use the arrow keys to page through the list of participants
POWERQUALITY SKLEIN: Will the session be available for downloading?
POWERQUALITY BRIAN: yes, Mike we will publish in PQ Magazine
POWERQUALITY WARD: Part of the agreement for high quality power should be that the customer receiving the power will not disturb the utility system.
POWERQUALITY BRIAN: if john let's us . . . .
POWERQUALITY GRAVELY: I tried that, however, netcruiser has a software problem and I cannot see all of the names.
POWERQUALITY SAM: most utilities rules and regulations already require that a customer not put anything back out on the utility system
POWERQUALITY BRIAN: MIKE G.>>WE WILL PUBLISH THIS IN PQ MAG NEXT MONTH IF ASNDY LETS US
POWERQUALITY BRIAN: HOW ABOUT IT ANDY?
POWERQUALITY ANDYV: ok
POWERQUALITY BRIAN: COOL

POWERQUALITY WARD: Standards will have to be set for what constitutes a disturbance, and then the utility should work with customers, install filters, etc., to be sure they stay within the rules.

POWERQUALITY BRIAN: THANKS ANDY

POWERQUALITY ANDYV: a meeting review or a summary of events

POWERQUALITY GRAVELY: It would be good to take a few minutes to recommend how the 15 November session could be more effective.

POWERQUALITY BRIAN: A SYNAPSE OF THIS CHAT WILL BE IN NEXT MONTHS PQ MAG

POWERQUALITY WINDSONG:

POWERQUALITY SKLEIN: I don't get PQ mag. Will it be on the Net?

POWERQUALITY BRIAN: STAN SIGN UP FOR IT ON OUR HOME PAGE

POWERQUALITY DOUGC: the transcript of this conference will be available on the EnergyOne pages.

POWERQUALITY BRIAN: YOU CAN SIGN UP ON LINE

POWERQUALITY BRIAN: HTTP://WWW.UTILICORP.COM

POWERQUALITY WINDSONG: Good comment Gravely Comments from the users would be greatly appreciated!!

POWERQUALITY SAM: PQ magazine is available online on the UCU internet bulletin board, http://www.utilicorp.com

POWERQUALITY ANDYV: or link from powerquality.com

POWERQUALITY BRIAN: YOU CAN GET A FREE MAG SUBSCRIPTION FROM

UTILICORP'S HOME PAGE

POWERQUALITY SKLEIN: Thanks

POWERQUALITY BRIAN: ALSO, THERE IS A PQ FORUM ON OUR HOME PAGE

POWERQUALITY JOHNMUNG: for November 15 shall we pick five key topics? suggest health care, energy storage rfi/emc as a few topics—also new gas turbine 25 kw generator just announce today—just some suggestions

POWERQUALITY BRIAN: GOOD SUGGESTION JOHN

POWERQUALITY ANDYV: lets develop an outline of topics for next time.

POWERQUALITY BRIAN: OK

POWERQUALITY GRAVELY: One suggestion for 15 November—Have participants place a list of desired topics on your other chat box and prioritize by interest level.

POWERQUALITY SKLEIN: How about deregulation and retail wheeling.

POWERQUALITY BRIAN: COMMENTS SHOULD BE SENT TO ME BY EMAIL

POWERQUALITY BRIAN: BSPENCER@UTILICORP.COM

POWERQUALITY BRIAN: 15 minutes remaining

POWERQUALITY ANDYZYREK: Let's discuss the new standard IEEE 1159.

POWERQUALITY ANDYV: may be we could generate an online questionaire to see what people are needing discussed.

POWERQUALITY BRIAN: but the chat is available for 24 hrs/day 7 days a week

POWERQUALITY ANDYV: what does IEEE1159 address?

POWERQUALITY BRIAN: Please send all suggestion to me for our next chat

POWERQUALITY BRIAN: Bobbin is not banned now

POWERQUALITY BRIAN: my fault

POWERQUALITY ANDYZYREK: New PQ measuring techniques. We have not received our issue yet.

POWERQUALITY ANDYV: You should have it my now.

POWERQUALITY BRIAN: Bobbin is not banned anymore

POWERQUALITY ANDYV: you can e-mail me or john at: editors@powerquality.com

POWERQUALITY BRIAN: is two hours right for this feature

POWERQUALITY JOHNMUNG: do i understand that many programmable logic controllers can be hardened by addition of simple CVT like a sola?

POWERQUALITY ANDYZYREK: Yes, but it is being delivered by snail mail.

POWERQUALITY ANDYV: no 2nd class

POWERQUALITY BRIAN: 15 minutes to go

POWERQUALITY ANDYV: Please e-mail me you complete name and address and I will mail you one today 1st class . . . now is that service or what?

POWERQUALITY BRIAN: Is two hours long enough for this chat?

POWERQUALITY TKEY: Im back

POWERQUALITY WARD: Brian, I think two hours is about right.

POWERQUALITY BRIAN: hi tom

POWERQUALITY BRIAN: good . . . .

POWERQUALITY ANDYV: yes I agree 2 hrs

POWERQUALITY BRIAN: anyone else

POWERQUALITY ANDYV: it the time of day correct?

POWERQUALITY BRIAN: questions now . . . .

POWERQUALITY SKLEIN: The topic foremost in my mind right now is what to eat for lunch. I enjoyed the discussion, which I understand has been historic in some sense. But I think I will sign off now and go eat.

POWERQUALITY SAM: 2 hours seems to work very well

POWERQUALITY DANIELH: time of day is good

POWERQUALITY BILLMANN: 2 hrs is fine

POWERQUALITY MSTEARS: Two hours work well, the middle of the day allows east and west coast to be involved

POWERQUALITY BRIAN: good, Will everyone be back for the next chat

POWERQUALITY GRAVELY: Brian, I will forward my recommendations on email, thanks.

POWERQUALITY BILLMANN: yes i'll be back

POWERQUALITY ANDYZYREK: Brian, would it be possible to have a forum published on your home page prior to November 15.

POWERQUALITY BRIAN: I would like to do another chat before November 15th, any thoughts

POWERQUALITY ANDY: U bet

POWERQUALITY SAM: I believe that this chat may set an attendance record for most participants during a first session

POWERQUALITY JOHNMUNG: a parting thought—"harmonics make the music rich, they make the tone insprinng—harmonics in your power line WILL BLOW THE BUILDINGS WIRING" tIM MUNGENAST

POWERQUALITY BRIAN: Your're all invited to return

POWERQUALITY BRIAN: the next chat

POWERQUALITY BRIAN: This chat feature will help set standards of how we view our industry

POWERQUALITY WARD: For me this was two hours very well spent, and it was quite enjoyable.

POWERQUALITY BRIAN: Tell a colleague about our chat November 15th

POWERQUALITY BRIAN: Thanks Ward

POWERQUALITY BRIAN: I would like to do this on a weekly basis, any thoughts yet

POWERQUALITY GRAVELY: John: talk it up in Germany!!

POWERQUALITY ANDY: I would like to thank utilicorp and everyone envolved.

POWERQUALITY BRIAN: Thanks Andy for your help

POWERQUALITY WARD: Did this notice go out to the Power Globe mailing list?
POWERQUALITY BRIAN: No, but could help us Ward with that
POWERQUALITY BRIAN: Lets all get the word out about this chat
POWERQUALITY WARD: I'm on the list and will be glad to forward anything you wish to it.
POWERQUALITY BRIAN: Please use it whenver you wish, even schedule your own chats whenver
POWERQUALITY JOHNMUNG: MANY THANKS TO uTILICORP AND ALL INVOLVED-FROM AN OLD STEAM BOATER :-)
POWERQUALITY BRIAN: thanks ward
POWERQUALITY BRIAN: Hi duane
POWERQUALITY BRIAN: This chat is officially over, but do stick around for foir more chatting
POWERQUALITY BRIAN: Thanks to all, cya on November 15th
POWERQUALITY MSTEARS: Ward, Tom, and John I appreciate your participation
POWERQUALITY BRIAN: Thanks Guys and Ladies!!!!!!!!!!
POWERQUALITY SWPPD: WHAT IS HAPPENING ON NOVEMBER 15
POWERQUALITY BRIAN: our next chat with a panel of experts
POWERQUALITY BRIAN: topic yet to be decided
POWERQUALITY DPSWOBO: Hi Brian, Sorry I was on the phone and could not respond right away. Did I get the time incorrectly for the chat?
POWERQUALITY BRIAN: please send us a suggestions
POWERQUALITY ANDY: good bye ;-)
POWERQUALITY BRIAN: Yeah, but stick around to chat with some friends
POWERQUALITY BRIAN: We had a total of 50 people and avg of 20 people at one time
POWERQUALITY BRIAN: Thanks everyone!!!Lunch Time
POWERQUALITY BRIAN: Next Chat November 15th at 10-12 ct
POWERQUALITY BRIAN: But this chat line is available 24 hrs/day/7 days a week
POWERQUALITY BRIAN: Please use it whenever
POWERQUALITY GRAVELY: Thanks to the panel and Utilicorp for the session!
POWERQUALITY BRIAN: Talk to your colleagues and friends about any particular topic
POWERQUALITY BRIAN: Come see our home page for new topics and chats
POWERQUALITY BRIAN: http://www.utilicorp.com
POWERQUALITY BRIAN: Thanks Power Quality Assurance Magazine and All our panel members
POWERQUALITY BRIAN::)
POWERQUALITY SWPPD: MISSED THIS SESSION. ICAN WE GET HARD COPY INFO?
POWERQUALITY BRIAN: yes swwp, it will be published in pq mag and our home page
POWERQUALITY BRIAN: catch our next session on November 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY SWPPD: THANKS A BUNCH!!
POWERQUALITY SWPPD: GOOD BYE!
POWERQUALITY BRIAN: no prob
POWERQUALITY BRIAN: cya
POWERQUALITY DESWETT:

POWERQUALITY TKEY: Good session brian, ddorr and I will be signing off now, look forward to the next session
POWERQUALITY DPSWOBO: Thanks for the info on the next session, we will get on next time
POWERQUALITY DMARKS: I hope everyone enjoyed this session.
POWERQUALITY MSTEARS: I am logging off Thanks
POWERQUALITY SAM: This is Tony and I am watching the action . . . we made history. Great work guys.
POWERQUALITY BRIAN: Lunch time
POWERQUALITY BRIAN: Next chat is November 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: please continue to look at utilicorp's hp
POWERQUALITY BRIAN: for more info
POWERQUALITY BRIAN: email if you have any questions regarding the chat
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: later
SUPPORT BRIAN: hi guys
SUPPORT BRIAN: success
SUPPORT BRIAN: yess!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
SUPPORT BRIAN: thanks for the help
SUPPORT BRIAN: cya
POWERQUALITY BRIAN: next chat on November 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: any suggestion on topics please contact me by email
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: hi chuck
POWERQUALITY BRIAN: hi randy
POWERQUALITY CPREECS: hello brian
POWERQUALITY BRIAN: How are you chuck
POWERQUALITY CPREECS: how has the participation been?
POWERQUALITY BRIAN: I am sorry you missed the official chat, but do come back at any time for some chatting
POWERQUALITY BRIAN: great 20 people avg. 50 total people
POWERQUALITY CPREECS: ?yes, i got some conflicting info
POWERQUALITY BRIAN: transcripts will be in PQ mag next month and on utilicorp's home page
POWERQUALITY CPREECS: what were the topics discussed?
POWERQUALITY BRIAN: how is that chuck
POWERQUALITY BRIAN: power quality, standards,
POWERQUALITY BRIAN: retail wheeling
POWERQUALITY BRIAN: cya, lunch time
POWERQUALITY CPREECS: later
POWERQUALITY BRIAN: bye all
POWERQUALITY BRIAN: email me chuck
POWERQUALITY RB: sorry I missed it. I got 12-2 est off the net. bye.
POWERQUALITY BRIAN: sorry RB
POWERQUALITY BRIAN: miss information
POWERQUALITY BRIAN: next chat is 10-12
POWERQUALITY BRIAN: ct
POWERQUALITY BRIAN: November 15th
POWERQUALITY BRIAN: bye
POWERQUALITY RB: thanks
POWERQUALITY BRIAN: no prob, tell all
POWERQUALITY ANDY: Is anyone still here talking about power quality?
POWERQUALITY DAVE: Just signed on that is what I was trying to find out

POWERQUALITY ANDY: the PQ chat was running from 11:00-1:00 cst
POWERQUALITY ANDY: Were you involved then?
POWERQUALITY DAVE: No I just got a chance to sign on now
POWERQUALITY ANDY: there were some great discussions.
POWERQUALITY ANDY: The transcripts will be available to down load at utilicorp.com Brian Spencer says.
POWERQUALITY ANDY: What is your experience in PQ
POWERQUALITY DAVE: That is what I was looking for, are they available to down load now, I work in a data center and have worked with UPS systems for about 12 years
POWERQUALITY DAVE: I did field service for Exide
POWERQUALITY ANDY: Brian just went to Lunch in KS I don/t know when it will available.
POWERQUALITY DAVE: Thanks for the Info on the downloads, I hope they do this again
POWERQUALITY ANDY: so do I.
POWERQUALITY DAVE: What is your experience on PQ
POWERQUALITY ANDY: I am the editor or Power quality mag.
POWERQUALITY DAVE: Good mag., I pick up alot in it
POWERQUALITY ANDY: do your receive power quality assurance magazine?
POWERQUALITY ANDY: great glad to hear it.
POWERQUALITY DAVE: We get it at work but I have asked to have it sent to my home
POWERQUALITY ANDY: did you get the latest issue with the lighting on the cover?
POWERQUALITY DAVE: Not yet, have seen it on line though
POWERQUALITY ANDY: great.
POWERQUALITY ANDY: any suggestion for editorial?
POWERQUALITY DAVE:
POWERQUALITY DAVE: no it is good
POWERQUALITY ANDY: ok.
POWERQUALITY ANDY: I am currently editing an article about VRLA battery charging.
POWERQUALITY DAVE: I am working on a resonant problem with Utility and was looking for info
POWERQUALITY ANDY: explain
POWERQUALITY ANDY: by the way my e-mail is andy@powerquality.com
POWERQUALITY DAVE: we are running a lot of 5th har. across our system in a large data center
POWERQUALITY ANDY: I see
POWERQUALITY ANDY: I will try to address this in an upcomming issue. may be march/april or even sooner.
POWERQUALITY DAVE: we have 4800 kw of UPS cap on two transformers and we have alot of 5th on our other boards
POWERQUALITY ANDY: If you are interested in writing up a case history including you solutions I would like to review it and poss. publish
POWERQUALITY MSTONEHAM: Is this chat session still active?
POWERQUALITY ANDY: YES
POWERQUALITY ANDY: We can'nt get enough!!!
POWERQUALITY DAVE: when we can get it fixed, It looks like we have a problem with input filtering on a couple of UPS, s
POWERQUALITY ANDY: input fro the utility or a generator?
POWERQUALITY DAVE: utility
POWERQUALITY MSTONEHAM: I understand there was a chat session earlier today with some guest" chatters". Is there an archive of the discussion since I missed it?

POWERQUALITY DAVE: we have 66 kv to 12 kv then to 480 v by 4 trans on property
POWERQUALITY ANDY: What are you leaning towards in a solution dave
POWERQUALITY ANDY: MTONEHAM>>yes but I don't know when. contact BSPENCER@utilicorp.com
POWERQUALITY DAVE: the computer seem to have no problem, but we have alot of motor heating/bad PF
POWERQUALITY MSTONEHAM: Thanks!
POWERQUALITY DAVE: we currently are working with a consulant but I am looking for more info
POWERQUALITY ANDY: will capacitors solve your problem
POWERQUALITY ANDY:
POWERQUALITY ANDY: there also is a forum under utilicorp.com where you can post you questions.
POWERQUALITY DAVE: Each 600 kw UPS has Input filtering/may need trap for 5th
POWERQUALITY ANDY: or you can access it form powerquality.com
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: Talk to ya later dave
POWERQUALITY DAVE: is PQ.com your Mag
POWERQUALITY ANDY: bye
POWERQUALITY DAVE: bye
POWERQUALITY ANDY: yes
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: :-)
POWERQUALITY MSTONEHAM:
POWERQUALITY MSTONEHAM: Is anyone else hear? There doesn't seem to be much traffic.
POWERQUALITY MSTONEHAM:
POWERQUALITY CILCOJRG: Hello—is the conference over?
POWERQUALITY CILCOJRG:
POWERQUALITY CILCOJRG: hello
POWERQUALITY BRIAN: yes
POWERQUALITY BRIAN: the conference was from 10-12 ct
POWERQUALITY BRIAN: someone gave out the wrong information
POWERQUALITY BRIAN: hello cilco
POWERQUALITY BRIAN: anyone still there
SUPPORT BRIAN: hi all
SUPPORT BRIAN: anyone there
POWERQUALITY BRIAN: jenny>>are you there
POWERQUALITY CJBOUTCHER: is anyone here a utility employee?
POWERQUALITY BRIAN: Hi chris
POWERQUALITY BRIAN: how are you?
POWERQUALITY CJBOUTCHER: hi brian it is quiet in here
POWERQUALITY BRIAN: the conference was at 10:00 ct
POWERQUALITY CJBOUTCHER: ah I see
POWERQUALITY CJBOUTCHER: when is the next one?
POWERQUALITY BRIAN: November 15th
POWERQUALITY BRIAN: 10-12
POWERQUALITY BRIAN: ct
POWERQUALITY CJBOUTCHER: is the channel open at other times?
POWERQUALITY BRIAN: yes 24 hours a dfay
POWERQUALITY CJBOUTCHER: but not much discussion?
POWERQUALITY BRIAN: not right now,
POWERQUALITY BRIAN: cya
POWERQUALITY CJBOUTCHER: bye
POWERQUALITY BRIAN: hi jenny

POWERQUALITY JOSH: hello?
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: are you awake yet?
POWERQUALITY BRIAN: just giving present this a.m.
POWERQUALITY BRIAN::)
POWERQUALITY BRIAN: who is guest96
POWERQUALITY GUEST96: test

While a particular embodiment of the present invention has been disclosed, it is to be understood that various different modifications are possible and are within the true spirit of the invention, the scope of which is to be determined with reference to the claims set forth below. There is no intention, therefore, to limit the invention to the exact disclosure presented herein as a teaching of one embodiment of the invention.

The invention claimed is:

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 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 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, 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.

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, 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, the method including:

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

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

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.

3. The method of claim 2, wherein at least one of the messages includes data representing sound.

4. The method of claim 3, further including:

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.

5. The method of claim 2, wherein at least one of the messages includes data representing video.

6. The method of claim 5, further including:

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.

7. The method of claim 2, wherein at least one of the messages includes data representing sound and video.

8. The method of claim 7, further including:

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.

9. The method of claim 2, further including:

storing, for the first user identity, an authorization associated with presentation of multimedia, the multimedia comprising graphic data; and

based on the authorization, presenting the multimedia at one of the participator computers corresponding to the second user identity.

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 receive communications from another of the members, 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 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.

**11**. The apparatus of claim **10**, wherein at least one of the messages includes data representing sound.

**12**. The apparatus of claim **11**, wherein the computer system is further programmed to provide access to a member-associated image.

**13**. The apparatus of claim **10**, wherein at least one of the messages includes data representing video.

**14**. The apparatus of claim **13**, wherein the computer system is further programmed to provide access to a member-associated image.

**15**. The apparatus of claim **10**, wherein at least one of the messages includes data representing sound and video.

**16**. The apparatus of claim **15**, wherein the computer system is further programmed to provide access to a member-associated image.

**17**. The apparatus of claim **10**, wherein the computer system is further programmed to provide access to a member-associated image.

**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 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.

**19**. The apparatus of claim **18**, wherein 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.

**20**. The apparatus of claim **19**, wherein the computer system is further programmed to provide access to a member-associated image.

**21**. The apparatus of claim **18**, wherein the multimedia data comprises graphic data.

**22**. The apparatus of claim **21**, wherein 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.

**23**. The apparatus of claim **22**, wherein the computer system is further programmed to provide access to a member-associated image.

**24**. The apparatus of claim **18**, wherein the multimedia data comprises audio data.

**25**. The apparatus of claim **24**, wherein 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.

**26**. The apparatus of claim **25**, wherein the computer system is further programmed to provide access to a member-associated image.

**27**. The apparatus of claim **24**, wherein the computer system is further programmed to provide access to a member-associated image.

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

**29**. The apparatus of claim **28**, wherein the computer system is programmed to allow the participator computers to communicate, in real time communications among members of the group, a pointer that produces a pointer-triggered message on demand.

**30**. The apparatus of claim **29**, wherein the computer system is further programmed to provide access to a member-associated image.

**31**. The apparatus of claim **28**, wherein the computer system is further programmed to provide access to a member-associated image.

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

**33**. The apparatus of claim **32**, wherein 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.

**34**. The apparatus of claim **33**, wherein the computer system is further programmed to provide access to a member-associated image.

**35**. The apparatus of claim **32**, wherein the computer system is further programmed to provide access to a member-associated image.

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

**37**. The apparatus of claim **36**, wherein 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.

**38**. The apparatus of claim **37**, wherein the computer system is further programmed to provide access to a member-associated image.

**39**. The apparatus of claim **36**, wherein the computer system is further programmed to provide access to a member-associated image.

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

**41**. The apparatus of claim **40**, wherein 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.

**42**. The apparatus of claim **41**, wherein the computer system is further programmed to provide access to a member-associated image.

**43**. The apparatus of claim **40**, wherein the computer system is further programmed to provide access to a member-associated image.

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

**45**. The apparatus of claim **44**, wherein the computer system is programmed to allow the participator of computers to communicate, in real time communications among members of the group, a pointer that produces a pointer-triggered message on demand.

**46**. The apparatus of claim **45**, wherein the computer system is further programmed to provide access to a member-associated image.

**47**. The apparatus of claim **44**, wherein the computer system is further programmed to provide access to a member-associated image.

**48**. The apparatus of claim **18**, wherein the computer system is further programmed to provide access to a member-associated image.

**49**. The apparatus of claim **18**, wherein the computer system is further programmed to provide access to member identity 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 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 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.

**51**. The apparatus of claim **50**, wherein the computer system is programmed to allow the participator computers to communicate, in real time communications among members of the group, a pointer that produces a pointer-triggered message on demand.

**52**. The apparatus of claim **51**, wherein the computer system is further programmed to provide access to a member-associated image.

**53**. The apparatus of claim **50**, wherein the computer system is further programmed to provide access to a member-associated image.

**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 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, 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; and

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

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.

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

**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.

**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.

**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 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 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, 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 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.

**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; wherein

at least some of the user messages are multimedia messages; 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, 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.

**60**. The system of claim **59**, further comprising participator software respectively operating on and directing each of the participator computers to enable one of said users to send one of the user messages to the controller computer and to enable the arbitrating and the distributing of the one of the user messages.

**61**. The system of claim **59**, wherein the user messages include an address to instruct the participator computers to optionally locate another multimedia message.

**62**. The system of claim **59**, wherein the user messages include an address to compel the participator computers to locate an other message and to present the other message at the output device.

**63**. The system of claim **59**, wherein the other message is a multimedia message.

**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 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, the method including:

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

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

arbitrating, in accordance with predefined rules including a test for an authenticated user identity, which ones of the participator computers can be a 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.

* * * * *

US008694657B1

(12) **United States Patent**
**Marks**

(10) **Patent No.: US 8,694,657 B1**
(45) **Date of Patent: *Apr. 8, 2014**

(54) **REAL TIME COMMUNICATIONS SYSTEM**

(76) Inventor: **Daniel L Marks**, Chappel Hill, NC (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/399,578**

(22) Filed: **Sep. 20, 1999**

**Related U.S. Application Data**

(63) Continuation of application No. 08/617,658, filed on Apr. 1, 1996, now Pat. No. 5,956,491.

(51) **Int. Cl.**
***G06F 15/16*** (2006.01)

(52) **U.S. Cl.**
USPC ........... **709/229**; 709/204; 709/206; 709/207; 709/225

(58) **Field of Classification Search**
USPC ......... 709/203, 231, 316, 204–207, 225, 229; 379/401, 202.01
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

| | | | | |
|---|---|---|---|---|
| 4,525,779 | A | 6/1985 | Davids et al. | |
| 4,710,917 | A | 12/1987 | Tompkins et al. | 709/204 |
| 4,953,159 | A | 8/1990 | Hayden et al. | 370/265 |
| 5,008,853 | A | 4/1991 | Bly et al. | |
| 5,195,086 | A | 3/1993 | Baumgartner et al. | 370/264 |
| 5,257,306 | A | 10/1993 | Watanabe | 348/14.09 |
| 5,325,419 | A | 6/1994 | Connolly et al. | 379/60 |
| 5,333,266 | A | 7/1994 | Boaz et al. | |
| 5,347,306 | A | 9/1994 | Nitta | 348/14.1 |
| 5,347,632 | A | 9/1994 | Filepp et al. | |
| 5,408,470 | A | 4/1995 | Rothrock et al. | |
| 5,440,624 | A * | 8/1995 | Schoof, II | 379/202.01 |
| 5,452,299 | A | 9/1995 | Thessin et al. | |
| 5,465,370 | A | 11/1995 | Ito et al. | 709/204 |
| 5,471,318 | A | 11/1995 | Ahuja et al. | 386/125 |
| 5,491,743 | A | 2/1996 | Shiio et al. | 709/204 |
| 5,528,671 | A | 6/1996 | Ryu et al. | |
| 5,548,506 | A | 8/1996 | Srinivasan | |
| 5,563,804 | A | 10/1996 | Mortensen et al. | |
| 5,572,248 | A | 11/1996 | Allen et al. | 348/14.1 |
| 5,572,643 | A | 11/1996 | Judson | 709/218 |
| 5,592,478 | A | 1/1997 | Weiss | 370/260 |
| 5,608,786 | A | 3/1997 | Gordon | |
| 5,613,056 | A | 3/1997 | Gasper et al. | 345/473 |
| 5,616,876 | A | 4/1997 | Cluts | 84/609 |

(Continued)

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| EP | 336 552 A2 | 10/1989 |

OTHER PUBLICATIONS

Kazuo Watabe et al., Distributed Multiparty Desktop Conferencing System: MERMAID, Oct. 1990, Proceedings CSCW '90, ACM, pp. 27-38.*

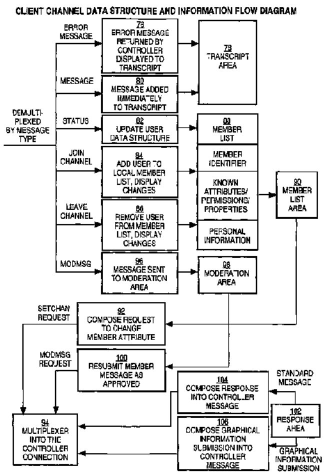
(Continued)

*Primary Examiner* — Patrice Winder
(74) *Attorney, Agent, or Firm* — Peter K. Trzyna, Esq.

(57) **ABSTRACT**

A system and method communicating via an Internet network, the system including: a plurality of computers connected to a computer system such that one of the plurality of computers, corresponding to a first of the user identities, and an other of the plurality of computers, corresponding to a second of the user identities, can send communications, and some of the communications are received in real time via the Internet. There can be a determination as to whether some of the communications are allowed.

**671 Claims, 22 Drawing Sheets**


CLIENT CHANNEL DATA STRUCTURE AND INFORMATION FLOW DIAGRAM
DEMULTI-PLEXED BY MESSAGE TYPE
ERROR MESSAGE
76 ERROR MESSAGE RETURNED BY CONTROLLER DISPLAYED TO TRANSCRIPT
78 TRANSCRIPT AREA
MESSAGE
80 MESSAGE ADDED IMMEDIATELY TO TRANSCRIPT
STATUS
82 UPDATE USER DATA STRUCTURE
88 MEMBER LIST
MEMBER IDENTIFIER
KNOWN ATTRIBUTES/ PERMISSIONS/ PROPERTIES
PERSONAL INFORMATION
JOIN CHANNEL
84 ADD USER TO LOCAL MEMBER LIST, DISPLAY CHANGES
90 MEMBER LIST AREA
LEAVE CHANNEL
86 REMOVE USER FROM MEMBER LIST, DISPLAY CHANGES
MODMSG
96 MESSAGE SENT TO MODERATION AREA
98 MODERATION AREA
SETCHAN REQUEST
92 COMPOSE REQUEST TO CHANGE MEMBER ATTRIBUTE
MODMSG REQUEST
100 RESUBMIT MEMBER MESSAGE AS APPROVED
STANDARD MESSAGE
104 COMPOSE RESPONSE INTO CONTROLLER MESSAGE
102 RESPONSE AREA
94 MULTIPLEXER INTO THE CONTROLLER CONNECTION
106 COMPOSE GRAPHICAL INFORMATION SUBMISSION INTO CONTROLLER MESSAGE
GRAPHICAL INFORMATION SUBMISSION

## (56) References Cited

U.S. PATENT DOCUMENTS

| | | | | | |
|---|---|---|---|---|---|
| 5,617,539 | A | | 4/1997 | Ludwig et al. | 709/205 |
| 5,621,727 | A | | 4/1997 | Vaudreuil | |
| 5,627,978 | A | | 5/1997 | Altom et al. | 715/758 |
| 5,659,692 | A | | 8/1997 | Poggie et al. | |
| 5,682,469 | A | | 10/1997 | Linnett et al. | 345/473 |
| 5,689,553 | A | * | 11/1997 | Ahuja et al. | 370/352 |
| 5,713,019 | A | | 1/1998 | Keaten | 707/10 |
| 5,721,763 | A | | 2/1998 | Joseph et al. | 379/88.04 |
| 5,724,508 | A | | 3/1998 | Harple, Jr. et al. | |
| 5,729,684 | A | | 3/1998 | Kuzma | 709/204 |
| 5,740,231 | A | | 4/1998 | Cohn et al. | |
| 5,754,775 | A | | 5/1998 | Adamson et al. | 709/204 |
| 5,761,201 | A | | 6/1998 | Vaudreuil | |
| 5,771,355 | A | | 6/1998 | Kuzma | 395/200.62 |
| 5,774,668 | A | | 6/1998 | Choquier et al. | 709/223 |
| 5,784,568 | A | | 7/1998 | Needham | 709/234 |
| 5,793,365 | A | * | 8/1998 | Tang et al. | 715/758 |
| 5,794,006 | A | | 8/1998 | Sandermah | 709/223 |
| 5,794,210 | A | | 8/1998 | Goldhaber et al. | 705/14 |
| 5,799,151 | A | * | 8/1998 | Hoffer | 709/204 |
| 5,801,700 | A | | 9/1998 | Ferguson | 715/748 |
| 5,802,281 | A | | 9/1998 | Clapp et al. | 709/228 |
| 5,812,552 | A | * | 9/1998 | Arora et al. | 370/401 |
| 5,822,523 | A | | 10/1998 | Rothschild et al. | 709/236 |
| 5,826,085 | A | * | 10/1998 | Bennett et al. | 709/316 |
| 5,832,212 | A | | 11/1998 | Cragun et al. | 395/188.01 |
| 5,850,442 | A | | 12/1998 | Muftic | 705/65 |
| 5,880,731 | A | | 3/1999 | Liles et al. | 715/758 |
| 5,889,843 | A | | 3/1999 | Singer et al. | 379/202.01 |
| 5,894,321 | A | * | 4/1999 | Downs et al. | 370/260 |
| 5,894,556 | A | | 4/1999 | Grimm et al. | |
| 5,924,082 | A | | 7/1999 | Silverman et al. | 705/37 |
| 5,933,599 | A | | 8/1999 | Nolan | 715/734 |
| 5,941,947 | A | * | 8/1999 | Brown et al. | 709/225 |
| 5,951,694 | A | | 9/1999 | Choquier et al. | |
| 5,956,509 | A | | 9/1999 | Kevner | 719/330 |
| 5,960,173 | A | | 9/1999 | Tang et al. | |
| 5,974,409 | A | | 10/1999 | Sanu et al. | 707/3 |
| 5,987,401 | A | | 11/1999 | Trudeau | 704/2 |
| 6,064,723 | A | | 5/2000 | Cohn et al. | |
| 6,119,101 | A | | 9/2000 | Peckover | |
| 6,289,390 | B1 | | 9/2001 | Kavner | |
| 6,560,707 | B2 | * | 5/2003 | Curtis et al. | 713/163 |
| 6,692,359 | B1 | | 2/2004 | Williams et al. | 463/42 |
| 8,407,356 | B1 | | 3/2013 | Marks | |

OTHER PUBLICATIONS

Tak K Woo and Michael J. Rees, A Synchronous Collaboration Tool for the World Wide Web, The Proceedings of Second International WWW Conference: Mosaic and the Web, Jul. 1994, 10 pages.*

Vinod Anupam et al., SHASTRA—An architecture for Development of Collaborative Applications, Apr. 1993, IEEE, pp. 155-166.*

Paul Tarau et al., LogiMOO: an Extensible Multi-User Virtual World with Natureal Language Control, The Journal of Logic Programming, 1993, vol. 12, pp. 1-23.*

"Microsoft NetMeeting Conferencing Spftware Provides Easy Voice, Dad Internet Communications; Available on the Web Now", May 29, 1996, http://www.microsoft.com/presspass/press/1996/may96/INCONFPR.asp.

"Mechanisms for Specifying and Describing the Format of Internet Message Bodies", Nathaniel Borenstein, Ned Freed, Jun. 1991, pp. 1-40.

"Network Security via Private-Key Certificates", Don Davis and Ralph Swick, pp. 1-4, Oct. 1990.

"Discuss in Section 9", Athena Zepher and Kerberos, 1988, pp. 1-11.

"www.cs.columbia.edu/~hgs/rpt/" complete printout of website, compiled Feb. 3, 2002.

"History of IRC", Daniel Stenberg , Version: 0.7—Jan. 8, 2002.

"Index of /pub/academic/communications/logs/Gulf-War/", www.ibiblio.org/pub/academic/communicaations/logs/Gulf-War/desert-storm/01, retrieved May 2, 2002.

"Join a Dungeon Adventure", Daniel James, Nov. 30, 2001, www.techtv.com/screensavers/supergeek/story/0,24330,3012300,00.html.

"Google Search Results for MUDs", Google.com, http://directory.google.com/Top/Games/Internet/MUDs/, retreived May 5, 2002.

"A Brief History of SOF", http://sofeq.sofguild.com/history.htm, Jun. 1998.

"Adventures On-Line", Michael Ciraolo, www.atarimagazines.com/v2n7/online.html, Antic vol. 3, No. 7, Nov. 1984.

"Host Extensions for IP Multicasting," S. Deering, Stanford University, Aug. 1989, 16 Pages.

"Complaint: Brian Hollander vs. Peter K. Trzyna and PTK Technologies, LLC," Dated Nov. 13, 2007, pp. 1-18.

Winder, Patrice L., "Notice of Allowance" mailed Mar. 21, 2013, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006. pp. 1-26. USA.

Trzyna, Peter K., "Amendment After Allowance" filed Mar. 22, 2013, for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006. pp. 1-22. USA.

Winder, Patrice L., "Office Action-Final Rejection" mailed Jan. 10, 2013, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006. pp. 1-37. USA.

Trzyna, Peter K., "Amendment After Final and Response" filed Sep. 6, 2012, for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006. pp. 1-30. USA.

Winder, Patrice L., "Notice of Allowance" mailed Apr. 5, 2013, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006. pp. 1-23. USA.

Trzyna, Peter K., "Amendment After Allowance" filed Apr. 5, 2013, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006. pp. 1-18. USA.

Trzyna, Peter K., "Supplemental Amendment and Response After Final" filed Mar. 12, 2013, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006. pp. 1-18. USA.

Prakash, Atul et al. "Distview: Support for Building Efficient Collaborative Applications using Replicated Objects." Software Systems Research Laboratory, Department of Electrical Engineering and Computer Science, University of Michigan. pp. 1-12. Ann Arbor, MI.

Anupam, Vinod "Collaborative Multimedia Environments for Problem Solving." A Thesis Submitted to Purdue University. (Aug. 1994), pp. 1-212, Ann Arbor, MI.

Bajaj, Chandrajit et al. "Collaborative Multimedia in Shastra." 3rd International Conference on Multimedia, San Francisco, CA (1995). pp. 365-366.

Ahuja, S.R. et al. "The Rapport Multimedia Conferencing System." AT&T Bell Laboratories. pp. 1-8. Holmdel, NJ.

Anupam, Vinod et al. "Collaborative Multimedia in Scientific Design." Proceedings: First ACM Multimedia Conference, ACM Multimedia 93, Anaheim, California, ACM Press, (1993). pp. 447-456.

Anupam, Vinod et al. "Shastra—An Architecture for Development of Collaborative Applications." Proceedings: Second IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Morgantown, (1993). pp. 155-166.

Bajaj, Chandrajit et al. "Brokered Collaborative Infrastructure for CSCW." Proceedings: Fourth IEEE Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, Berkeley Springs, West Virginia, IEEE Computer Society Press, (1995), pp. 207-213.

Anupam, Vinod et al. "Shastra: Multimedia Collaborative Design Environment." IEEE Multimedia, 1, 2, (1994), pp. 39-49.

Anupam, Vinod et al. "Distributed and Collaborative Visualization." IEEE Computer, 27, 7, (Jul. 1994), pp. 37-43.

Bajaj, Chandrajit et al. "Web based Collaborative Visualization of Distributed and Parallel Simulation." In Proceedings of the 1999 IEEE Symposium on Parallel Visualization and Graphics, (Oct. 24-29, 1999), San Francisco, CA, pp. 47-54.

Bajaj, Chandrajit et al. "NLS: Collaborative Virtual Environment to Promote Shared Awareness." Proceedings: Workshop on New Paradigms in Information Visualization and Manipulation NPIV'96, In conjunction with Fifth ACM International Conference on Information and Knowledge Management (CIKM'96), (1996), pp. 41-45.

Bajaj, Chandrajit et al. "Web Based Collaboration-Aware Synthetic Environments" Proceedings of the 1997 GVU/NIST TEAMCAD workshop, Atlanta, GA, 1997, 143-150.

## (56) References Cited

OTHER PUBLICATIONS

Trzyna, Peter K., "Amendment After Final and Request for Reconsideration" filed Jan. 16, 2013, for U.S. Appl. No. 11/836,633, filed Aug. 9, 2007. pp. 1-14. USA.

Trzyna, Peter K., "Amendment and Request for Reconsideration" filed Jul. 16, 2012 , for U.S. Appl. No. 11/510,351, filed Aug. 24, 2006. pp. 1-32. USA.

T. Socolofsky et al., Request for Comments (RFC) 1180: A TCP/IP Tutorial, Network Working Group, Jan. 1991, pp. 1-29.

J. Oikarinen et al., Request for Comments (RFC) 1459: Internet Relay Chat Protocol, Network Working Group, May 1993, pp. 1-66.

Andreas Dieberger, Providing Spatial Navigation for the World Wide Web, Spatial Information theory a Theoretical Baisi for GIS, Lecture Notes in Computer Science, vol. 988, 1995, pp. 93-106.

Lee Newberg et al., Integrating the World-Wide Web and Multi-User Domains to Support Advanced Network-Based Learning Experiments, Conference Proceedings of ED-MEDIA 1995, pp. 494-499.

T Y Hou et al., An active multimedia System for Delayed Conferencing, Proceedings of the SPIE Conference on High-Speed Networking and Multimedia Computing, San Jose CA, 1994, pp. 97-104.

Roy Rada and Claude Ghaoui. "Medical Multumedia" Intellect Ltd. Great Britain (1995) Suite 2, 108/110 London Road, Oxford OX3 9AW.

"CCCP: Conference Control Channel Protocol a Scalable Base for Building Conference Control Applications," Mark Handley et al., V1.4 pp. 1-18, Aug. 28-Sep. 1, 1995.

"CCCP: Conference Control Channel Protocol a Scalable Base for Building Conference Control Applications," Mark Handley et al., pp. 1-13, Aug. 28-Sep. 1, 1995.

"An Application Legel Video Gateway," Elan Amir et al., pp. 1-10, Aug. 28-Sep. 1, 1995.

"Vic: A Flexible Framework for Packet Video," Steven McCanne, et al. pp. 1-12. Aug. 28-Sep. 1, 1995.

"Argo: A System for Distributed Collaboration," Hania Gajewska, et al., 8 pages, ACM Multimedia 1994.

"Scalable Feedback Control for Multicast Wideo Distribution in the Internet," Jean-Chrysostome Bolot, et al., 10 Pages, Proceedings of SIGCOMM '94, ACM.

"Argohalls: Adding Support for Group Awareness to the Argo Telecollaboration System," Hania Gajewska, et al., 2 Pages, Nov. 13-17, 1995.

"PSSST: Side Conversations in the Argo Telecollaboration System," Lance Berc, et al. 2 Pages. Nov. 14-17, 1995.

"A World-Wide Web User Interface for an Electronic Meeting Tool," Michael J. Rees and Tak K. Woo, Howard & Lueng, Nov. 28-Dec. 1, 1994, pp. 187-192.

Rules for IRC networking—Ratified Jul. 6, 1994; Edited Jun. 29 by #EU-Opers.

IRC—Internet Relay Chat, doc/MANUAL; Copyright 1990, Karl Kleinpaste.

Undemet IRC FAQ (Part I).(updated Jul. 28, 1995)—Weekly Report.

Undemet IRC FAQ (Part II) (updated Jul. 28, 1995)—Weekly Report.

A short IRC primer; Edition 1.1b, Feb. 28, 1993.

Internet Relay Chat Protocol; J. Oikarinen, D. Reed; May 1993.

Electropolis: Communication and Community on Internet Relay Chat; Elizabeth M. Reid 1991.

CU-SeeMe, Updated: Thursday Dec. 21, 1995.

Real Time Groupware on the Information Highway, Saul Greenberg, Deparrment of Computer Science, University of Calgary, Alberta Canada (1994).

Real Time Groupware as a Distributed System: Concurrently Control and Its Effect on the the Interface, Saul Greenberg and David Marwood, Department of Computer Science, University of Calgary, Alberta Canada (1994).

A Groupware Environment for Complete Meetings, Ted O'Grady and Saul Greenberg, The University of Calgary, Alberta Canada (1992).

Group Kit a Groupware Toolkit for Building Real-Time Conferencing Applications, Mark Roseman and Saul Greenberg, Department of Computer Science, University of Calgary, Alberta Canada, CSCW 92 Proceedings (1992).

Issues and Experiences Designing and Implementing Two Group Drawing Tools. Saul Greenberg, Mark Roseman, David Webster and Ralph Bohnet , Department of Computer Science, University of Calgary, Alberta Canada (1992).

Liveware: A New Approach to Sharing Data in Social Networks, Ian H. Witten, Computer Science, University of Calgary, Canada, Harold W. Thimbleby, Computing Science, Stirling University, Stiring, Scotland, UK, George Coulouris, Queen Mary and Westfield Collete, London, Saul Greenberg. Computer Science, University of Calgary, Calgary, Canada (Received May 1, 1990 and accepted in revised form Aug. 1, 1990).

Groupsketch: A Mult-User Sketchpad for Geographically-Distributed Small Groups, Saul Greenberg, Department of Computer Science, University of Calgary, Alberta Canada, Ralph Bohnet, MPR TelTech Ltd., Burnaby, Canada, CSCW (1991(b)).

The World Wide Web Unleashed, John December and Neil Randall, SAMS Publishing, Indianapolis, IN, (1994).

Plato: The Emergence of On-Line Community, Copyright 1994 by David R. Woolley. Matrix News, vol. 4, No. 1, (1994).

Gtalk Owners Manual, David W. Jeske (1995).

Muds Grow Up: Social Virtual Reality in the Real World; Pavel Curtis and David A. Nichols, Xerox Parc (1993).

Collaborative Networked Communication: MUDS as Systems Tools, Remy Evard, 1993 Lisa, Nov. 1-5, 1993.

Proceedings of the Seventh Systems Administration Conference (USA VII), Monterey. CA, USENIX Association, (1993) (One Page).

The History of NWN, Neverwinter Nights Archive (1991-1997), netgamesn™ Your Guide to the Games People Play on the Electronic Highway, A Michael Wolff Book, Kelly Maloni, Derek Baker and Nathaniel Wice.

Baudy Tales From The Cyburbs: A Guide to On-Line Games, (includes related articles on UseNet Message Groups and Suggested reading (Evaluation) (Software Review), Full Text: Copyright 1994 zdnet, Computer Gaming World, v 123 (1994).

AMS: Area Message Service for SLC, M. Crane, R. Mackenzie, D. Millsom, M. Zelazny, Stamford Linear Accelerator Center, Stanford University, Stanford, CA, PAC (1993).

An Experimental Multi-Media Bridging System, E.J. Addeo, A.B. Dayao, A.D. Gelman, V.F. Massa, Bell Communications Research, Morristown, NJ, ACM (1988).

Quilt: A Collaborative Tool for Cooperative Writing, Robert S. Fish, Robert E. Kraut, Mary D. P. Leland, Bell Communications Research, Michael Cohen, University of Washington, ACM (1988).

RFC 1459 Internet Relay Chat Protocal, J. Oikarinen, D. Reed (1993).

Groupware for Real-Time Drawing—A Designer's Guide, Saul Greenberg, Stephen Hayne, Roy Rada, McGraw-Hill Book Company, Berkshire, England (1995).

Collaborative Document Production Using Quilt, Mary D.P. Leland, Robert S. Fish and Robert E. Kraut, Bell Communications Research, Inc, Morristown, NJ ACM (1988).

The Rapport Multimedia Conferencing System, S.R. Ahuja, J. Robert Ensor and David N. Horn, AT&T Bell Laboratories, Holmdel, NJ, ACM (1988).

Software Architecture for Integration of Video Services in the Etherphone System, P. Venkat Rangan, Member, IEEE, and Daniel C. Swinehart, Member, IEEE (1991).

Multimedia Conferencing in the Etherphone Environment, Herrick V. Vin, Polle T. Zellweger, Daniel C. Swinehart, and P. Venkat Rangan, Xerox Palo Alto Research Center, (1991).

Tools for Supporting the Collaborative Process, James R. Rhyne, Catherine G. Wolf, IBM Thomas J. Watson Research Center, Yorktown Heights, NY, UIST (1992).

System Support for Computer Multimedia Collaborations, Harrick M. Vin, P. Venkrat Rangan, University of California at San Diego, LaJolla, CA, Mon-Song Chen, IBM T. J. Watson Research Center, Yorktown Heights, NY, CSCW 92 Proceedings (1992).

(56) **References Cited**

OTHER PUBLICATIONS

Collaboration in KMS, A Shared Hypermedia System, Elise Yoder, Robert Aksyn, Donald McCracken, Knowledge Systems Incorporated, Murrysville, PA, ACM (1989).

The Rendezvousd Architecture and Language for Constructing Multiuser Applications, Ralph D. Hill, Tom Brinck, Steven Rohall, John F. Patterson and Wayne Wilner, ACM Transactions on Computer-Human Interaction, vol. 1, No. 2 (1994).

Collaboration Support Provisions in Augment, Douglas C. Engelbart, Tymshare, Inc. (1983).

Building Real-Time Groupware With Groupkit, A Groupware Toolkit, Mark Roseman and Saul Greenberg, University of Calgary, ACM Transactions on Computer-Human Interaction, vol. 3, No. 1, (1996).

Architecture for a Multimedia Teleconferencing System, L. Aguilar, J.J. Garcia-Luna-Aceves, D. Moran, E.J. Craighill, R. Brungardt, Information Services and Technology Center, SSRI International, Menlo Park, CA, ACM (1986).

Special Issue on CSCW: Part 1, Human and Technical Factors of Distributed Group Drawing Tools, Saul Greenberg, Mark Roseman, Dave Webster and Ralph Bohnet, Interacting With Computers, vol. 4, No. 3 (1992).

Design of a Multi-Media Vehicale for Social Browsing, Robert W. Root, Bell Communications Research, NJ, ACM (1988).

Supporting Collaborative Writing of Hyperdocuments in Sepia, Jorg M. Haake and Brian Wilson, GMD-IPSI, Federal Republic of Germany. CSCW 92 Proceedings (1992).

Filling Html Forms Simultaneously: Coweb-Architecture and Functionality, Stephen Jacobs, Michael Gebhardt, Stefanie Kethers, Wojtek Rzasa, RWTH Aachen, Informatik V, Fifth International World Wide Web Conference, Paris, France (May 1996).

Webchat 0.2 Source Distribution, e-mail from Michael Fremont, Internet Roundtable Society, dated Feb. 10, 1995.

Supporting Development of Synchronous Collaboration Tools on the Web With Groco, Michael Walther, Proceedings of the ERCIM workshop on CSCW and the Web, Sankt Augustin, Germany (Feb. 7-9, 1996).

The University of Calgary, Design of Real-Time Groupware Toolkit, Mark Roseman, A Thesis Submitted to the Faculty of Graduate Studies in Partial Fulfillment of the Requirements for the Degree of Master of Science, Department of Computer Science, Calgary, Alberta (Feb. 1993).

Session Management for Collaborative Applications, W. Keith Edwards, Graphics, Visualization & Usability Center College of Computing, Georgia Institute of Technology, GA, Association for Computer Machinery, Published in Proceedings of the ACM Conference on Computer-/supported Work (CSCW '94).

Social Activity Indicators: Interface Components for CSCW Systems, Mark S. Ackerman, Brian Starr, Department of Information and Computer Science, University of California, Irvine, UIST (No. 14-17 (1995).

Social Activity Indicators: Interface Components for CSCW Systems, Symposium on User Interface Software and Technology, Proceedings of the 8$^{th}$ Annual ACM Symposium on User Interface and Software Technology, Pittsburgh, PA (1995).

Distview: Support for Building Efficient Collaborative Applications Using Replicated Objects, Atul Prakash and Hyong Sop Shim, Software Systems Research Laboratory, Department of Electrical Engineering and Computer Science, University of Michigan, MI ACM (1994).

Gtalk Source License Agreement, David W. Jeske, Jun. 2, 1998).

Englebart Douglas C.: "Authorship Provisions in AUGMENT" COMPCON '84 Digest Proceedings of the COMPCON Conference, San Francisco, CA, Feb. 27-Mar. 1, 1984, pp. 465-472.

Englebart, Douglas C.: "Toward High-Performance Knowledge Workers," OAC '82 Digest. Proceedings of the AFIPS Office Automation Conference, San Francisco, CA, Apr. 5-7, 1982, pp. 279-290.

Lee, Andrew: "Anonymous collaboration: An alternative technique for working together" ACM SIGCHI Bulletin vol. 26 ,Issue 3, Jul. 1994, pp. 40-46.

Abdel-Wahab, Hussein: "Reliable Information Service for Internet Computer Conferencing" Proceedings . Second Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises, IEEE Comput. Soc. Press, 1993, pp. 128-142.

French, Robert S et al: "The Zephyr Programmer's Manual" Protocol Version ZEPH0.2, Apr. 5, 1989.

Fermann, Carla J.:"Distributed consulting in a distributed environment" New Centerings in Computing Services, Proceedings of the 18th annual ACM SIGUCCS conference on User services Cincinnati, Ohio, United States . 1990 pp. 117-120.

Cohen, Abbe: "Inessential Zephyr" The Student Information Processing Board, Aug. 23. 1993.

French, Robert /mit/zephyr/repository/zephyr/clients/zaway/zaway.c, v S; Copyright (c) 1987, 1993 by the Massachusetts Institute of Technology.

Sunkavally, N et al: "Using MIT's Athena Computing System" The Tech, vol. 119, No. 39, Thursday, Sep. 2, 1999.

Tony Della Fera et al.: "Zephyr—Sephyr Notification Service" MIT Project Athena (Jul. 1, 1988) Zephyr Notification Service.

Horus: A Flexible Group Communications System, Robbed van Renesse. Kenneth P. Birman. and Silvano Maffeis, Communications of the ACN, Apr. 1996, vol. 39. No. 4.

French Robert S.: "Zaway—tell other people via Zephyr that you aren't around" MIT Project Athena, Jul. 1, 1988.

Kurlander, David et al: "Comic Chat" Proceedings of SIGGRAPH'96 (New Orleans, Aug. 1996), Computer Graphics Proceedings, Annual Conference Series, pp. 225-236, New York. 1996. ACM SIGGRAPH.

Maes, P: "Artificial Life meets Entertainment: Interacting with Lifelike Autonomous Agents", In: Special Issue on New Horizons of Commercial and Industrial Al 38, 11 (1995) 108-114. Communications of the ACM, ACM Press.

Walker, Janet H. et al: "Using a Human Face in an Interface", ACM Human Factors in Computing Systems. Apr. 24-28, 1994 pp. 85-91.

"Visual Dialog Showing Speech Interaction with an Intelligent Agent" IBM Technical Disclosure Bulletine, vol. 39, No. 1, Jan. 1996, pp. 237-239.

An Intelligent Network Service Prototype Using Knowledge Processing. Int. Conf. on Tools for Al (1991).

Julia's Home Page, Julie. a Chatterbot (Dec. 19, 1994).

Chatterbots, Tinymuds. and the Turing Test, Entering the Loebner Price Competition (Jan. 24, 1994).

Entertaining Agents: Julia (1993).

What is an Agent, Anyway? A Sociological Case Study, Leonard N. Foner, (May 1993).

Social Activity Indicators: Interface Components for CSCW Systems. Mark S. Ackerman and Brian Starr, Dept. of Info. and Computer Science, Univ. of California, Irvine (Nov. 14-17, 1995) UIST '95.

Software Secretaries: Learning and Negotiating Personal Assistants for the Daily Office Work, Siegfried Bocionek, Siemens AG, Munich. Germany (1994 IEEE).

MUDs in Education: New Environments, New Pedagogies. Tari Lin Fanderclai, Computer—Mediated Communication Magazine, vol. 2, No. 1, Jan. 1, 1995.

The Evolution of Intercat-Scale Event Notification Services: Past, Present and Future, Adam Rifkin and Rohit Khare, Aug. 10, 1998.

The Zephyr Help Assistance: Promoting Ongoing Activity in a CSCW System; Mark Ackerman and Leysia Palen. Department of Information and Computer Science, University of Calioromia, Irvine (to appear in the Proceedings of the ACM Conference on Human Factors in Computing Systems (CHI '96)).

The Zephyr Notification Service, C. Anthony DellaFera et al., Digital Equipment Corp., Project Athena, Massachusetts Institute of Technology, Cambridge, MA, 1996.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Complaint" filed Jun. 24, 2004.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Notice of Claim Involving a Patent" filed Jun. 24, 2004.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "First Amended Answer to the Complaint, and Counterclaim of Defendant America Online. Inc." filed Sep. 14, 2004.

(56) **References Cited**

OTHER PUBLICATIONS

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Plaintiff's Reply to the First Amended Counterclaim of Defendant America Online, Inc." filed Sep. 28, 2004.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "AOL's Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4)" dated Apr. 29, 2005.

"Internet hasn't focused on good photography as much as it could" Article, The Dallas Morning News, Sep. 1995 (AOL-B 0001478).

"Group dynamics add fun to guided online tours" Article, USA Today, Oct. 1995 (AOL-B 0001479).

"People with addictions band together for support on line", Article, Jun. 1995 (AOL-B 0001480).

"Netscape Communications Introduces Netscape Internet Applications Family for Electronic Commerce" Netscape Company Press Relations, Mar. 1995 (AOL-B 0005712-0005713).

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Expert Report of Bruce M. Maggs" dated Aug. 5, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Supplemental Rebuttal Expert of Bruce M. Maggs Regarding Invalidity of U.S. Patent 5,956,491" dated Sep. 26, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, Rebuttal Expert Report of Bruce M. Maggs Regarding Invalidity of U.S. Patent 5,956,491 dated Aug. 28, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, AOL's Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4) dated Apr. 29, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, AOL's Second Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4) dated May 20, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, AOL's Third Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4) dated Aug. 11, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, AOL's Fourth Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4) dated Sep. 20, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, AOL's Fifth Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4) dated Sep. 27, 2005.

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "Declaration of Mr. David W. Jeske" dated Jun. 6, 2005.

"Netscape adds tools," Responsive Database Services, Inc., Press Release Mar. 1995 (Aol 1206861-1206862).

"Netscape communications introduces Netscape interne applications family for electronic commerce," PR Newswire Association Inc. Press Release, Mar. 1995 (AOL 1206863-1206864).

Full Scale Commerce With Netscape, Business Communications Co., Press Release, Apr. 1995 (AOL 1206865-1206866).

"Netscape spins Web extensions; adds firewall, Usenet servers, electronic shopping software Netscape Communications Proxy Server, Isore, Merchant System, Publishing System, Community System," Information Access Company, Apr. 1995 (AOL 1206867-1206868).

"Netscape offers bookmark, chat services on Web," InfoWorld Media Group, Aug. 1995 (AOL 1206869).

"Netscape for Windows 95 Announced," Newsweek Business Information, Inc., Aug. 1995 (AOL 1206870-1206873).

"Netscape introduces Netscape Smartmarks and Netscape Chat; Applications Bring New Navigation and Communications Capabilities to Users of Netscape Navigator for Windows," Netscape Chat Help Contents (AOL 613173-613243).

*Windy City Innovations, LLC* v. *America Online, Inc.*, Civil Action No. 04 C 4240, "AOL's Second Supplemental Response to Plaintiff Windy City Innovations, LLC's First Set of Interrogatories (No. 4)" dated Mat 20, 2005.

Netscape, "Netscape Power Pack Bookmarks, Chat, and Multimedia Add-Ons". (AOL 613167-613172).

Netscape, "Netscape Announces Add-On Product Suite for Popular Netscape Navigator Software, Netscape Power Pack Includes Netscape SmartMarks, Netscape Chat and Multimedia Add-On Applications From Adobe, Apple, and Progressive Networks" Press Release, May 11, 2005, pp. 1-3. (AOL 613244-613246).

PR Newswire Assoc., Inc. "Netscape Announces Add-On Product Suite for Popular Netscape Navigator Software" Article, Oct. 25, 1999, pp. 1-2. (AOL 613247-613248).

Netscape, "Netscape Chat Help Contents" Manual. (AOL 613173-613243).

Wired Channeling "Tips for Foiling the NSA" Article, Jan. 1996, p. 174. (AOL 469104-469105).

Flash News "Market Support News, Jacksonville Update" Article, May 19, 1995, pp. 1-4, (AOL 469106-469109).

Palfreyman, et al., "A Protocol for User Awareness on the World Wide Web", Article, 1996, pp. 130-139. (AOL 469110-469119).

Robinett, "Interactivity and Individual Viewpoint in Shared Virtual Worlds: The Big Screen vs. Networked Personal Displays", Article, Computer Graphics, vol. 28, No. 2, May 1994, pp. 127-130. (AOL 074871-074974).

Ohya, et al., "Real-Time Reproduction of 3D Human Images in Virtual Space Teleconferencing", Article, pp. 408-414. (AOL 074875-074881).

Fukuda, et al., "Hypermedia Personal Computer Communication System: Fujitsu Habitat", Fujitsu Sci. Tech. J. Oct. 1990, vol. 26, No. 3, pp. 197-206. (AOL 074882-074893).

Carlsson, "DIVE—a Multi-User Virtual Reality System", Article, IEEE 1993, pp. 394-400. (AOL 074894-074900).

Benford, et al., "Supporting Cooperative Work in Virtual Environments", The Computer Journal, vol. 37, No. 8, 1994, pp. 653-668. (AOL 074901-074916).

Berlage, et al., "A Framework for Shared Applications With a Replicated Architecture", Article, Nov. 3-5, 1993, pp. 249-257. (AOL 075027-075035).

Sohlenkamp, "A Virtual Office Environment Supporting Shared Applications", Article, Feb. 7-11, 1994. (AOL 075036-075044).

Handley, et al., "The Conference Control Channel Protocol (CCCP): A Scalable Base for Building Conference Control Applications", Article, 1995, pp. 275-287. (AOL 075145-075157).

Sasse, et al., "Remote Seminars through Multimedia Conferencing: Experiences from the MICE Project", Article, Proc. INET '94/ JENC5, pp. 1-8. (AOL 075158-075165).

Kirstein, et al., "Piloting of Multimedia Integrated Communications for European Researchers (MICE)", Article, Proc. INET '93, pp. 1-12. (AOL 075197-075208).

Kirstein, et al., "Recent Activities in the MICE Conferencing Project", Article, Proc. INET '95. (AOL 075209-075218).

Sasse, et al., "Remote Seminars through Multimedia Conferencing: Experiences form the MICE Project", Article, Proc. INET '94/ JENC5. (AOL 075249-075260).

Byte, "Network and Windows 95 Take Top BYTE Awards", Article, Jul. 1995. (AOL 055731-055732).

CompuServe, "CompuServe Producer User Guide", Article, Apr. 19, 1995, pp. 1-36. (AOL 055743-055779).

Mawby, "Designing Collaborative Writing Tools", Article, 1991, pp. 1-191. (AOL 074678-074870).

Donath, "the Illustrated Conversation", Article, 1995, pp. 79-88. (AOL 052115-052124).

Donath, "Sociable Information Spaces", Article, Jun. 20-22, 1995, pp. 269-273. (AOL 052127-052131).

Masinter, "Collaborative Information Retrieval: Gonner from MOO", Article, Proc. INET '93 (AOL 052153-052161).

Roseman, et al., "TeamRooms: Groupware for Shared Electronic Spaces", Article. (AOL 052162-052163).

Curtis, Mudding Social Phenomena in Text-Based Virtual Realities, Article, Mar. 3, 1992, pp. 1-21. (AOL 052181-052201).

(56) **References Cited**

OTHER PUBLICATIONS

Nichols, et al., "High-Latency, Low-Bandwidth Windowing in the Jupiter Collaboration System", Article, UIST '95, Nov. 14-17, 1995, pp. 111-120. (AOL 052202-052211).

Curtis, et al., "The Jupiter Audio/Video Architecture: Secure Multimedia in Network Places", Article, 1995, pp. 1-12. (AOL 052212-052223).

Lee, "Xsketch: A Multi-User Sketching Tool for X11", Article, 1990, pp. 169-173. (AOL 052251-052255).

Patterson, et al., "Rendezvous: An Architecture for Synchronous Multi-User Applications", Article, Oct. 1990, pp. 317-328. (AOL 052272-052283).

Patterson, "Comparing the Programming Demands of Single-User and Multi-User Applications", Article, UIST'91, Nov. 11-13, 1991, pp. 87-94. (AOL 052284-052291).

Lu, et al., "Idea Management in a Shared Drawing Tool", Article, ECSCW 1991, pp. 97-112. (AOL 052292-052307).

Lu, "Supporting Idea Management in a Shared Drawing Tool", Article, 1992, pp. 29-113. (AOL 052308-052364).

Wexelblat, "Building Collaborative Interfaces", Article, May 1991, pp. 1-40. (AOL 052385-052405).

Watabe, et al., "Distributed Desktop Conferencing System with Multiuser Multimedia Interface", Article, 1991 IEEE, pp. 531-539. (AOL 052406-052414).

Watabe, et al., "Distributed Multiparty Desktop Conferencing System: MERMAID", Article, Oct. 1990, pp. 27-38. (AOL 052415-052426).

Horn, et al., "An ISDN Multimedia Conference Bridge", Article, 1990 IEEE, pp. 853-856. (AOL 052427-052430).

Ahuja, et al., "Coordination and Control of Multimedia Conferencing", Communications Magazine, IEEE, May 1992, vol. 30, Iss. 5, pp. 38-43. (AOL 052431-052436).

Ensor, et al., "The Rapport Multimedia Conferencing System—A Software Overview", Article, Proc. $2^{nd}$ IEEE, Mar. 1998, pp. 52-58. (AOL 052437-052443).

Greenberg, "Personalizable Groupware: Accomodating Individual Roles and Group Differences", Article, ECSCW 1991, pp. 17-32. (AOL 052444-052459).

Greenberg, "Sharing Views and Interactions With Single-User Applications", Article, Apr. 1990, pp. 227-237. (AOL 052460-052470).

Sarin, et al., "Software for Interactive On-Line Conferences", Article, 1984, pp. 46-58. (AOL 052471-052484).

Bly, et al., "Media Spaces: Bringing People Together in a Video, Audio, and Computing Environment", Article, Jan. 1993, vol. 36, No. 1, pp. 28-47. (AOL 052486-052505).

NCSA, "The Second International WWW Conference '94 Mosaic and the Web", Jul. 14, 1994. (AOL 052506-052509).

Frega, et al., "A Multimedia Bulletin Board in WWW Environment", Article. (AOL 052567-052574).

Horn, et al., "An ISDN Multimedia Conference Bridge", Article, IEEE Region 10, Sep. 1990, pp. 853-856. (AOL 052575-052578).

Tang, et al., "Montage: Providing Teleproximity for Distributed Groups", Article, Apr. 24-28, 1994, pp. 37-43. (AOL 052579-052585).

Pearl, "System Support for Integrated Desktop Video Conferencing", Article, Dec. 1992, pp. 1-14. (AOL 052586-0522600).

Chang, et al., "Group Coordination in Participant Systems", Article, May 1990, pp. 589-599. (AOL 052601-052611).

Ensor, et al., "User Interfaces for Multiparty Communications", Article, 1993 IEEE, pp. 1165-1171. (AOL 052612-052618).

Tang, et al., "Supporting Distributed Groups with a Montage of Lightweight Interactions", Article, 1994, pp. 23-34. (AOL 052619-052630).

Brinck, et al., "A Collaborative Medium for the Support of Conversational Props", Article, Nov. 1992, pp. 171-178. (AOL 052636-052643).

Graham, et al., "Relational Views as a Model for Automatic Distributed Implementation of Multi-User Applications", Article, Nov. 1992, pp. 59-66. (AOL 052644-052651).

Rein, et al., "rIBIS: A Real-Time Group Hypertext System", Article, 1991, pp. 349-367. (AOL 052652-052670).

Gibbs, "LIZA: An Extensible Groupware Toolkit", Article, 1989, pp. 29-35. (AOL 052671-052677).

Clark, "Multipoint Multimedia Conferencing", Article, May 1992 IEEE, pp. 44-50. (AOL 052678-052684).

Hill, et al., "The Rendezvous Language and Architecture", Article, Jan. 1993, vol. 36, No. 1, pp. 81-125. (AOL 052697-052702).

Hill, et al., "The Rendezvous Architecture and Language for Constructing Multiuser Applications", ACM Transactions on Computer-Human Interaction, Jun. 1994, vol. 1, No. 2, pp. 81-125. (AOL 052703-052747).

"Office Action," dated Mar. 18, 2008, for U.S. Appl. No. 11/510,351.

"Amendment and Response," filed in U.S. Appl. No. 11/510,351 on Sep. 18, 2008.

"Preliminary Amendment," for U.S. Appl. No. 11/510,351, filed Nov. 30, 2007.

"Response to Notice of Non-Responsive reply and Supplemental Amendment and Response," for U.S. Appl. No. 11/510,351, filed Feb. 6, 2009.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,351, mailed Jul. 22, 2009. pp. 1-14.

"Amendment and Response" for U.S. Appl. No. 11/510,351, filed Jan. 19, 2010. pp. 1-18.

"Preliminary Amendment," for U.S. Appl. No. 11/510,463, filed Nov. 30, 2007. pp. 1-12.

"Second Preliminary Amendment," for U.S. Appl. No. 11/510,473, filed Nov. 30, 2007. pp. 1-21.

"Preliminary Amendment," for U.S. Appl. No. 11/836,633, filed Nov. 30, 2007. pp. 1-3.

Office Action—Non-Final Rejection for U.S. Appl. No. 11/510,473, mailed on Oct. 5, 2009. pp. 1-49.

Tim Meyer et al., A MOO-Based Collaboration Hypermedia System for WWW, Proceedings for Second International Conference for WWW, Oct. 1994.

Paul Kindberg et al., Mushroom: a framework for collaboration and interaction across the Internet, In the Proceedings of ERCIM Workshop on CSCW and the Web, Feb. 1996, 11 pages.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,463, mailed on Sep. 22, 2009. pp. 1-27.

Pavel Curtis et al., MUDS Grow Up: Social Virtual Reality in the Real World, Xerox PARC, Jan. 1993, 6 pages.

"Amendment and Response," for U.S. Appl. No. 11/510,473, filed Feb. 5, 2010. pp. 1-26.

"Amendment and Response," for U.S. Appl. No. 11/510,463, filed Mar. 22, 2010. pp. 1-16.

"Corrected Amendment and Response," for U.S. Appl. No. 11/510,463, filed Apr. 1, 2010. pp. 1-16.

"Third Preliminary Amendment," for U.S. Appl. No. 11/836,633, filed May 7, 2010. pp. 1-8.

"Preliminary Amendment," for U.S. Appl. No. 11/836,633, filed Apr. 14, 2010. pp. 1-8.

"Office Action-Non-Final Rejection" for U.S. Appl. No. 11/510,473, mailed May 12, 2010, pp. 1-14.

Atul Prakash et al., DistView for Building Efficient Collaborative Applications using Replicated Objects, Proceedings of the 1994 ACM conference on Computer supported cooperative work, pp. 153-164.

Bentley et al., Supporting collaborative information sharing with the World Wide Web: The BSCW shared workspace system, Proceedings of the 4th International World Wide Web Conference, Dec. 1995, 12 pages.

K.J. Maly et al., Mosaic + XTV = CoReview, Computer Networks and ISDN Systems, vol. 27 Issue 6, Apr. 1995, pp. 849-860, Proceedings of the Thrid International World Wide Web Conference.

"Preliminary Amendment" filed on Nov. 30, 2007, in U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Response to Notice of Non-Responsive reply and Supplemental Amendment and Response" filed on Feb. 6, 2009, in U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Jul. 22, 2009, in U.S. Appl. No. 11/510,351, filed Aug. 24, 2006, by inventor Daniel L. Marks.

(56) **References Cited**

OTHER PUBLICATIONS

"Amendment and Response" filed on Jan. 19, 2010, in U.S. Appl. No. 11/510,351. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Mar. 18, 2008, in U.S. Appl. No. 11/510,351. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Sep. 18, 2008, in U.S. Appl. No. 11/510,351. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Feb. 5, 2010, for U.S. Appl. No. 11/510,473. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/510,473. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Oct. 5. 2009, for U.S. Appl. No. 11/510,473. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Final Rejection" mailed on May 12, 2010. for U.S. Appl. No. 11/510,473, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment After Final" filed on Jun. 11, 2010, for U.S. Appl. No. 11/510,473. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, in U.S. Appl. No. 11/510,463. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action" mailed on Sep. 22, 2009, in U.S. Appl. No. 11/510,463. filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Corrected Amendment and Response" filed on Apr. 1, 2010, in U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Amendment and Response" filed on Mar. 22, 2010, in U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Office Action-Final Rejection" mailed on Jun. 28, 2010, for U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Nov. 30, 2007, for U.S. Appl. No. 11/836,633. filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Preliminary Amendment" filed on Apr. 14, 2010, for U.S. Appl. No. 11/836,633. filed Aug. 9, 2007, by inventor Daniel L. Marks.

"Third Preliminary Amendment" filed on May 7, 2010, for U.S. Appl. No. 11/836,633, filed Aug. 9. 2007, by inventor Daniel L. Marks.

"Fourth Preliminary Amendment" filed on May 25, 2010, for U.S. Appl. No. 11/836.633. filed Aug. 9, 2007. by inventor Daniel L. Marks.

"Amendment and Response" filed on Jul. 23, 2010, in U.S. Appl. No. 11/510,463, filed Aug. 24, 2006, by inventor Daniel L. Marks.

Kankanahalli Srinivas et al., MONET: A Multi-media System for Conferencing and Application Sharing in Distributed Systems, Feb. 1992, CERC Techinical Report Series Research Note. 19 pages.

Vinod Anupam and Chandrajit L. Bajai. Shastra: Multimedia Collaborative Design Environment. IEEE Multimedia. Summer; 1994. pp. 39-49. Purdue University.

Vinod Anupam and Chandrajit L. Bajai. Collaborative Multimedia Scientific Design in SHASTRA. pp. 1-12. Department of Computer Sciences, Purdue University, West Lafayette, Indiana.

Peter K. Trzyna, "Supplemental Amendment and Response" filed on Nov. 5, 2010, in U.S. Appl. No. 11/510,351, filed Aug. 24, 2006. pp. 1-18. USA.

Patrice L. Winder, "Office Action" mailed on Nov. 24. 2010, in U.S. Appl. No. 11/510,463, filed Aug. 24, 2006. pp. 1-25. USA.

Peter K. Trzyna, "Amendment and Response" filed on Jul. 23, 2010, in U.S. Appl. No. 11/510,463, filed Aug. 24, 2006. pp. 1-15. USA.

"ITU-T: Telecommunication Standardization of Sector ITU: Series T: Terminal Equipments and Protocols for Telematic Services," International Telecommunication Union, T.120, (Jul. 1996) pp. 1-24.

"T.120 Whitepaper: A Primer on the T.120 Series Standard," DataBeam Corporation, 1995, pp. 1-15.

"Complaint: Brian Hollander vs. Peter K. Trzyna and PTK Technologies, LLC," Filed Nov. 13, 2007, pp. 1-18.

Krishnamurthy, et al., "Yeast: A General Purpose Event-Action System," IEEE Transactions on Software Engineering, vol. 21, No. 10, Oct. 1995. (AOL 052778-052790).

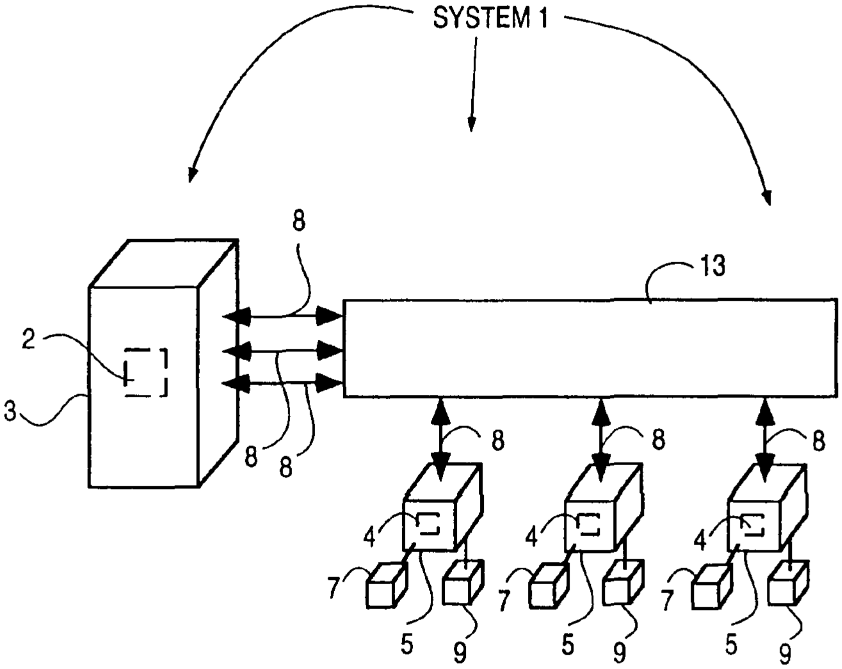
Lovestrand, et al., "Being Selectively Aware with the Khronika System," Proceedings of the Second European Conference on Computer-Supported Cooperative Work, Sep. 25-57, 1991, Amsterdam, The Netherlands, pp. 265-277. (AOL 052791-052803).

Dourish, et al., "Portholes: Supporting Awareness in a Distributed Work Group," Chi '92, May 3-7, 1992, pp. 541-547. (AOL 052804-052810).

Gaver, et al., "Realizing a Video Environment: Europarc's Rave System," Chi '92, May 3-7, 1992, pp. 27-35. (AOL 052811-052819).

* cited by examiner

FIG. 1



COMMUNICATIONS OVERVIEW

FIG. 2

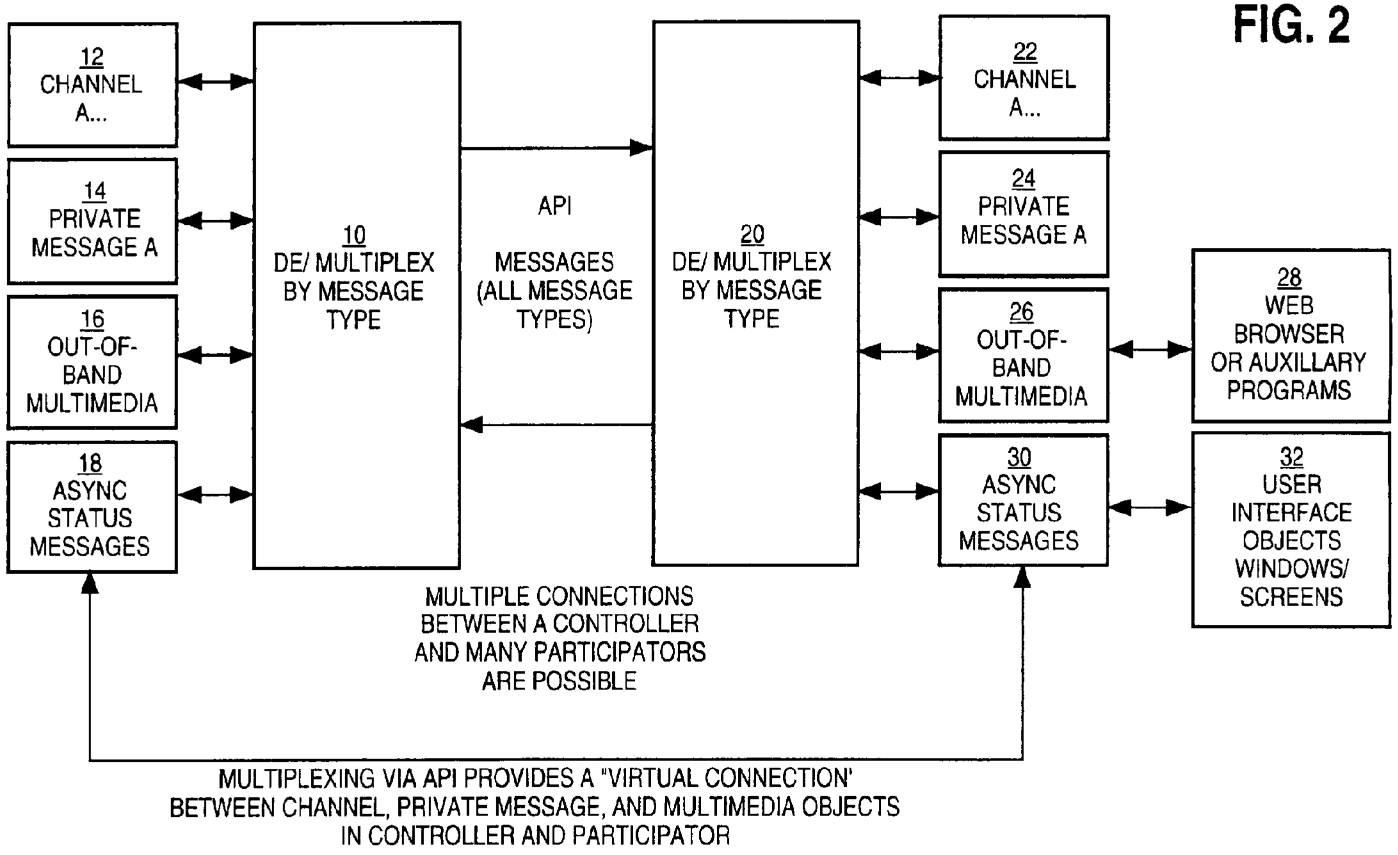

12 CHANNEL A...
14 PRIVATE MESSAGE A
16 OUT-OF-BAND MULTIMEDIA
18 ASYNC STATUS MESSAGES
10 DE/ MULTIPLEX BY MESSAGE TYPE
API
MESSAGES (ALL MESSAGE TYPES)
20 DE/ MULTIPLEX BY MESSAGE TYPE
22 CHANNEL A...
24 PRIVATE MESSAGE A
26 OUT-OF-BAND MULTIMEDIA
30 ASYNC STATUS MESSAGES
28 WEB BROWSER OR AUXILLARY PROGRAMS
32 USER INTERFACE OBJECTS WINDOWS/ SCREENS
MULTIPLE CONNECTIONS BETWEEN A CONTROLLER AND MANY PARTICIPATORS ARE POSSIBLE
MULTIPLEXING VIA API PROVIDES A "VIRTUAL CONNECTION' BETWEEN CHANNEL, PRIVATE MESSAGE, AND MULTIMEDIA OBJECTS IN CONTROLLER AND PARTICIPATOR

FIG. 3

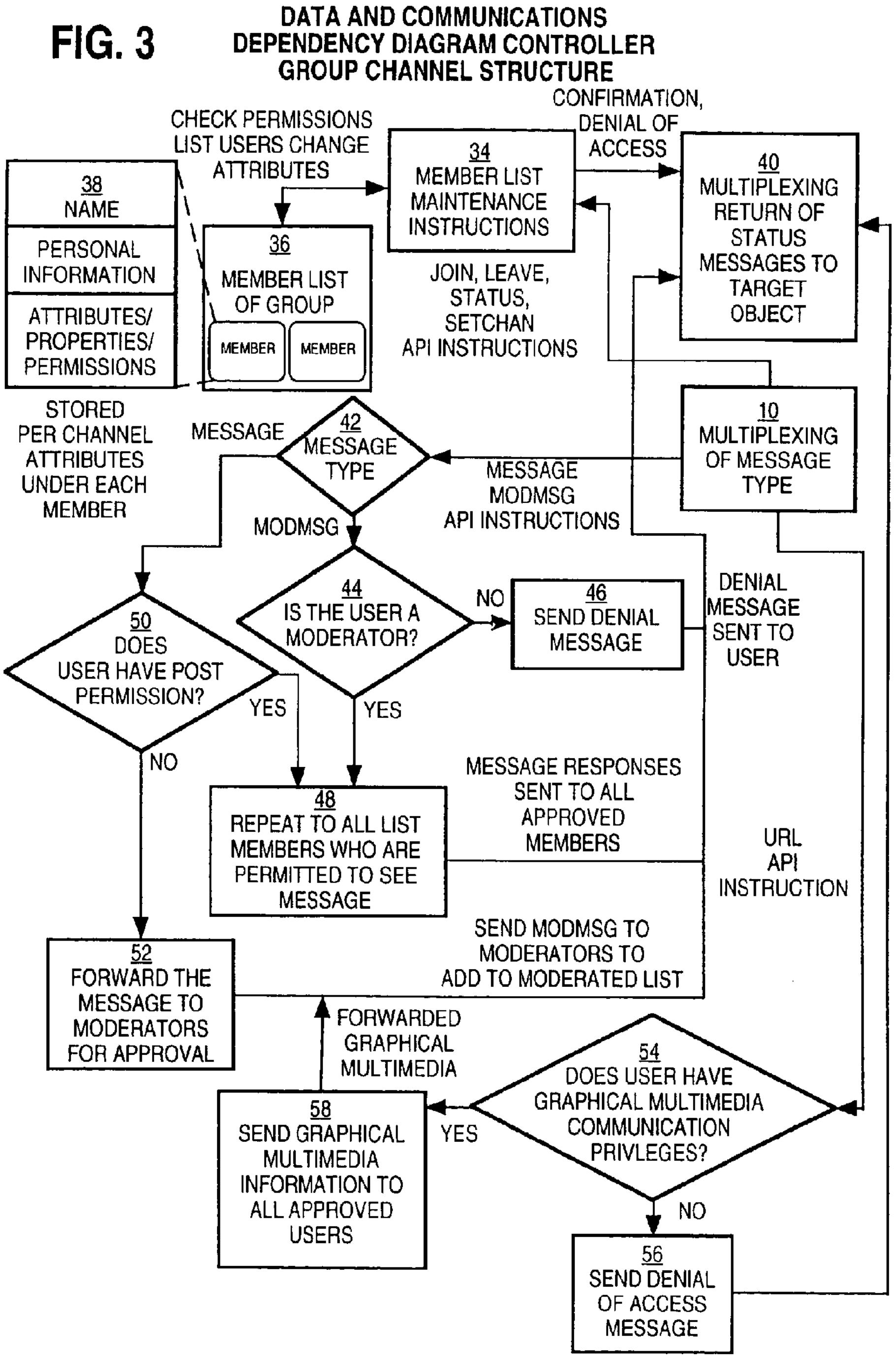

DATA AND COMMUNICATIONS
DEPENDENCY DIAGRAM CONTROLLER
GROUP CHANNEL STRUCTURE
CHECK PERMISSIONS LIST USERS CHANGE ATTRIBUTES
CONFIRMATION, DENIAL OF ACCESS
38 NAME
PERSONAL INFORMATION
ATTRIBUTES/ PROPERTIES/ PERMISSIONS
STORED PER CHANNEL ATTRIBUTES UNDER EACH MEMBER
34 MEMBER LIST MAINTENANCE INSTRUCTIONS
36 MEMBER LIST OF GROUP
MEMBER
MEMBER
JOIN, LEAVE, STATUS, SETCHAN API INSTRUCTIONS
40 MULTIPLEXING RETURN OF STATUS MESSAGES TO TARGET OBJECT
10 MULTIPLEXING OF MESSAGE TYPE
MESSAGE
42 MESSAGE TYPE
MESSAGE MODMSG API INSTRUCTIONS
MODMSG
44 IS THE USER A MODERATOR?
NO
46 SEND DENIAL MESSAGE
DENIAL MESSAGE SENT TO USER
50 DOES USER HAVE POST PERMISSION?
YES
YES
NO
48 REPEAT TO ALL LIST MEMBERS WHO ARE PERMITTED TO SEE MESSAGE
MESSAGE RESPONSES SENT TO ALL APPROVED MEMBERS
URL API INSTRUCTION
52 FORWARD THE MESSAGE TO MODERATORS FOR APPROVAL
SEND MODMSG TO MODERATORS TO ADD TO MODERATED LIST
FORWARDED GRAPHICAL MULTIMEDIA
54 DOES USER HAVE GRAPHICAL MULTIMEDIA COMMUNICATION PRIVLEGES?
YES
NO
58 SEND GRAPHICAL MULTIMEDIA INFORMATION TO ALL APPROVED USERS
56 SEND DENIAL OF ACCESS MESSAGE

FIG. 4

CENTRAL CONTROLLER LOOP COMMUNICATIONS

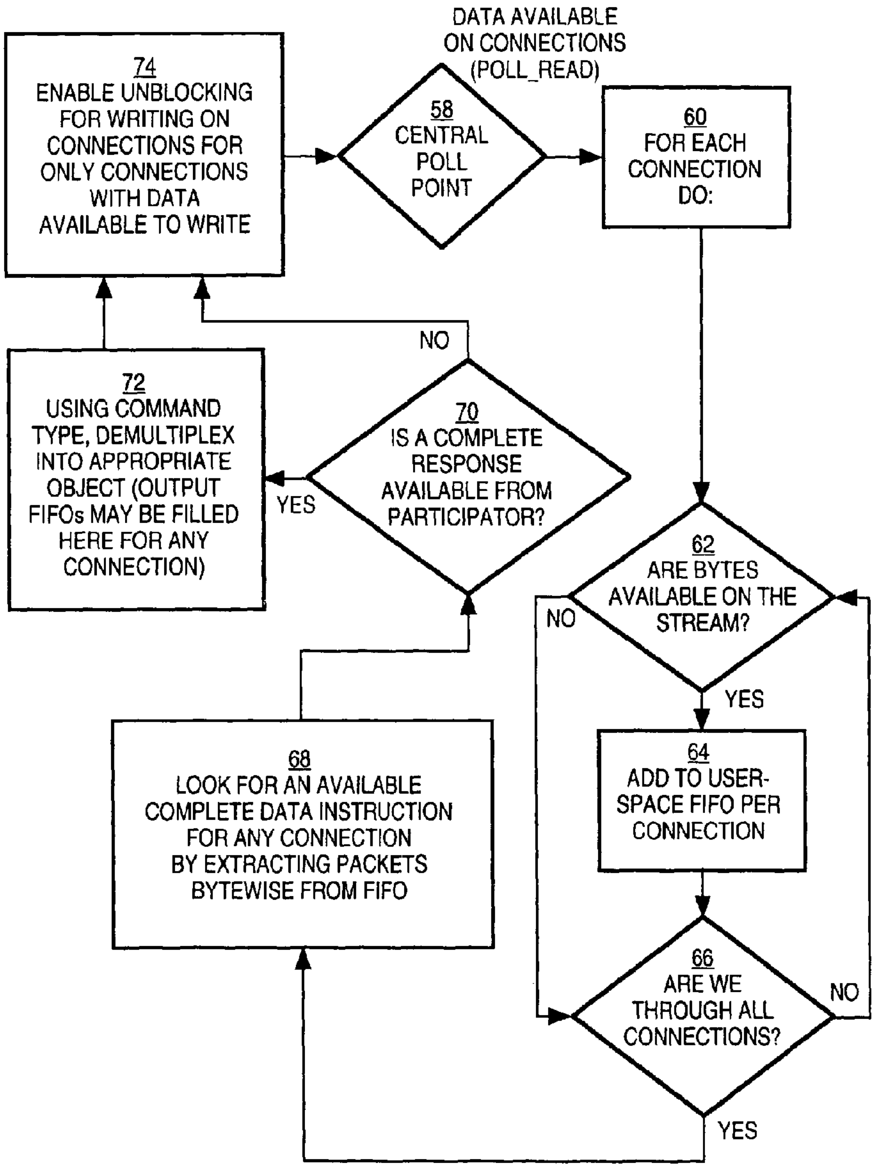

DATA AVAILABLE ON CONNECTIONS (POLL_READ)
74 ENABLE UNBLOCKING FOR WRITING ON CONNECTIONS FOR ONLY CONNECTIONS WITH DATA AVAILABLE TO WRITE
58 CENTRAL POLL POINT
60 FOR EACH CONNECTION DO:
NO
72 USING COMMAND TYPE, DEMULTIPLEX INTO APPROPRIATE OBJECT (OUTPUT FIFOs MAY BE FILLED HERE FOR ANY CONNECTION)
YES
70 IS A COMPLETE RESPONSE AVAILABLE FROM PARTICIPATOR?
62 ARE BYTES AVAILABLE ON THE STREAM?
NO
YES
68 LOOK FOR AN AVAILABLE COMPLETE DATA INSTRUCTION FOR ANY CONNECTION BY EXTRACTING PACKETS BYTEWISE FROM FIFO
64 ADD TO USER-SPACE FIFO PER CONNECTION
66 ARE WE THROUGH ALL CONNECTIONS?
NO
YES

FIG. 5

CLIENT CHANNEL DATA STRUCTURE AND INFORMATION FLOW DIAGRAM

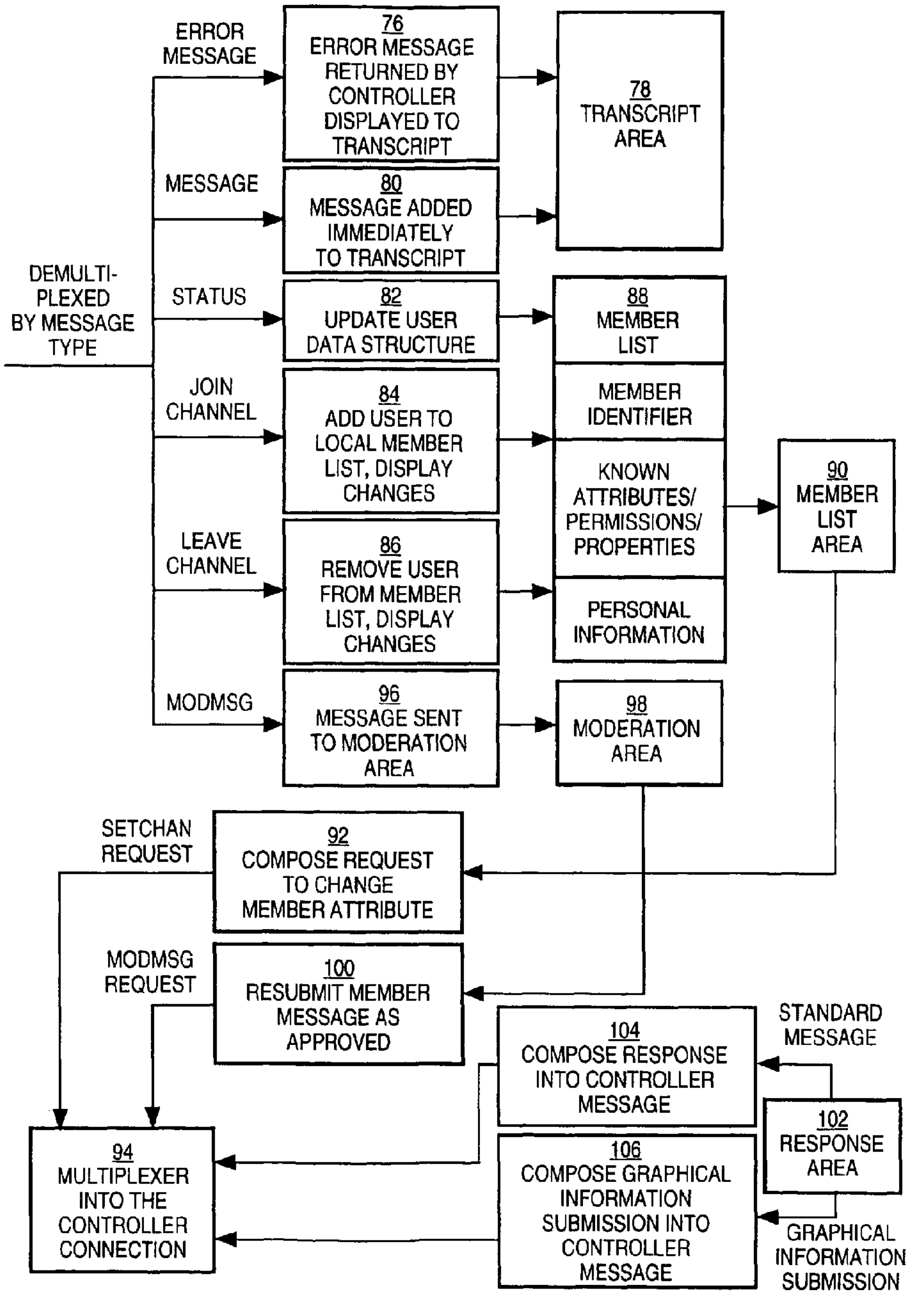

ERROR MESSAGE
76 ERROR MESSAGE RETURNED BY CONTROLLER DISPLAYED TO TRANSCRIPT
78 TRANSCRIPT AREA
MESSAGE
80 MESSAGE ADDED IMMEDIATELY TO TRANSCRIPT
DEMULTI-PLEXED BY MESSAGE TYPE
STATUS
82 UPDATE USER DATA STRUCTURE
88 MEMBER LIST
MEMBER IDENTIFIER
KNOWN ATTRIBUTES/ PERMISSIONS/ PROPERTIES
PERSONAL INFORMATION
JOIN CHANNEL
84 ADD USER TO LOCAL MEMBER LIST, DISPLAY CHANGES
90 MEMBER LIST AREA
LEAVE CHANNEL
86 REMOVE USER FROM MEMBER LIST, DISPLAY CHANGES
MODMSG
96 MESSAGE SENT TO MODERATION AREA
98 MODERATION AREA
SETCHAN REQUEST
92 COMPOSE REQUEST TO CHANGE MEMBER ATTRIBUTE
MODMSG REQUEST
100 RESUBMIT MEMBER MESSAGE AS APPROVED
STANDARD MESSAGE
104 COMPOSE RESPONSE INTO CONTROLLER MESSAGE
102 RESPONSE AREA
94 MULTIPLEXER INTO THE CONTROLLER CONNECTION
106 COMPOSE GRAPHICAL INFORMATION SUBMISSION INTO CONTROLLER MESSAGE
GRAPHICAL INFORMATION SUBMISSION

FIG. 6

PARTICIPATION SOFTWARE OUT-OF-BAND MULTIMEDIA
OUT-OF-BAND MULTIMEDIA INFORMATION FLOW DIAGRAM

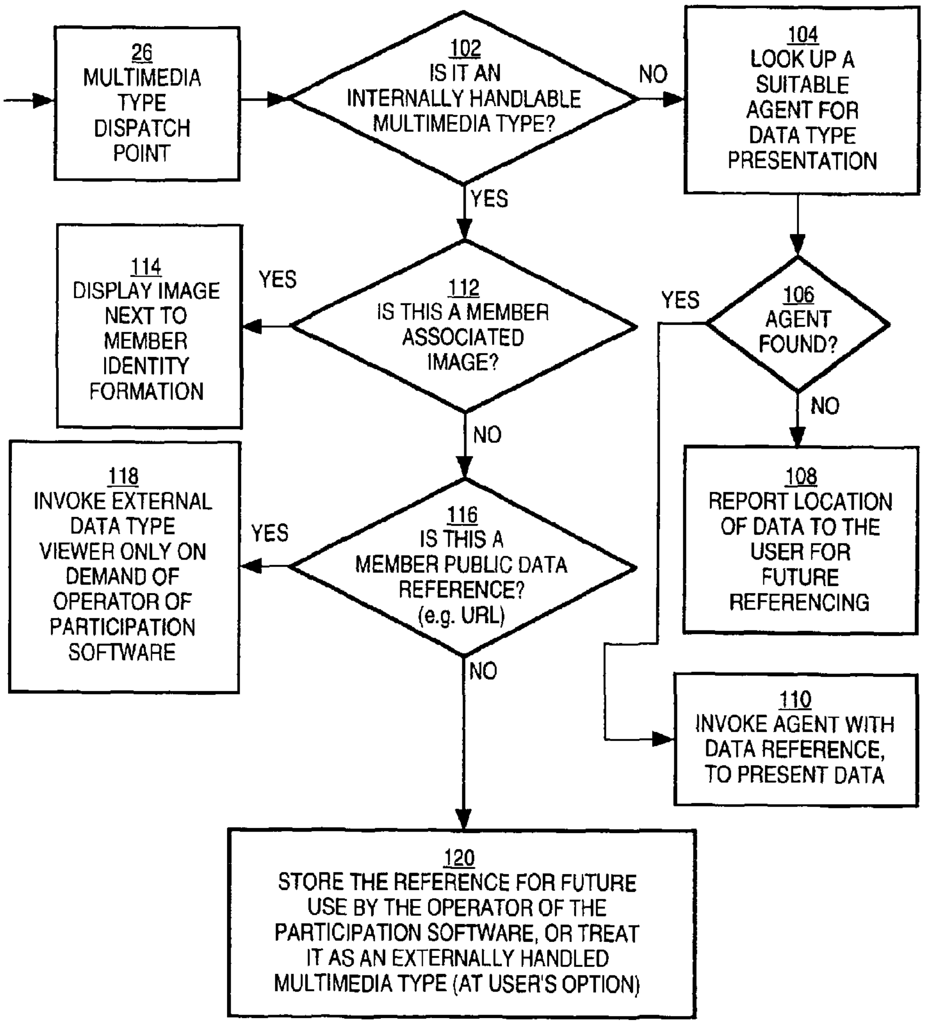
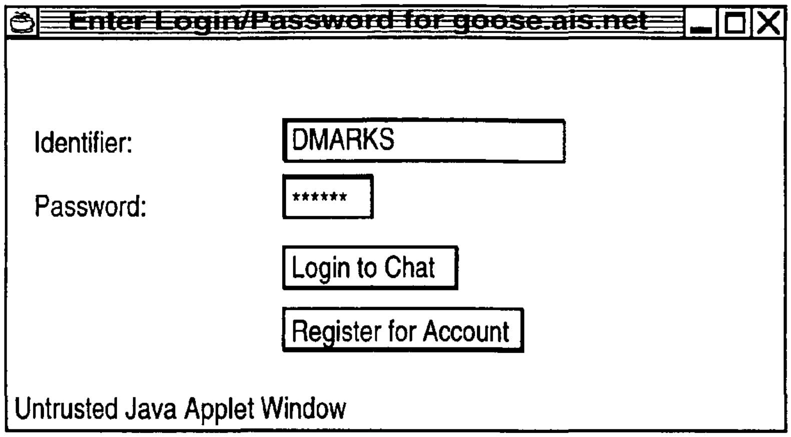

26
MULTIMEDIA TYPE DISPATCH POINT
102
IS IT AN INTERNALLY HANDLABLE MULTIMEDIA TYPE?
NO
104
LOOK UP A SUITABLE AGENT FOR DATA TYPE PRESENTATION
YES
114
DISPLAY IMAGE NEXT TO MEMBER IDENTITY FORMATION
YES
112
IS THIS A MEMBER ASSOCIATED IMAGE?
YES
106
AGENT FOUND?
NO
NO
118
INVOKE EXTERNAL DATA TYPE VIEWER ONLY ON DEMAND OF OPERATOR OF PARTICIPATION SOFTWARE
YES
116
IS THIS A MEMBER PUBLIC DATA REFERENCE? (e.g. URL)
108
REPORT LOCATION OF DATA TO THE USER FOR FUTURE REFERENCING
NO
110
INVOKE AGENT WITH DATA REFERENCE, TO PRESENT DATA
120
STORE THE REFERENCE FOR FUTURE USE BY THE OPERATOR OF THE PARTICIPATION SOFTWARE, OR TREAT IT AS AN EXTERNALLY HANDLED MULTIMEDIA TYPE (AT USER'S OPTION)

FIG. 7



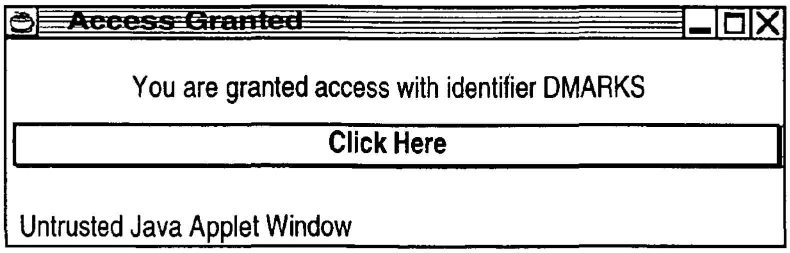
Enter Login/Password for goose.ais.net

Identifier: DMARKS

Password: ******

Untrusted Java Applet Window

FIG. 8



Access Granted

You are granted access with identifier DMARKS

Untrusted Java Applet Window

FIG. 9

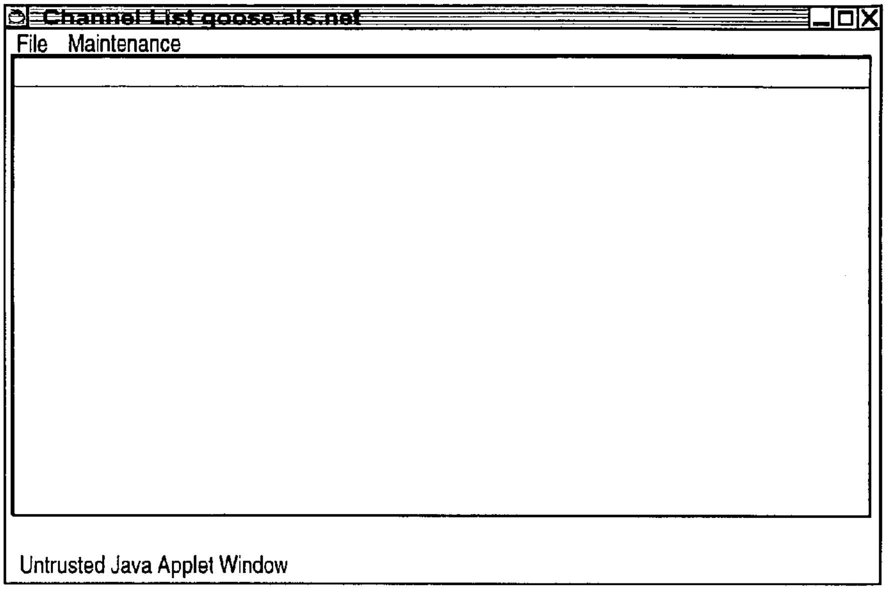
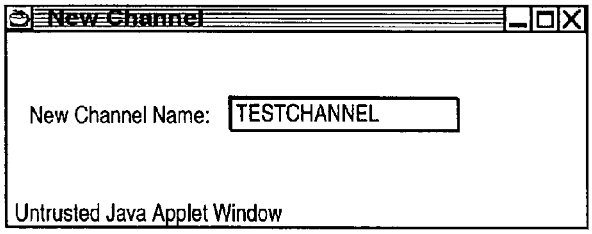
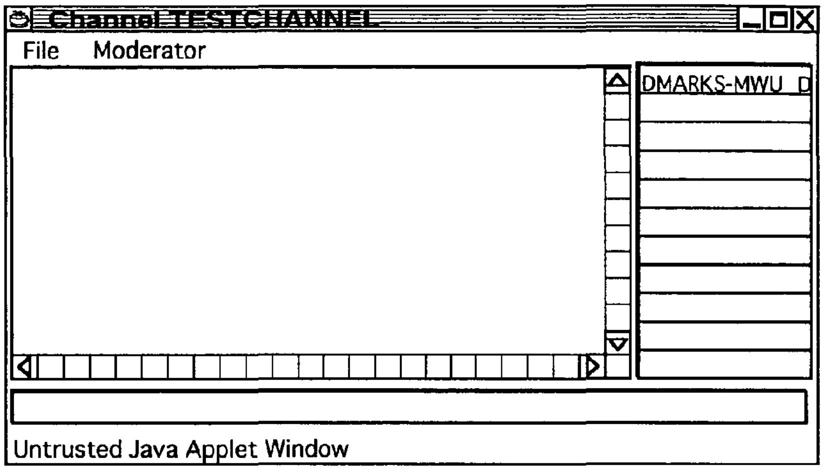


FIG. 10



New Channel Name: TESTCHANNEL

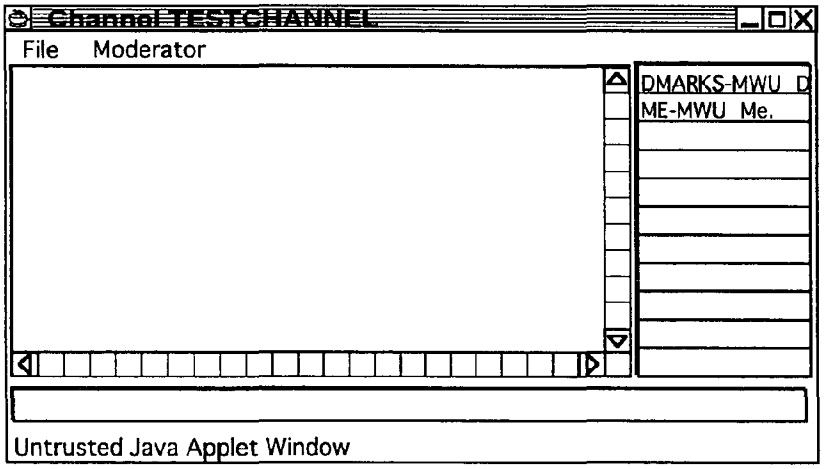
FIG. 11



Channel TESTCHANNEL

Untrusted Java Applet Window

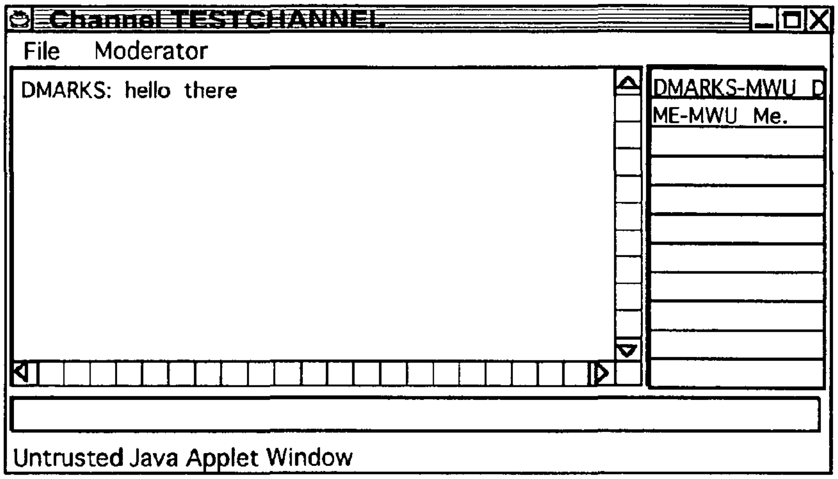
FIG. 12



Channel TESTCHANNEL

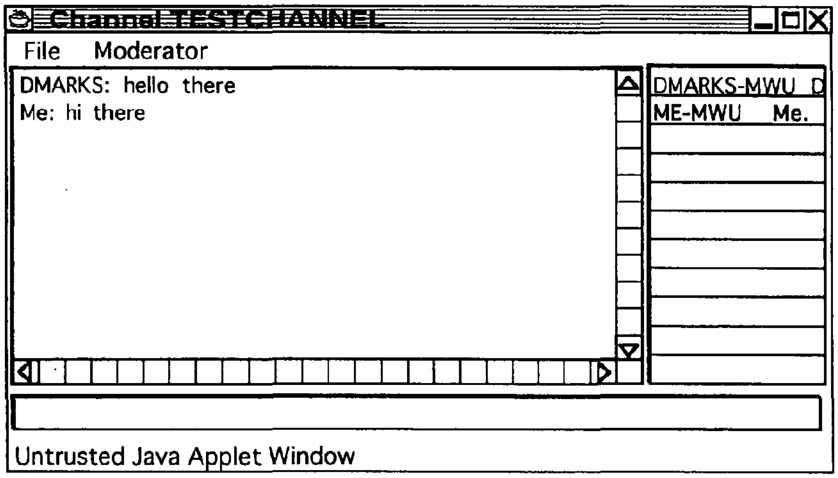
Untrusted Java Applet Window

FIG. 13



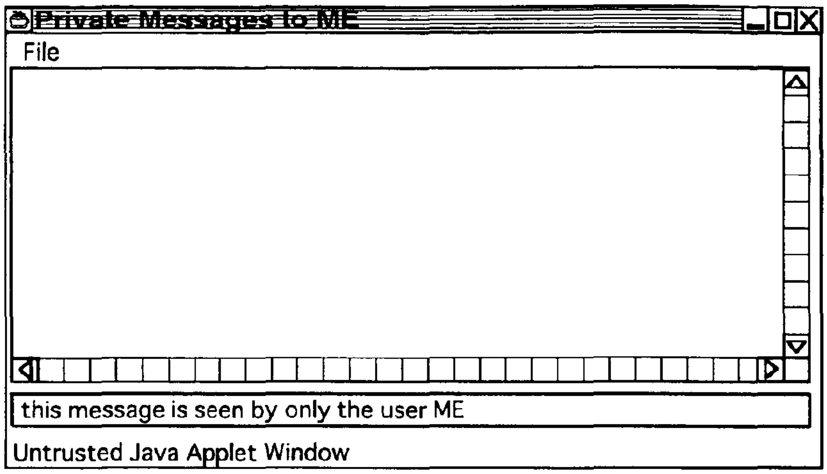
DMARKS: hello there

FIG. 14



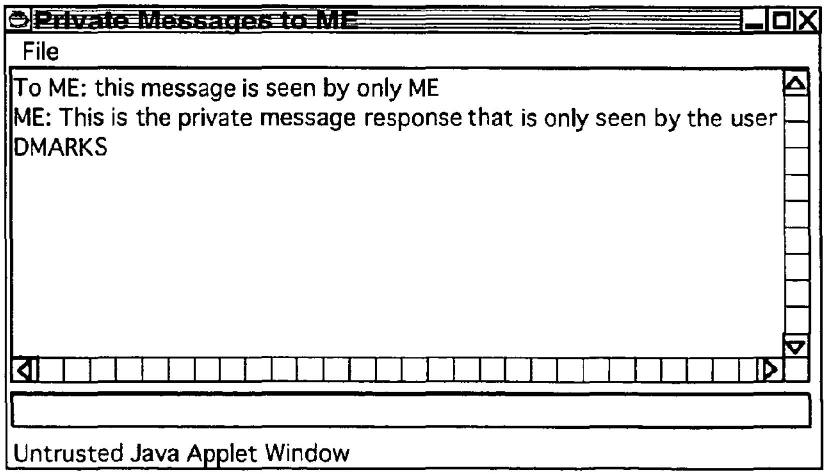
DMARKS: hello there
Me: hi there

FIG. 15



this message is seen by only the user ME

FIG. 16



To ME: this message is seen by only ME
ME: This is the private message response that is only seen by the user DMARKS

FIG. 17

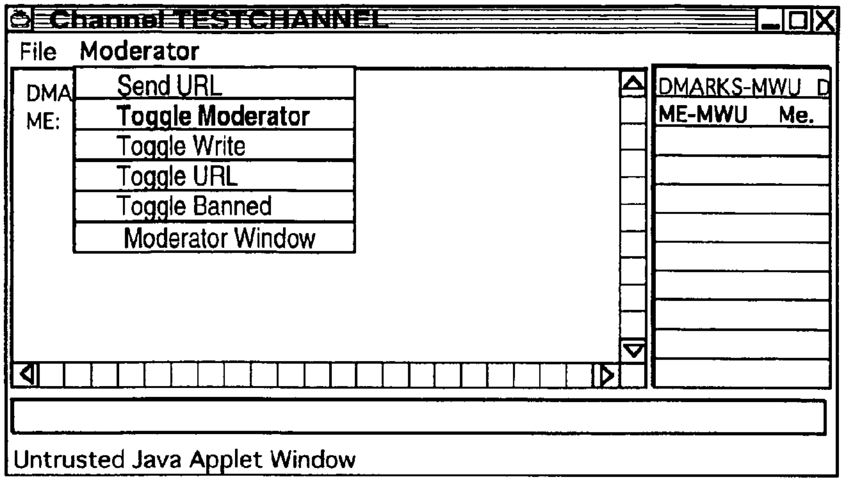
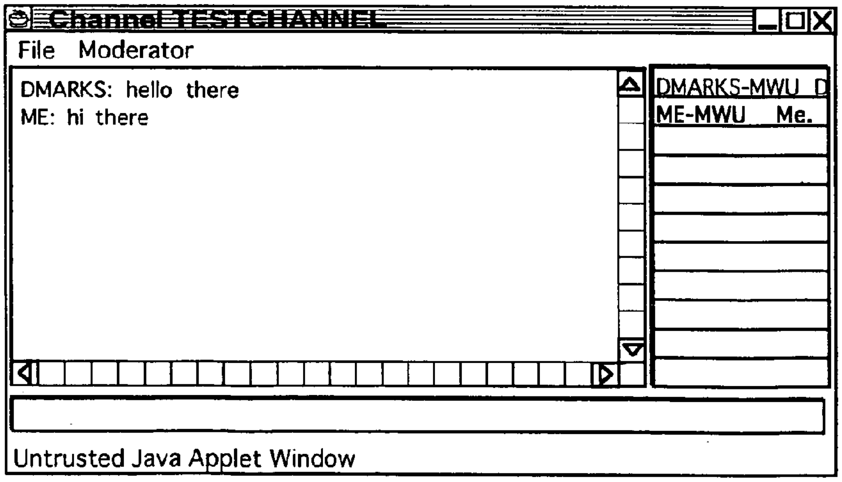


FIG. 18



DMARKS: hello there
ME: hi there

FIG. 19

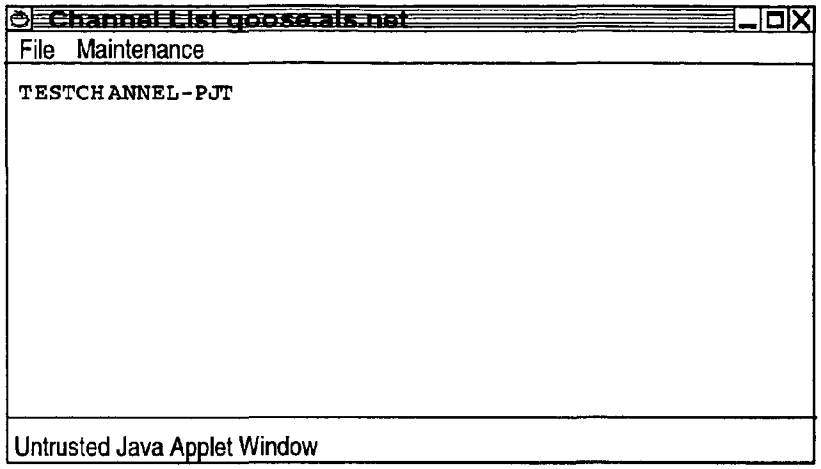

Channel List goose.als.net
File Maintenance
TESTCHANNEL-PJT
Untrusted Java Applet Window

FIG. 20

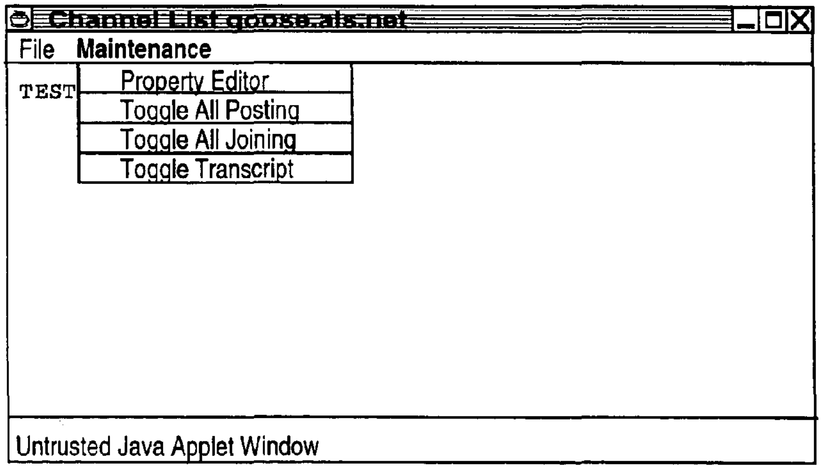
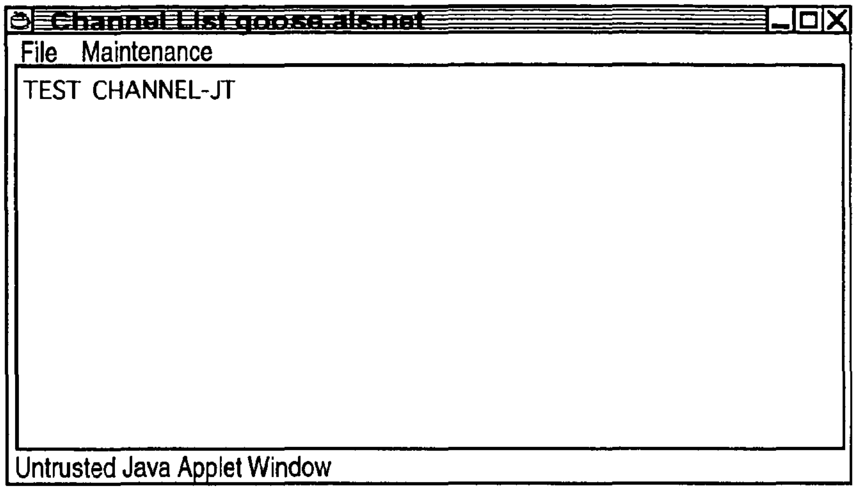
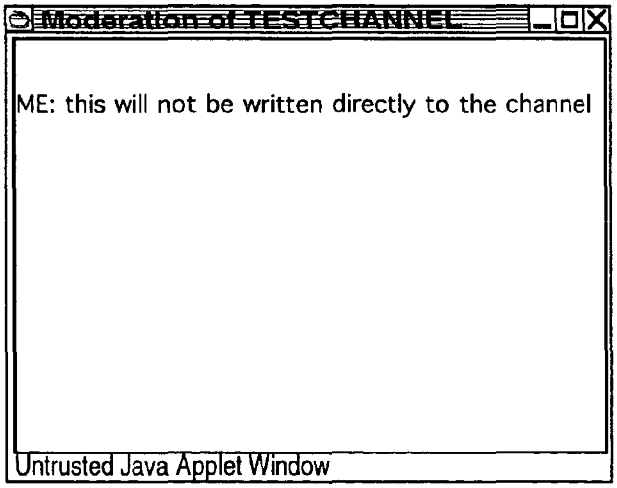

Channel List goose.als.net
File Maintenance
TEST
Property Editor
Toggle All Posting
Toggle All Joining
Toggle Transcript
Untrusted Java Applet Window

FIG. 21



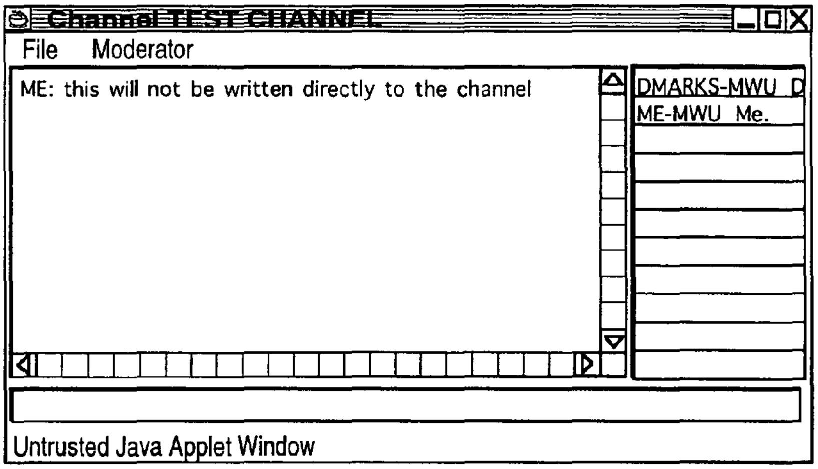
TEST CHANNEL-JT

FIG. 22



ME: this will not be written directly to the channel

FIG. 23

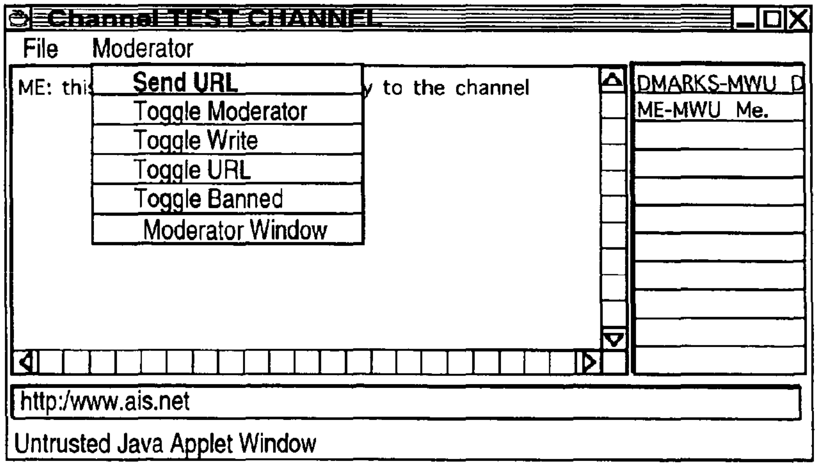


ME: this will not be written directly to the channel

DMARKS-MWU D
ME-MWU Me.

Untrusted Java Applet Window

FIG. 24



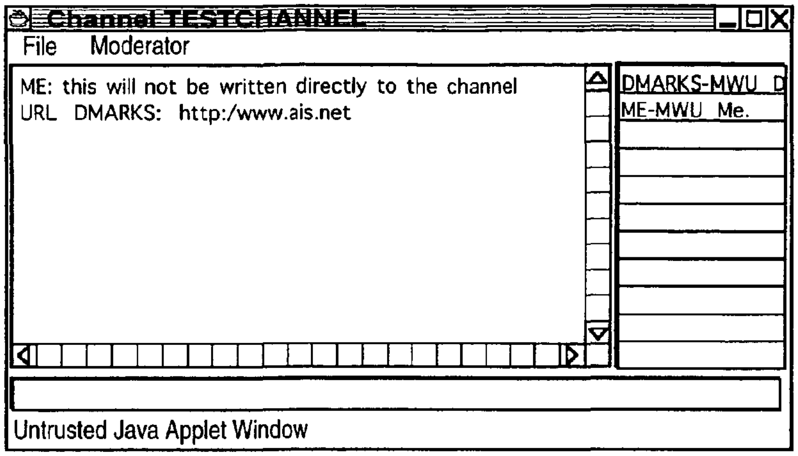
ME: thi y to the channel

DMARKS-MWU D
ME-MWU Me.

http:/www.ais.net

Untrusted Java Applet Window

FIG. 25



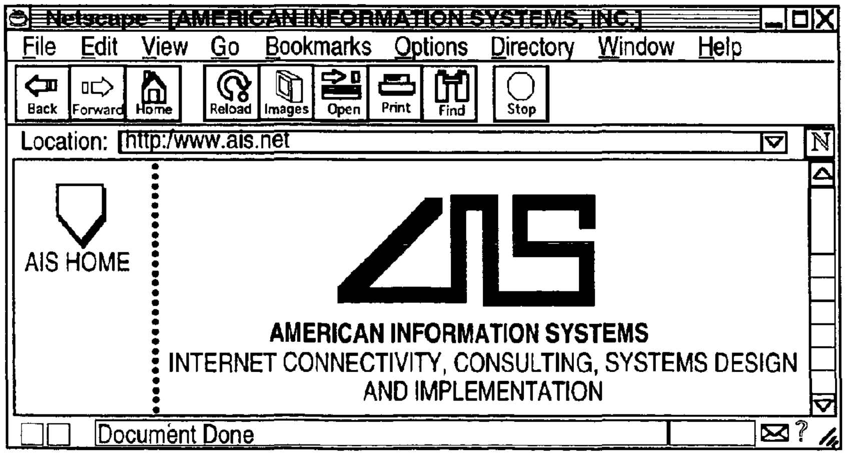
Channel TESTCHANNEL

ME: this will not be written directly to the channel
URL DMARKS: http:/www.ais.net

DMARKS-MWU D
ME-MWU Me.

Untrusted Java Applet Window

FIG. 26



Netscape - [AMERICAN INFORMATION SYSTEMS, INC.]

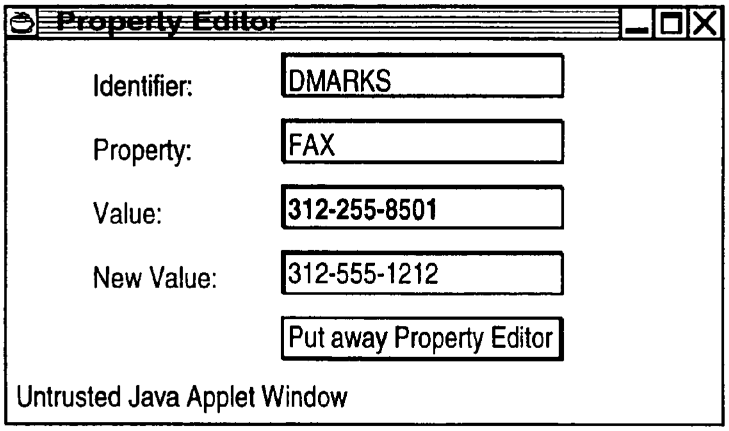
Location: http:/www.ais.net

AIS HOME

AMERICAN INFORMATION SYSTEMS
INTERNET CONNECTIVITY, CONSULTING, SYSTEMS DESIGN AND IMPLEMENTATION

Document Done

FIG. 27



Property Editor

Identifier: DMARKS

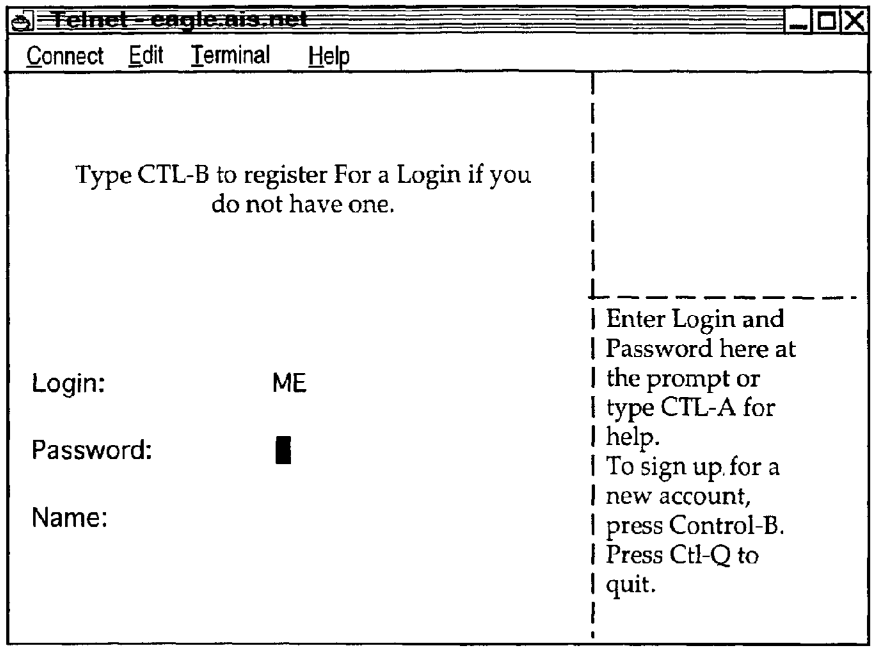
Property: FAX

Value: 312-255-8501

New Value: 312-555-1212

Untrusted Java Applet Window

FIG. 28



Type CTL-B to register For a Login if you do not have one.

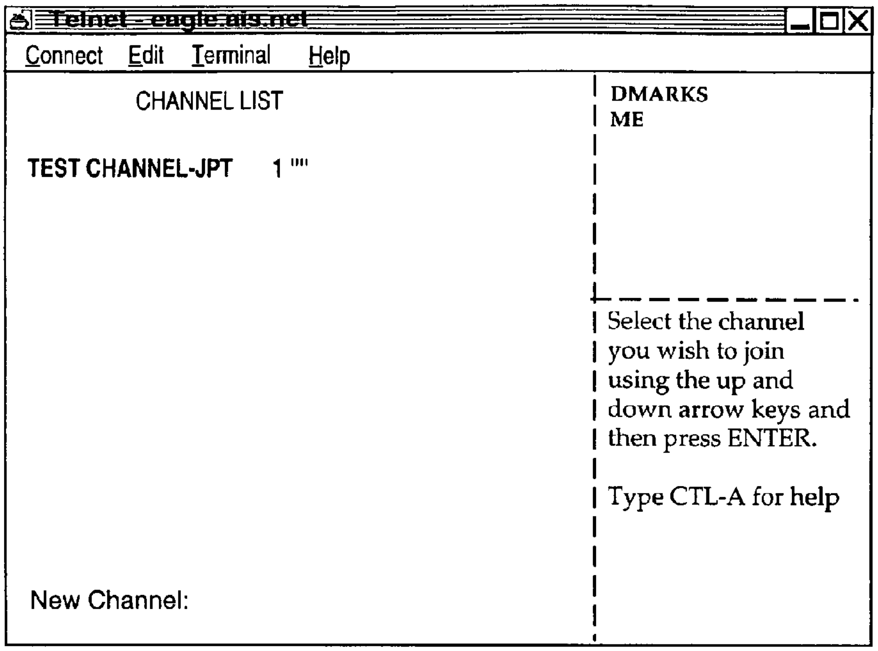
Login: ME

Password:

Name:

Enter Login and Password here at the prompt or type CTL-A for help.
To sign up for a new account, press Control-B.
Press Ctl-Q to quit.

FIG. 29



CHANNEL LIST

TEST CHANNEL-JPT 1 ""

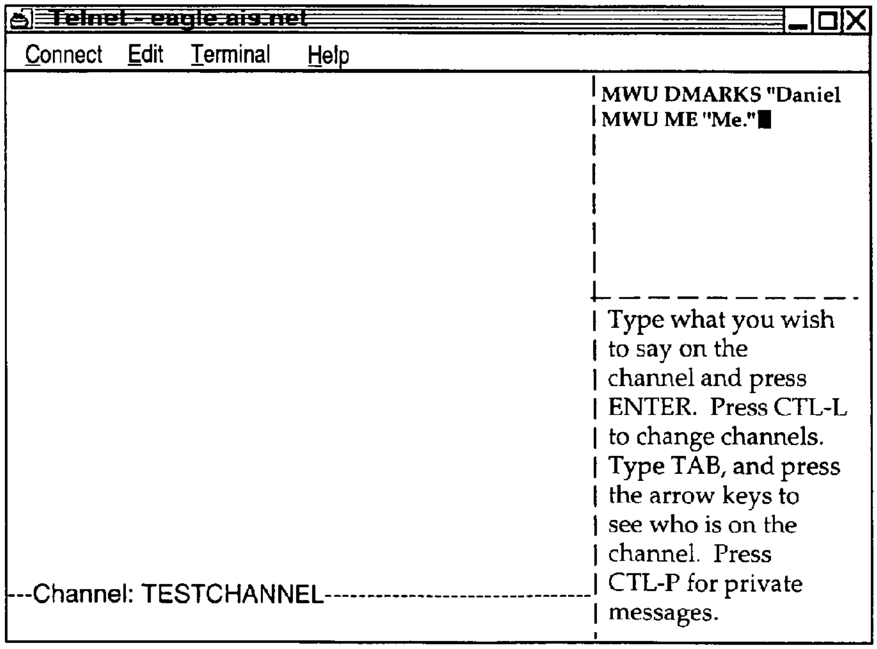
New Channel:

DMARKS
ME

Select the channel you wish to join using the up and down arrow keys and then press ENTER.

Type CTL-A for help

FIG. 30

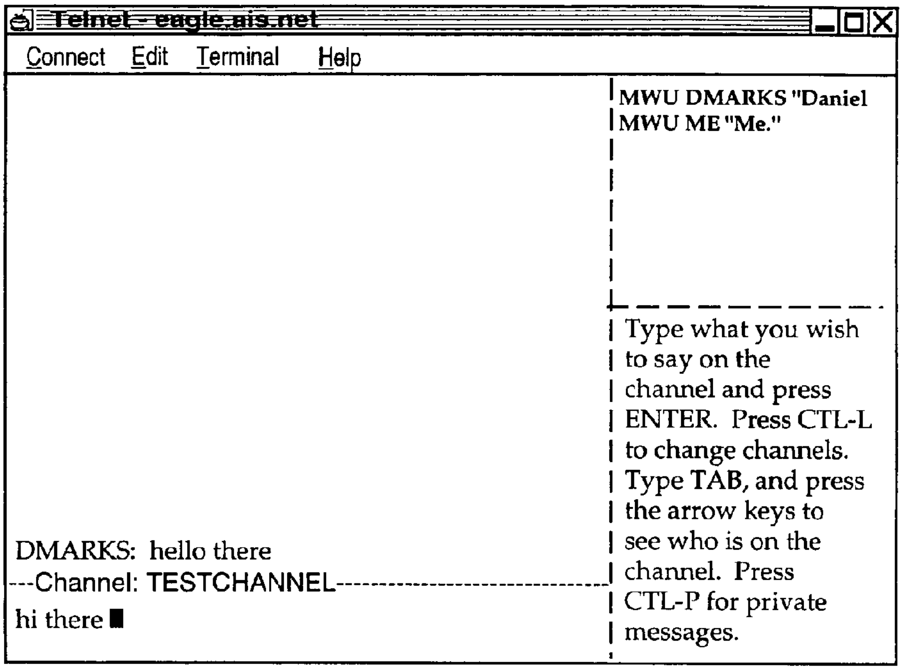


---Channel: TESTCHANNEL-----------------------------

MWU DMARKS "Daniel
MWU ME "Me."█

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

FIG. 31

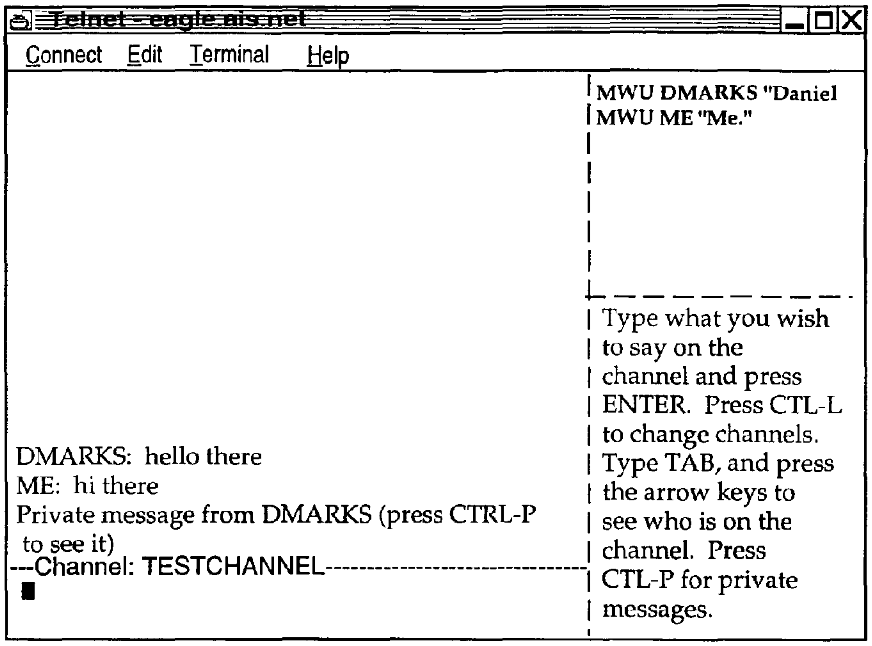


MWU DMARKS "Daniel
MWU ME "Me."

Type what you wish to say on the channel and press ENTER. Press CTL-L to change channels. Type TAB, and press the arrow keys to see who is on the channel. Press CTL-P for private messages.

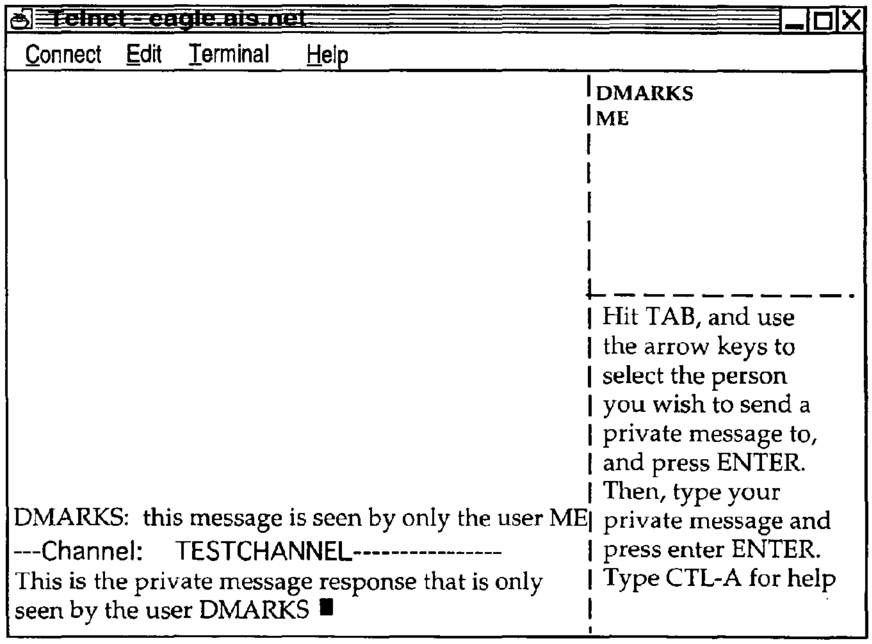
```
DMARKS:  hello there
---Channel: TESTCHANNEL-------------------------------
hi there █
```

FIG. 32



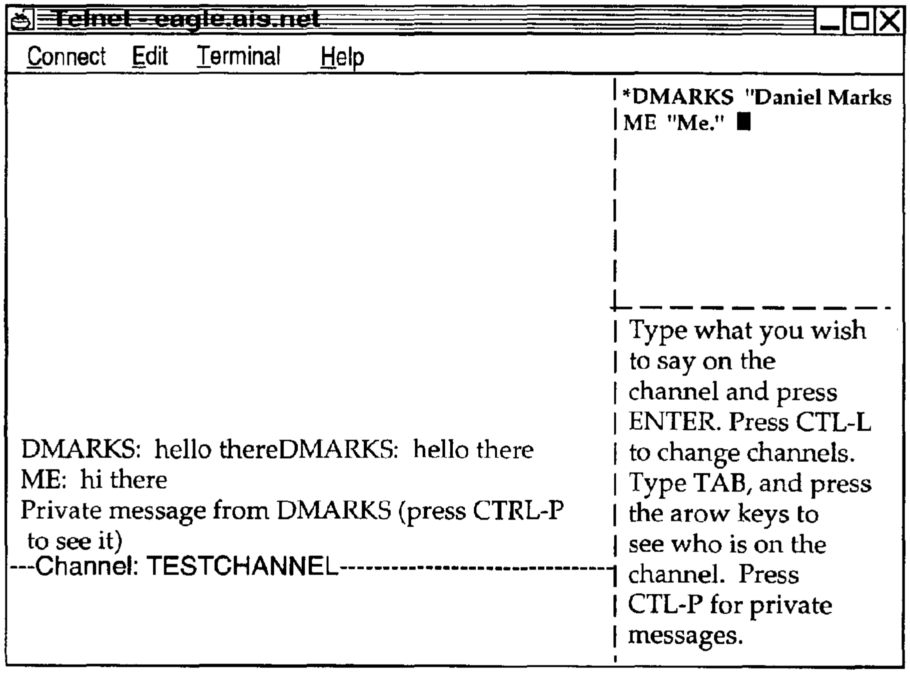
```
                                                   | MWU DMARKS "Daniel
                                                   | MWU ME "Me."
                                                   |
                                                   L- - - - - - - - - -
                                                   | Type what you wish
                                                   | to say on the
                                                   | channel and press
                                                   | ENTER.  Press CTL-L
                                                   | to change channels.
DMARKS:  hello there                               | Type TAB, and press
ME:  hi there                                      | the arrow keys to
Private message from DMARKS (press CTRL-P          | see who is on the
 to see it)                                        | channel.  Press
---Channel: TESTCHANNEL----------------------------| CTL-P for private
 ■                                                 | messages.
```

FIG. 33



```
                                                   | DMARKS
                                                   | ME
                                                   |
                                                   L- - - - - - - - - -
                                                   | Hit TAB, and use
                                                   | the arrow keys to
                                                   | select the person
                                                   | you wish to send a
                                                   | private message to,
                                                   | and press ENTER.
                                                   | Then, type your
DMARKS:  this message is seen by only the user ME  | private message and
---Channel:    TESTCHANNEL----------------         | press enter ENTER.
This is the private message response that is only  | Type CTL-A for help
seen by the user DMARKS ■                          |
```

FIG. 34



```
*DMARKS "Daniel Marks
ME "Me."
```

```
DMARKS: hello thereDMARKS: hello there
ME: hi there
Private message from DMARKS (press CTRL-P
 to see it)
---Channel: TESTCHANNEL------------------------------
```

```
Type what you wish
to say on the
channel and press
ENTER. Press CTL-L
to change channels.
Type TAB, and press
the arow keys to
see who is on the
channel. Press
CTL-P for private
messages.
```

## REAL TIME COMMUNICATIONS SYSTEM

This invention is a continuation of Ser. No. 08/617,658 filed Apr. 1, 1996, and issued as U.S. Pat. No. 5,956,491 on Sep. 21, 1999, directed to an apparatus, a manufacture, and methods for making and using the same, in a field of digital electrical computer systems.

### I. FIELD OF INVENTION

More particularly, the present invention is directed to a digital electrical computer system involving a plurality of participator computers linked by a network to at least one of a plurality of participator computers, the participator computers operating in conjunction with the controller computer to handle multiplexing operations for communications involving groups of some of the participator computers.

### II. BACKGROUND OF THE INVENTION

Multiplexing group communications among computers ranges from very simple to very complex communications systems. At a simple level, group communications among computers involve electronic mail sent in a one way transmission to all those in a group or subgroup using, say, a local area network. Arbitrating which computers receive electronic mail is a rather well understood undertaking.

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

Even more complex is linking computers to communicate in what has become known as a "chat room." Chat room communications can be text, as exemplified by such Internet service providers as America On Line. Multiplexing multimedia is more complex for this electronic environment.

The Internet was structured for one-way communications analogous to electronic mail, rather than for real time group chat room communications. Further, unlike the an Internet service provider, which has control over both the hardware platform and the computer program running on the platform to create the "chat room", there is no particular control over the platform that would be encountered on the Internet. Therefore, development of multiplexing technology for such an environment has been minimal.

Even with an emergence of the World Wide Web, which does have certain graphical multimedia capability, sophisticated chat room communication multiplexing has been the domain of the Internet service providers. Users therefore have a choice between the limited audience of a particular Internet Service provider or the limited chat capability of the Internet.

### III. SUMMARY OF THE INVENTION

It is an object of the present invention to overcome such limitations of the prior art and to advance and improve the technology of group computer multiplexing to enable better computerized group communications.

It is another object of the present invention to provide a computerized human communication arbitrating and distributing system.

It is yet another object of the present invention to provide a group communication multiplexing system involving a controller digital computer linked to a plurality of participator computers to organize communications by groups of the participator computers.

It is still another object of the present invention to link the controller computer and the plurality of computers with respective software coordinated to arbitrate multiplexing activities.

It is still a further object of the present invention to provide a chat capability suitable for handling graphical, textual, and multimedia information in a platform independent manner.

These and other objects and utilities of the invention, apparent from the discussion herein, are addressed by a computerized human communication arbitrating and distributing system. The system includes a controller digital electrical computer and a plurality of participator digital computers, each of the participator computers including an input device for receiving human-input information and an output device for presenting information to a user having a user identity. A connection such as the Internet links the controller computer with each of the participator computers.

Controller software runs on the controller computer, programming the controller computer to arbitrate in accordance with predefined rules including said user identity, which ones of the participator computers can interact in one of a plurality of groups communicating through the controller computer and to distribute real time data to the respective ones of the groups.

Participator software runs on each of the participator computers to program each of the participator computers to operate a user interface. The user interface permits one of the users to send and/or receive a multimedia information message to the controller computer, which arbitrates which of the participator computers receives the multimedia information message. The controller computer also conveys the multimedia information message to the selected participator computers to present the multimedia information to the respective user.

Therefore, for a computer system involving a plurality of programmed participator computers running the participator computer program can interact through a programmed controller computer with the controller computer multiplexing the communications for groups formed from the plurality, as well as arbitrating communications behavior.

### IV. BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a depiction of hardware suitable for performing the present invention;

FIG. **2** is a communications overview of the present invention.

FIG. **3** is a data and communications dependency diagram for the controller group channel structure of the present invention.

FIG. **4** is a flow chart of the central controller loop communications for the controller computer.

FIG. **5** is a client channel data structure and information flow diagram of the present invention.

FIG. **6** is a participator software out-of-band multimedia information flow diagram of the present invention.

FIG. **7** is an illustration of a login/password screen of the present invention.

FIG. **8** is an illustration of a confirmation screen of the present invention.

FIG. **9** is an illustration of a channel list area screen of the present invention.

FIG. **10** is an illustration of a New Channel option pull-down menu screen of the present invention.

FIG. **11** is an illustration of a member on a new channel screen of the present invention.

FIG. **12** is an illustration of a second member on the new channel screen of the present invention.

FIG. **13** is an illustration of a communication on the new channel screen of the present invention.

FIG. **14** is an illustration of a private message window on the new channel screen of the present invention.

FIG. **15** is an illustration of a private message displayed on the private message window on the new channel screen of the present invention.

FIG. **16** is a further illustration of the private message on the private message window on new channel screen of the present invention.

FIG. **17** is an illustration of an attribute revocation on the new channel screen of the present invention.

FIG. **18** is a further illustration of the new channel screen of the present invention.

FIG. **19** is an illustration of the channel list window screen of the present invention.

FIG. **20** is an illustration of the toggle posting option on a screen of the present invention.

FIG. **21** is an illustration of a moderated version of the new channel screen of the present invention.

FIG. **22** is an illustration of a communication on a moderation window screen of the present invention.

FIG. **23** is an illustration of the communication passed on to the moderated version of the new channel screen of the present invention.

FIG. **24** is an illustration of a communication, for sending a graphical multimedia message, on to the moderated version of the new channel screen of the present invention

FIG. **25** is an illustration, showing the name of the URL, on a moderated version of the new channel screen of the present invention.

FIG. **26** is an illustration of data associated with the graphical multimedia message on a moderated version of the new channel screen of the present invention.

FIG. **27** is an illustration of a proprietary editor, suitable for a dialog to change tokens, on a screen of the present invention.

FIG. **28** is an illustration of a text based interface login/password screen of the present invention.

FIG. **29** is an illustration of a text-based interface group screen of the present invention.

FIG. **30** is another illustration of a text-based interface group screen of the present invention.

FIG. **31** is another illustration of a text-based interface group screen of the present invention.

FIG. **32** is an illustration of a text-based interface private message screen of the present invention.

FIG. **33** is another illustration of a text-based interface private message screen of the present invention.

FIG. **34** is another illustration of a text-based interface group with moderator screen of the present invention.

## V. DETAILED DESCRIPTION OF THE DRAWINGS

In providing a detailed description of a preferred embodiment of the present invention, reference is made to an appendix hereto, including the following items.

Appendix Contents
ALLUSER C
ALLUSER H
CHANNEL C
CHANNEL H
CHANNEL HLP
CLIST C
CLIST H
CLIST HLP
EDITUSER C
EDITUSER H
ENTRYFRM C
ENTRYFRM H
ENTRYFRM HLP
HELP C
HELP H
HELPSCR C
HELPSCR H
LINEEDIT C
LINEEDIT H
LIST C
LIST H
LOGIN HLP
MAIN C
MAKEFILE
MESSAGE C
MESSAGE H
MODERAT HLP
PRIVATE C
PRIVATE H
PRIVATE HLP
SOCKIO C
SOCKIO H
STR C
STR H
UCCLIENT
USER C
USER H
WINDOW C
WINDOW H

While platform controlled embodiments are within the scope of the invention, it is particularly advantageous to have a platform independent embodiment, i.e., an embodiment that is byte code compiled.

Referring now to FIG. **1**, the overall functioning of a computerized human communication arbitrating and distributing System **1** of the present invention is shown with odd numbers designating hardware or programmed hardware, and even numbers designating computer program logic and data flow. The System **1** includes a digital Controller Computer **3**, such as an Internet service provider-type computer. The Controller Computer **3** is operating with an operating system.

System **1** also includes a plurality of digital Participator Computers **5**, each of which may be an IBM-compatible personal computer with a processor and a DOS operating system. Each of the Participator Computers **5** includes an Input Device **7** for receiving human-input information from a respective human user. The Input Device **7** can be, for example, a keyboard, mouse or the like. Each of the Participator Computers **5** also includes an Output Device **9** for presenting information to the respective user. The Output Device **9** can be a monitor, printer (such as a dot-matrix or laser printer), or preferably both are used. Each of the Participator Computers **5** also includes a Memory **11**, such as a disk storage means.

The System **1** includes a Connection **13** located between, so as to link, the Controller Computer **3** with each of the Participator Computers **5**. The Connection **13** can be an Internet or more particularly, a World Wide Web connection.

The Controller Computer **3** is running and under the control of Controller Software **2**, which directs the Controller Computer **3** to arbitrate in accordance with predefined rules including a user identity, which ones of the Participator Computers **5** can interact in one of a plurality of groups through the Controller Computer **3** and to distribute real time data to the respective ones of the groups.

The Participator Computers **5** are each running and under the control of Participator Software **4**, which directs each of the Participator Computers **5** to handle a user Interface permitting one said user to send a multimedia information Message **8** to the Controller Computer **3**, which arbitrates which of the Participator Computers **5** receives the multimedia information Message **8** and which conveys the multimedia information Message **8** to the selected participator computers **5** to present the multimedia information Message **8** to the respective user.

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**.

Turning now to FIG. **2**, there is shown a communications overview of the present invention. Beginning with the Controller Computer Software **2**, reference is made to Block **10**, which illustrates demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **10** links to Block **12**, which is illustrative of channel A . . . Block **10** also links to Block **14**, which illustrates handling private message A. Block **10** also links to Block **16**, illustrative of handling out-of-band media. Block **10** additionally links to Block **18**, which illustrates asynchronous status messages.

Multiple connections between the controller computer **3** and a plurality of participator computers **5** permit communication implemented via the interplay of controller software **2** and participator software **4**. With particular regard to the participator software **4** illustrated in FIG. **2**, Block **20** is illustrative of demultiplexing and multiplexing operations carried out by message type on API messages of all types. Block **20** links to Block **22**, which is illustrative of channel A . . . Block **20** also links to Block **24**, which illustrates handling private message A. Block **20** also links to Block **26**, illustrative of handling out-of-band media via Block **28**, which is illustrative of a Web browser or auxiliary computer program. Block **20** also links to Block **30**, which illustrates asynchronous status message handling via Block **32**, illustrative of user interface objects windows and screens.

De/multiplexing via API provides a "virtual connection" between Channel, Private Message, and Multimedia objects in the controller computer **3** and each participator computer **5**. An alternate architecture is to allow for a separate connection between each object so that multiplexing/demultiplexing is not necessary and each object handles its own connection. This would influence system performance, however.

Turning now to FIG. **3**, a data and communications dependency diagram controller group channel structure is illustrated. Beginning from what is designated as a portion of Block **10** the logic flows to Block **34** to consider JOIN, LEAVE, STATUS, SETCHAN API instructions. Block **34** examines member list maintenance instructions, accessing Block **36** to check permissions, list users, and change attributes. Note the exploded window **38** shows a display of member information including a user's name, personal information, and attributes/properties/permissions (operations involving the subsequently discussed tokens), i.e., stored per channel attributes under each member. In any case, confirmation or denial of access is communicated via Block **40** for multiplexing return of status messages to a target object.

From the portion of Block **10**, the logic flows to Block **42** for MESSAGE and MODMSG API instructions. Block **42** tests which of the two instructions were received, and for MODMSG, the logic flows to Block **44**, which tests whether the user is a moderator. If the user is not a moderator, the logic flows to Block **46**, which sends a denial message through Block **40**. If, however, the in Block **44** the user is a moderator, the logic flows to Block **48** for a repeat to all list members who are permitted to see the message, via Block **40**.

Returning to Block **42**, if MESSAGE is detected, the logic flows to Block **50**, which tests whether a user has post permission. If the user has post permission, the logic flows to Block **48**, etc. If the user does not have post permission, the logic flows to Block **52** to forward the message to moderators for approval, via Block **40**.

Additionally, the logic flows from Block **10** to Block **54** for a URL API instruction. Block **54** tests whether the user has graphical multimedia communication privileges, and if not, the logic flows via Block **56**, which sends a denial message via Block **40**. Otherwise, if the user does have graphical multimedia communications privileges in Block **54**, Block **58** sends graphical multimedia information to all approved users via Block **40**.

Turning now to FIG. **4**, central controller loop communications is illustrated. For the data on central poll point **58** (see Appendix POLL_POINT), a "do" loop begins at Block **60** for each connection. Block **62** tests whether bytes are available on the data stream. If they are, the bytes are added to user space FIFO per connection at Block **64**, leading to Block **66**, which tests whether there are any more connections. Note that in FIG. **4**, if there are no more bytes available in Block **62**, the logic skips to Block **66**, and if Block **66** is not finished with all connections, the loop returns to Block **62**. When all connections have been completed in Block **62**, the logic flows to Block **68**, which looks for an available complete data instruction for any connection by extracting packets byte-wise from the FIFO. Thereafter, Block **70** tests whether there is a complete response available from the participator computer. If the response is complete, the logic flows to Block **72** which, using a command type, demultiplexes into an appropriate object (output FIFOs may be filled here for any connection). The logic from Block **72** joins the "no" branch from Block **70** at Block **74**, which enables unblocking for writing connections for only connections with data available to write, looping back to Block **58**.

FIG. **5** shows a client channel data structure and information flow diagram. From a message that is demultiplexed by message type, there are six possibilities: ERROR MESSAGE, MESSAGE, STATUS, JOINCHANNEL, LEAVECHANNEL, and MODMSG. ERROR MESSAGE is communicated to Block **76**, where the error message is displayed to the transcript in the transcript area of Block **78**. MESSAGE is communicated to Block **80** where the message is immediately added to the transcript in transcript area **78**. STATUS is communicated to Block **82** to update user data structure; JOINCHANNEL is communicated to Block **84** to add a user from the member list and display the change; and LEAVECHANNEL is communicated to Block **86**. From Block **82**, Block **84**, and Block **86**, the logic flows to Block **88**, which includes a member list, a member identifier, known attributes/permissions/properties, and personal information. From Block **88**, the logic proceeds to Block **90**, a member list area, and on to Block **92** to compose a request to change a member attribute. This "SETCHAN request is then communicated to Block **94**, which is the multiplexer leading to the controller computer connection.

MODMSG is communicated to Block **96**, which sends the message to the moderation area of Block **98**, and then to Block **100** to resubmit a member message as approved, thereby conveying a MODMSG request to Block **94**.

Note that a response is prepared in the response area of Block **102**. If the response is a standard message, it is conveyed to Block **104** to compose the response into a controller message, thereby sending a MESSAGE request to box **94**. If, however, the message is a graphical information submission, the logic flows from Block **102** to Block **106** to compose the graphical information submission into a controller message, thereby sending a URL request to Block **94**.

FIG. **6** is a participator software out-of-band multimedia information flow diagram, which begins with Block **26**, the multimedia type patch point. Block **26** leads to Block **102**, which tests whether there is an internally handlable multimedia type. If not, Block **104** looks up a suitable agent for data type presentation, which leads to Block **106**, which tests whether an agent was found. If not, Block **108** reports location of data to the user for future referencing. If the agent is found in Block **106**, the logic flows to Block **110**, which invokes the agent with a data reference to present the data.

If the multimedia type is internally handlable from Block **102**, the logic flows to Block **112**, which tests whether this is a member associated image. If it is a member associated image, Block **114** displays the image next to member identity information, and if it is not, the logic flows to Block **116**, which tests if this is a member public data reference (e.g., a URL). 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).

With further regard to the manner of interaction between the controller computer **3** and the participator computers **5**, and their respective computer programs **2** and **4**, includes a moderation capability that is controlled, or arbitrated, pursuant to system **1** recognizing user identity. Note that using the user identity for moderation purposes is a use additional to the use of the user identity for security purposes.

One embodiment of the present invention is to bring chat capability to the internet and World Wide Web. However, another embodiment involves non-internet relay chat. In either embodiment, System **1** is state driven such that synchronous and asynchronous messages can be communicated. For an asynchronous notification, each message is sent through the system **1** (API), which updates the information on the output device of the participator computers **5**. For a synchronous notification, a participator computer **5** must interrogate the system **1** for a message.

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 in a control computer base, along with personal information about the user, such as the user's age. The control computer database serves as a repository of tokens for other programs to access, thereby affording information to otherwise independent computer systems. In the database, the storage of tokens can be by user, group, and content, and distribution controls can also be placed on the user's tokens as well as the database.

Each token is used to control the ability of a user to gain access to other tokens in a token hierarchy arbitration process. The arbitration also includes controlling a user's ability to moderate communications involving a group or subgroup of the participator computers **5**. Once in a group, temporary tokens are assigned for priority to moderate/submoderate groups (a group is sometimes known as a channel in multiplexing terminology).

Accordingly, tokens are used by the controller computer **5** to control a user's group priority and moderation privileges, as well as controlling who joins the group, who leaves the group, and the visibility of members in the group. Visibility refers to whether a user is allowed to know another user is in the chat group.

Tokens are also used 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.

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

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

With regard to controlling communications in a group (which is in essence a collection of user identities), control extends to seeing messages, seeing the user, regulating the size of the communication, as well as the ability to see and write to a specific user. Control further extends to the ability to send multimedia messages.

Note that tokens for members in group can involve multiples formed in real time, say, within the span of a conversation. For example, for private communication, tokens are immediately formed to define a group of 2 users. Hierarchical groups within groups can also be formed, with each inheriting the properties of the group before it. Thus, a subgroup can include up to all members or more by adding any surplus to the former group.

With further regard to the controller computer **3**, e.g., a server, information is controlled for distribution to the user interfaces at selected ones of the participator computers **5**. The controller computer program, in one embodiment, can be a resident program interface (such as a JAVA application). There can be a token editor object (window/tear down, etc.) per group, private communication, user, channel listings, user listings, etc. Each can link up in a token hierarchy for arbitration control.

The controller computer **3**, by means of the controller computer program **2**, keeps track of states and asynchronous messages as well as generating a synchronous message as a user logs in or interrogates system **1**.

With regard to multimedia information messages **8**, such messages are of independent data types, e.g., audio/video data types. The content of the message (e.g., a URL) permits the System **1** to automatically determine the handling of the message: either the Controller Computer **3** passes the content of Message **8** directly, or the Controller Computer **3** determines from the Message **8** how to find the content, say via Netscape. Accordingly, Message **8** can communicate video and sound (or other multimedia, e.g., a URL) to users, subject only to the server arbitration controls over what can be sent.

Turning now to an illustration of using the invention, the session starts with verifying the user's identity (at FIG. **7**). The login/password screen is shown, and the user enters his/her assigned login/password combination and clicks the "Login To Chat" button. If the password was entered correctly, a confirmation box appears on the screen.

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

To create a new group, the "New Channel" option is selected from a pull-down menu (at FIG. **9**). The name of the channel is entered by the input device **7**.

If the user has permission (this one does), a new channel is created for the group (at FIG. **10**). The window that displays the channel area has three regions: the bottom region, where responses are entered; the largest region, where a transcript of the communication is followed; and the rightmost region, which lists the group's current members. This list is continuously updated with asynchronously generated status messages received immediately when a new member joins the group. Only "DMARKS" is currently in this group. The "MWU" is the properties currently associated with DMARKS—the ability to moderate, write to the channel, and send multimedia messages.

A new member has joined the channel, and the member list status area is updated right away (at FIG. **11**). This new member has a login of "ME."

The user DMARKS now types "hello there" into the response area and presses RETURN (at FIG. **12**). This message is passed to the controller computer **5**, which sends the message to all channel members, i.e., those using participator computers **5**, including DMARKS.

The user ME now sends a message to the controller: "hi there" (at FIG. **13**). This message is also sent to all members by the controller computer **5**. Now user DMARKS clicks (using input device **7**, a mouse) on the name of the user "ME" in the member list window. The participator software **4** will now create a private message window, so that the users ME and DMARKS can exchange private messages. Private messages are only sent to the intended recipient by the controller, and no one else.

A private message window appears in response to DMARKS's request to open private communications with ME (at FIG. **14**). Now DMARKS types a message into the private message window's response area to ME: "this message is seen only by the user ME." When complete, the participator software **4** will forward this message to the controller computer **3**.

In response, the user ME has entered "This is the private message response that is only seen by the user DMARKS." which has been forwarded to user DMARKS (at FIG. **15**). This message is displayed immediately on DMARKS's window.

DMARKS now returns to the channel window for the group "TESTCHANNEL" (at FIG. **16**). To modify the permission attributes associated with user ME on the channel TEST CHANNEL, DMARKS (who is a moderator of the channel), clicks on the user ME in the member list to select ME, pulls down the Moderator menu, and selects "Toggle Moderator." This removes the moderator privileges from ME.

As a result of the attribute revocation, the "M" has disappeared from next to ME's name in the member list (at FIG. **17**), indicating that the property is no longer associated with the user ME.

Now DMARKS returns to the Channel List window (at FIG. **18**). DMARKS wishes to fully moderate the contents of the channel TESTCHANNEL, censoring all unwanted communications to the channel. DMARKS returns to the channel list, and selects the channel TESTCHANNEL by clicking on its name in the channel list.

Now DMARKS selects the "Toggle All Posting" option in the Maintenance pull-down menu (at FIG. **19**). This will turn off the channel property "posting," (or sending communications to the channel without moderator approval) which will be indicated by the removal of the letter "P" from next to the name TESTCHANNEL (at FIG. **20**).

Now the letter "P" is removed from after the name TESTCHANNEL in the Channel List window (at FIG. **21**), indicating that this channel is now moderated and will only have free posting ability by designated members.

Now, type user ME (who is also on channel TESTCHANNEL) wishes to send communications: "this will not be written directly to the channel" (at FIG. **22**). The controller, instead of sending it immediately to the channel to be seen by all members, will instead forward the message to the moderators for approval. The moderator, DMARKS, will then see the message on the Moderation Window, which provides a preview of any messages to be sent. To approve a message for general viewing, DMARKS now clicks on the message.

Now that DMARKS has clicked directly on the message, it is displayed inside the group's Channel window for all members to see (at FIG. **23**).

DMARKS now wishes to send a graphical multimedia message. This implementation sends graphical multimedia images by allowing a channel member to specify an Internet URL of a graphical multimedia resource to be presented to the group members. In this example, DMARKS wishes to the URL corresponding to the World Wide Web home page of American Information Systems, Inc. to the channel members. DMARKS enters the URL into the response window, and selects "Send URL" from the Moderator pull-down menu (at FIG. **24**).

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 NavigatorÔ, 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.

Finally, DMARKS wishes to manually modify the attribute tokens associated with the user (at FIG. **27**). The user invokes the Property Editor dialog, which allows the user to view and change the tokens associated with a user. A property of a given user is determined by the Identifier and Property names. An old value of the property is shown, and a token value can be changed in the "New Value" field. With this property editor, a user with sufficient permissions (tokens) can change any of the tokens or security parameters of any user, or a user's ability to change security parameters can be restricted.

To start with an alternate embodiment using a text-based interface, a user is presented by the login/password screen (at FIG. **28**). This screen is where a user enters the information that proves his/her identity. The user must now enter his/her login and password to identify themselves.

After the user has been identified by the controller the Channel List screen appears (at FIG. **29**). The names of channels and their associated properties are shown on this screen. By using the arrow keys and highlighting the desired channel, ME may enter any publicly joinable group. Currently, there is only one group TESTCHANNEL, which ME will join.

Now the screen for the channel TESTCHANNEL appears (at FIG. **29**). The screen is split into four regions. The bottom left region is the response line, where messages users wish to enter appear. The upper left region is the transcript area where the communications of the group's channel appear as they occur. The upper right region is the Member List region, where a continuously updated list of members' names appear, with their attributes.

A message appears in the transcript area. The controller has forwarded a message to the group from DMARKS, "hello there" (at FIG. **31**), which is seen by all members of the group, including ME. Now ME will respond, by entering "hi there" into the response area.

When ME is finished entering his response, the participator software forwards the response to the controller, which sends it to the members of the channel. In the transcript area, the participator software notifies the user that it has received a private message from DMARKS, which is waiting inside the private message screen. To see the private message, ME presses the private message screen hot key.

A private message screen appears (at FIG. **32**), and the private message from DMARKS is at the bottom of the transcript area. Now to reply, ME types his response into the response area.

Now ME will return to the screen for the channel TESTCHANNEL. The member list area has changed because DMARKS has revoked ME's moderator permission. ME is no longer permitted to see the permissions of other users, so this information has been removed from his display (at FIG. **33**). The only information he can see now is who is moderator (at FIG. **34**). A "*" next to the identifier of a member of the group indicates the member is a moderator of the group. ME is no longer a moderator, and therefore a "*" does not appear the identifier ME.

To further exemplify the use of the present invention, the following is a transcript of communications produced in accordance herewith.

POWERQUALITY JOHNMUNG: unclear about meaning of "first contingency"
POWERQUALITY SAM: mike, that is correct on IEEE 519
POWERQUALITY SKLEIN: In assessing network security (against outage) the first contingencies are tested to see how the power system should be reconfigured to avoid getting a second contingency and cascading into an outage.
POWERQUALITY MSTEARS: These outages point out the need for reliability as part of the overall customer picture of PQ
POWERQUALITY BRIAN: Hi Jennifer, hit crt-p for private message
POWERQUALITY SKLEIN: In simpler terms, a single point failure shouldn't crash the system.
POWERQUALITY SKLEIN: Are we all chatted out?
POWERQUALITY ANDYV: brian, johnmung has been banned!!! why?
POWERQUALITY BRIAN: no way, new subject
POWERQUALITY BRIAN: just a sec, andy
POWERQUALITY BRIAN: No banning on this channel, John is back on
POWERQUALITY TKEY: ieee 519 limits the harmonic current a customer can inject back into the pcc and limit the vthd the utility provides at the PCC
POWERQUALITY JOHNMUNG: thanks guys, for unbanning me—i've been thrown out of better places than this!
POWERQUALITY BRIAN: New subject . . . now . . .
POWERQUALITY BRIAN: good one john . . . :)
POWERQUALITY MSTEARS: For critical facilities dual feeds or other backup capability need to be economically evaluated to keep the facility in operation
POWERQUALITY SAM: John, I remember that club very well

POWERQUALITY JOHNMUNG: question: please comment on frequency of complaints involving spikes, sags or harmonics
POWERQUALITY WARD: Problems caused by sags is the main complaint.
POWERQUALITY BRIAN: What subject does anyone want to see the next chat
POWERQUALITY WARD: Surges is probably next; harmonics really don't cause that many problems, although they are certainly there.
POWERQUALITY ANDYV: what is the solution ward?
POWERQUALITY TKEY: Agree they are the most frequent (sags) and the panel session on the cost of voltage sags at PES drew **110** people
POWERQUALITY SAM: harmonics tend to be an interior problem within a facility, rather than on the distribution system
POWERQUALITY WARD: The best solution is making the equipment less susceptible to sags. This requires working with the manufacturers.
POWERQUALITY ANDYV: won't that cost more
POWERQUALITY MSTEARS: The complaint of surges covers many things in the customers eyes sags have become a real problem because they are harder to resolve
POWERQUALITY GRAVELY: John—The latest EPRI results confirms the 90+ % of the time SGS are the problem and short term ones.
POWERQUALITY WINDSONG: What is the topic for the 25??
POWERQUALITY WARD: Each problem can be dealt with as it occurs, but the time involved gets very expensive.
POWERQUALITY JOHNMUNG: making equipment less susceptible causes legal problems for manufacturers—as each improvement can be cited by compinant as example of malfeasance
POWERQUALITY WARD: AndyV: The cost to the manufacturer increases. The overall cost to everyone involved decreases.
POWERQUALITY TKEY: customer pays any way you cut it, if the eqpt is more immune customers pay only once instead of every time the process fails
POWERQUALITY BRIAN: The topic is regarding Power Quality
POWERQUALITY BRIAN: This chat is available for everyone 24 hours a day
POWERQUALITY ANDYV: ddorr>>will the manufacturer spend more to produce a better product
POWERQUALITY WARD: And as Tom says, the cost to the customer is far less.
POWERQUALITY BRIAN: This chat will be functioning 24 hrs/day
POWERQUALITY BRIAN: please usae it
POWERQUALITY BRIAN: The next panel discussion is Nov 15th
POWERQUALITY WARD: Andy, that's where standards come in.
POWERQUALITY SKLEIN: Is the customer capable of resolving the fingerpointing among the manufacturers and utilities?
POWERQUALITY DDORR: andy, only if the end users create a market for pq compatible eqpt by demanding better products
POWERQUALITY MSTEARS: The manufacturers problems in including fixes is being competative with some who doesn't provide the fix
POWERQUALITY ANDYV: how will we educate the general consumer?

POWERQUALITY GRAVELY: Is it possible to have a basic theme topic or some core questions for 15 Nov chat?

POWERQUALITY WARD: Stan, the customer cannot be expected to resolve the fingerpointing. The manufacturers and utilities need to work together.

POWERQUALITY ANDYV: about power quality and reliability?

POWERQUALITY SKLEIN: If electric power is going to be treated as a fungible commodity, there has to be a definition. Like, everyone knows what number 2 heating oil is.

POWERQUALITY SAM: Ideally a manufacturer would not be able to compete if they don't add the protective function in their products, but alot more public education is required before we get to this point.

POWERQUALITY WARD: Andy, there are many ways to educate the customers, but they require a lot of contact between the utility and the customers. The Western Resources Power Technology Center in Wichita is doing it, just as an example.

POWERQUALITY DDORR: standard power vs premium power is one solution as is std qpt vs Pq compatible eqpt

POWERQUALITY SKLEIN: I want to buy number 2 electric power and to be able to check the nameplates of my appliances to be sure they can take it. Just like I buy regular gasoline.

POWERQUALITY MSTEARS: Sam I agree, that is partly the utilities responsibilitysince we serve the customers

POWERQUALITY BBOYER: What differentiates number 2 from number 1?

POWERQUALITY SKLEIN: I used the analogy of number 2 heating oil. I don't know what number 1 heating oil is.

POWERQUALITY DDORR: Number two has cap switching and all the normal utility operational events while number one is much better

POWERQUALITY SKLEIN: Perhaps we can just say regular vs high test.

POWERQUALITY SAM: mike, yes a joint effort between the utility, manufacturer and standards jurisdictions is a goal for utilicorp as we move forward with offering from our strategic marketing partners, and bring PQ technologies to the public

POWERQUALITY TKEY: We are finding that many mfgrs want to produce pq compatible equipment, but they have no clue as to what to test for

POWERQUALITY ANDYV: Tom>>will the IEC standards help?

POWERQUALITY TKEY: Its up to the utility to help define normal events IEC will take time

POWERQUALITY SKLEIN: You can't have a commodity product with all the variation in specifications we have been discussing. It has to be regular, premium, and super premium or it won't work.

POWERQUALITY JOHNMUNG: Tom as a former manufacturer i sympathize—your work at PEAC is invaluable but anecdotal knowledge from utility people on the firing line is equally important

POWERQUALITY TKEY: Super premium, does that mean a UPS?

POWERQUALITY ANDYV: how do you stop a facility from affecting you super-premium power?

POWERQUALITY TKEY: John, Good Point

POWERQUALITY SAM: Tkey, a ups, local generation or redundant service

POWERQUALITY SKLEIN: This is what I meant earlier by electricity being a non-virtualizable service. You can't make each customer see the power system as though they had their own dedicated generating plant.

POWERQUALITY BRIAN: THE CHAT CHANNEL WILL BE OPEN 24/HRS/DAY 7 DAYS A WEEK

POWERQUALITY TKEY: I must sign out for about 5 minutes but I'll be back

POWERQUALITY BRIAN: OK TOM

POWERQUALITY MSTEARS: PQ for facilities need to be done with a system perspective to to get the right resolution

POWERQUALITY BBOYER: Andy's question is still relevant—how do stop a facility from downgrading utility service to other customers?

POWERQUALITY BRIAN: MIKE>>LETS SWITCH BACK TO RETAIL WHEELING POWERQUALITY WARD: You work with that customer to do whatever is needed to correct their disturbances.

POWERQUALITY BBOYER: Be more specific

POWERQUALITY MSTEARS: Interaction between facilites can be evaluated and designed for

POWERQUALITY JOHNMUNG: as a key to hardening it helps to identify the most sensitive circuits, i.e. microprocessor logic, test for vulnerability under common surges, sags, rfi, and then notify users that their equipment contains these subsystems—for a start

POWERQUALITY BRIAN: hI DOUG

POWERQUALITY GRAVELY: Brian: Are you saving this session as a file? Can we get a list of chat session participants?

POWERQUALITY BRIAN: s, we may

POWERQUALITY DMARKS: gravely: hit TAB and use the arrow keys to page through the list of participants

POWERQUALITY SKLEIN: Will the session be available for downloading?

POWERQUALITY BRIAN: yes, Mike we will publish in PQ Magazine

POWERQUALITY WARD: Part of the agreement for high quality power should be that the customer receiving the power will not disturb the utility system.

POWERQUALITY BRIAN: if john let's us . . .

POWERQUALITY GRAVELY: I tried that, however, netcruiser has a software problem and I cannot see all of the names.

POWERQUALITY SAM: most utilities rules and regulations already require that a customer not put anything back out on the utility system

POWERQUALITY BRIAN: MIKE G.>>WE WILL PUBLISH THIS IN PQ MAG NEXT MONTH IF ASNDY LETS US

POWERQUALITY BRIAN: HOW ABOUT IT ANDY?

POWERQUALITY ANDYV: ok

POWERQUALITY BRIAN: COOL

POWERQUALITY WARD: Standards will have to be set for what constitutes a disturbance, and then the utility should work with customers, install filters, etc., to be sure they stay within the rules.

POWERQUALITY BRIAN: THANKS ANDY

POWERQUALITY ANDYV: a meeting review or a summary of events

POWERQUALITY GRAVELY: It would be good to take a few minutes to recommend how the 15 Nov session could be more effective.

POWERQUALITY BRIAN: A SYNAPSE OF THIS CHAT WILL BE IN NEXT MONTHS PQ MAG

POWERQUALITY WINDSONG:

POWERQUALITY SKLEIN: I don't get PQ mag. Will it be on the Net?

POWERQUALITY BRIAN: STAN SIGN UP FOR IT ON OUR HOME PAGE

POWERQUALITY DOUGC: the transcript of this conference will be available on the EnergyOne pages.

POWERQUALITY BRIAN: YOU CAN SIGN UP ON LINE

POWERQUALITY BRIAN: HTTP://WWW.UTILICORP.COM

POWERQUALITY WINDSONG: Good comment Gravely Comments from the users would be greatly appreciated!!

POWERQUALITY SAM: PQ magazine is available online on the UCU internet bulletin board, http://www.utilicorp.com

POWERQUALITY ANDYV: or link from powerquality.com

POWERQUALITY BRIAN: YOU CAN GET A FREE MAG SUBSCRIPTION FROM UTILICORP'S HOME PAGE

POWERQUALITY SKLEIN: Thanks

POWERQUALITY BRIAN: ALSO, THERE IS A PQ FORUM ON OUR HOME PAGE

POWERQUALITY JOHNMUNG: for nov 15 shall we pick five key topics? suggest health care, energy storage rfi/emc as a few topics—also new gas turbine 25 kw generator just announce today—just some suggestions

POWERQUALITY BRIAN: GOOD SUGGESTION JOHN

POWERQUALITY ANDYV: lets develop an outline of topics for next time.

POWERQUALITY BRIAN: OK

POWERQUALITY GRAVELY: One suggestion for 15 Nov—Have participants place a list of desired topics on your other chat box and prioritize by interest level.

POWERQUALITY SKLEIN: How about deregulation and retail wheeling.

POWERQUALITY BRIAN: COMMENTS SHOULD BE SENT TO ME BY EMAIL POWERQUALITY BRIAN: BSPENCER@UTILICORP.COM POWERQUALITY BRIAN: 15 minutes remaining

POWERQUALITY ANDYZYREK: Let's discuss the new standard IEEE 1159.

POWERQUALITY ANDYV: may be we could generate an online questionaire to see what people are needing discussed.

POWERQUALITY BRIAN: but the chat is available for 24 hrs/day 7 days a week

POWERQUALITY ANDYV: what does IEEE1159 address?

POWERQUALITY BRIAN: Please send all suggestion to me for our next chat

POWERQUALITY BRIAN: Bobbin is not banned now

POWERQUALITY BRIAN: my fault

POWERQUALITY ANDYZYREK: New PQ measuring techniques. We have not received our issue yet.

POWERQUALITY ANDYV: You should have it my now.

POWERQUALITY BRIAN: Bobbin is not banned anymore

POWERQUALITY ANDYV: you can e-mail me or john at: editors@powerquality.com

POWERQUALITY BRIAN: is two hours right fdo rhtis feature

POWERQUALITY JOHNMUNG: do i understand that many programmable logic controllers can be hardened by addition of simple CVT like a sola?

POWERQUALITY ANDYZYREK: Yes, but it is being delivered by snail mail.

POWERQUALITY ANDYV: no 2nd class

POWERQUALITY BRIAN: 15 minutes to go

POWERQUALITY ANDYV: Please e-mail me you complete name and addess and I will mail you one today 1st class . . . now is that serice or what?

POWERQUALITY BRIAN: Is two hours long enough for tthis chat?

POWERQUALITY TKEY: Im back

POWERQUALITY WARD: Brian, I think two hours is about right.

POWERQUALITY BRIAN: hi tom

POWERQUALITY BRIAN: good . . .

POWERQUALITY ANDYV: yes I agree 2 hrs

POWERQUALITY BRIAN: anyone else

POWERQUALITY ANDYV: it the time of day correct?

POWERQUALITY BRIAN: questions now . . .

POWERQUALITY SKLEIN: The topic foremost in my mind right now is what to eat for lunch. I enjoyed the discussion, which I understand has been historic in some sense. But I think I will sign off now and go eat.

POWERQUALITY SAM: 2 hours seems to work very well

POWERQUALITY DANIELH: time of day is good

POWERQUALITY BILLMANN: 2 hrs is fine

POWERQUALITY MSTEARS: Two hours work well, the middle of the day allows east and west coast to be involved

POWERQUALITY BRIAN: good, Will everyone be back for the next chat

POWERQUALITY GRAVELY: Brian, I will forward my recommendations on email, thanks.

POWERQUALITY BILLMANN: yes i'll be back

POWERQUALITY ANDYZYREK: Brian, would it be possible to have a forum published on your home page prior to Nov 15.

POWERQUALITY BRIAN: I would like to do another chat before Nov 15th, any thoughts

POWERQUALITY ANDY: U bet

POWERQUALITY SAM: I believe that this chat may set an attendance record for most participants during a first session

POWERQUALITY JOHNMUNG: a parting thought "harmonics make the music rich, they make the tone insprinng—harmonics in your power line WILL BLOW THE BUILDINGS WIRING" tIM MUNGENAST

POWERQUALITY BRIAN: Your're all invited to return

POWERQUALITY BRIAN: the next chat

POWERQUALITY BRIAN: This chat feature will help set standards of how we view our industry

POWERQUALITY WARD: For me this was two hours very well spent, and it was quite enjoyable.

POWERQUALITY BRIAN: Tell a colleague about our chat Nov 15th

POWERQUALITY BRIAN: Thanks Ward

POWERQUALITY BRIAN: I would like to do this on a weekly basis, any thoughts yet

POWERQUALITY GRAVELY: John: talk it up in Germany!!

POWERQUALITY ANDY: I would like to thank utilicorp and everyone envolved.

POWERQUALITY BRIAN: Thanks Andy for your help

POWERQUALITY WARD: Did this notice go out to the Power Globe mailing list?

POWERQUALITY BRIAN: No, but could help us Ward with that

POWERQUALITY BRIAN: Lets all get the word out about this chat

POWERQUALITY WARD: I'm on the list and will be glad to forward anything you wish to it.

POWERQUALITY BRIAN: Please use it whenver you wish, even schedule your own chats whenver

POWERQUALITY JOHNMUNG: MANY THANKS TO uTILICORP AND ALL INVOLVED—FROM AN OLD STEAM BOATER :-)

POWERQUALITY BRIAN: thanks ward

POWERQUALITY BRIAN: Hi duane

POWERQUALITY BRIAN: This chat is offically over, but do stick around for foir more chatting

POWERQUALITY BRIAN: Thanks to all, cya on Nov 15th

POWERQUALITY MSTEARS: Ward, Tom, and John I appreciate your participation

POWERQUALITY BRIAN: Thanks Guys and Ladies!!!!!!!!!!

POWERQUALITY SWPPD: WHAT IS HAPPENING ON NOV. 15
POWERQUALITY BRIAN: our next chat with a panel of experts
POWERQUALITY BRIAN: topic yet to be decided
POWERQUALITY DPSWOBO: Hi Brian, Sorry I was on the phone and could not respond right away. Did I get the time incorrectly for the chat?
POWERQUALITY BRIAN: please send us a suggestions
POWERQUALITY ANDY: good bye ;-)
POWERQUALITY BRIAN: Yeah, but stick around to chat with some friends
POWERQUALITY BRIAN: We had a total of 50 people and avg of 20 people at one time
POWERQUALITY BRIAN: Thanks everyone!!! Lunch Time
POWERQUALITY BRIAN: Next Chat Nov 15th at 10-12 ct
POWERQUALITY BRIAN: But this chat line is available 24 hrs/day/7 days a week
POWERQUALITY BRIAN: Please use it whenever
POWERQUALITY GRAVELY: Thanks to the panel and Utilicorp for the session!
POWERQUALITY BRIAN: Talk to your collegues and friends about any particular topic
POWERQUALITY BRIAN: Come see our home page for new topics and chats
POWERQUALITY BRIAN: http://www.utilicorp.com
POWERQUALITY BRIAN: Thanks Power Quality Assurance Magazine and All our panel members
POWERQUALITY BRIAN: :)
POWERQUALITY SWPPD: MISSED THIS SESSION. ICAN WE GET HARD COPY INFO?
POWERQUALITY BRIAN: yes swwp, it will be published in pq mag and our home page
POWERQUALITY BRIAN: catch our next session on nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY SWPPD: THANKS A BUNCH!!
POWERQUALITY SWPPD: GOOD BYE!
POWERQUALITY BRIAN: no prob
POWERQUALITY BRIAN: cya
POWERQUALITY DESWETT:
POWERQUALITY TKEY: Good session brian, ddorr and I will be signing off now, look forward to the next session
POWERQUALITY DPSWOBO: Thanks for the info on the next session, we will get on next time
POWERQUALITY DMARKS: I hope everyone enjoyed this session.
POWERQUALITY MSTEARS: I am logging off Thanks
POWERQUALITY SAM: This is Tony and I am watching the action . . . we made history. Great work guys.
POWERQUALITY BRIAN: Lunch time
POWERQUALITY BRIAN: Next chat is nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: please continuie to look at utilicorp's hp
POWERQUALITY BRIAN: for more info
POWERQUALITY BRIAN: email if you have any questions regarding the chat
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: later
SUPPORT BRIAN: hi guys
SUPPORT BRIAN: success
SUPPORT BRIAN: yess!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
SUPPORT BRIAN: thanks for the help
SUPPORT BRIAN: cya

POWERQUALITY BRIAN: next chat on Nov 15th
POWERQUALITY BRIAN: 10-12 ct
POWERQUALITY BRIAN: any suggestion on topics please contact me by email
POWERQUALITY BRIAN: bspencer@utilicorp.com
POWERQUALITY BRIAN: hi chuck
POWERQUALITY BRIAN: hi randy
POWERQUALITY CPREECS: hello brian
POWERQUALITY BRIAN: How are you chuck
POWERQUALITY CPREECS: how has the participation been?
POWERQUALITY BRIAN: I am sorry you missed the offical chat, but do come back at any time for some chatting
POWERQUALITY BRIAN: great 20 people avg. 50 total people
POWERQUALITY CPREECS: ? yes, i got some conflicting info
POWERQUALITY BRIAN: transcripts will be in PQ mag next month and on utilicorp's home page
POWERQUALITY CPREECS: what were the topics discussed?
POWERQUALITY BRIAN: how is that chuck
POWERQUALITY BRIAN: power quality, standards,
POWERQUALITY BRIAN: retail wheeling
POWERQUALITY BRIAN: cya, lunch time
POWERQUALITY CPREECS: later
POWERQUALITY BRIAN: bye all
POWERQUALITY BRIAN: email me chuck
POWERQUALITY RB: sorry I missed it. I got 12-2 est off the net. bye.
POWERQUALITY BRIAN: sorry RB
POWERQUALITY BRIAN: miss information
POWERQUALITY BRIAN: next chat is 10-12
POWERQUALITY BRIAN: ct
POWERQUALITY BRIAN: nov 15th
POWERQUALITY BRIAN: bye
POWERQUALITY RB: thanks
POWERQUALITY BRIAN: no prob, tell all
POWERQUALITY ANDY: Is anyone still here talking about power quality?
POWERQUALITY DAVE: Just signed on that is what I was trying to find out
POWERQUALITY ANDY: the PQ chat was running from 11:00-1:00 est
POWERQUALITY ANDY: Were you involved then?
POWERQUALITY DAVE: No I just got a chance to sign on now
POWERQUALITY ANDY: there were some great discussions.
POWERQUALITY ANDY: The transcripts will be available to down load at utilicorp.com Brian Spencer says.
POWERQUALITY ANDY: What is your experience in PQ
POWERQUALITY DAVE: That is what I was looking for, are they available to down load now, I work in a data center and have worked with UPS systems for about 12 years
POWERQUALITY DAVE: I did field service for Exide
POWERQUALITY ANDY: Brian just went to Lunch in KS I don/t know when it will availalbe.
POWERQUALITY DAVE: Thanks for the Info on the downloads, I hope they do this again
POWERQUALITY ANDY: so do I.
POWERQUALITY DAVE: What is your experience on PQ
POWERQUALITY ANDY: I am the editor or Power quality mag.
POWERQUALITY DAVE: Good mag., I pick up alot in it
POWERQUALITY ANDY: do your receive power quality assurance magazine?

POWERQUALITY ANDY: great glad to hear it.
POWERQUALITY DAVE: We get it at work but I have asked to have it sent to my home
POWERQUALITY ANDY: did you get the latest issue witht the lighting on the cover?
POWERQUALITY DAVE: Not yet, have seen it on line though
POWERQUALITY ANDY: great.
POWERQUALITY ANDY: any suggestion for editorial?
POWERQUALITY DAVE:
POWERQUALITY DAVE: no it is good
POWERQUALITY ANDY: ok.
POWERQUALITY ANDY: I am currently editing an article about VRLA battery charging.
POWERQUALITY DAVE: I am working on a resonant problem with Utility and was looking for info
POWERQUALITY ANDY: explain
POWERQUALITY ANDY: by the way my e-mail is andy@powerquality.com
POWERQUALITY DAVE: we are running a lot of 5th har. across our system in a large data center
POWERQUALITY ANDY: I see
POWERQUALITY ANDY: I will try to address this in an upcomming issue. may be march/april or even sooner.
POWERQUALITY DAVE: we have 4800 kw of UPS cap on two transformers and we have alot of 5th on our other boards
POWERQUALITY ANDY: If you are interested in writing up a case history including you solutions I would like to review it and poss. publish
POWERQUALITY MSTONEHAM: Is this chat session still active?
POWERQUALITY ANDY: YES
POWERQUALITY ANDY: We can'nt get enough! ! !
POWERQUALITY DAVE: when we can get it fixed, It looks like we have a problem with input filtering on a couple of UPS,s
POWERQUALITY ANDY: input fro the utility or a generator?
POWERQUALITY DAVE: utility
POWERQUALITY MSTONEHAM: I understand there was a chat session earlier today with some guest "chatters". Is there an archive of the discussion since I missed it?
POWERQUALITY DAVE: we have 66 kv to 12 kv then to 480 v by 4 trans on property
POWERQUALITY ANDY: What are you leaning towards in a solution dave
POWERQUALITY ANDY: MTONEHAM>>yes but I don't know when. contact BSPENCER@utilicorp.com
POWERQUALITY DAVE: the computer seem to have no problem, but we have alot of motor heating/bad PF
POWERQUALITY MSTONEHAM: Thanks!
POWERQUALITY DAVE: we currently are working with a consulant but I am looking for more info
POWERQUALITY ANDY: will capacitors solve your ptoblem
POWERQUALITY ANDY:
POWERQUALITY ANDY: there also is a forum under utilicorp.com where you can post you questions.
POWERQUALITY DAVE: Each 600 kw UPS has Input filtering/may need trap for 5th
POWERQUALITY ANDY: or you can access it form powerquality.com
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: Talk to ya later dave
POWERQUALITY DAVE: is PQ.com your Mag
POWERQUALITY ANDY: bye
POWERQUALITY DAVE: bye
POWERQUALITY ANDY: yes
POWERQUALITY DAVE: thanks
POWERQUALITY ANDY: :-)
POWERQUALITY MSTONEHAM:
POWERQUALITY MSTONEHAM: Is anyone else hear? There doesn't seem to be much traffic.
POWERQUALITY MSTONEHAM:
POWERQUALITY CILCOJRG: Hello—is the conference over?
POWERQUALITY CILCOJRG:
POWERQUALITY CILCOJRG: hello
POWERQUALITY BRIAN: yes
POWERQUALITY BRIAN: the conference was from 10-12 ct
POWERQUALITY BRIAN: someone gave out the wrong information
POWERQUALITY BRIAN: hello cilco
POWERQUALITY BRIAN: anyone still there
SUPPORT BRIAN: hi all
SUPPORT BRIAN: anyone there
POWERQUALITY BRIAN: jenny>>are you there
POWERQUALITY CJBOUTCHER: is anyone here a utility employee?
POWERQUALITY BRIAN: Hi chris
POWERQUALITY BRIAN: how are you?
POWERQUALITY CJBOUTCHER: hi brian it is quiet in here
POWERQUALITY BRIAN: the conference was at 10:00 ct
POWERQUALITY CJBOUTCHER: ah I see
POWERQUALITY CJBOUTCHER: when is the next one?
POWERQUALITY BRIAN: nov 15th
POWERQUALITY BRIAN: 10-12
POWERQUALITY BRIAN: ct
POWERQUALITY CJBOUTCHER: is the channel open at other times?
POWERQUALITY BRIAN: yes 24 hours a dfay
POWERQUALITY CJBOUTCHER: but not much discussion?
POWERQUALITY BRIAN: not right now,
POWERQUALITY BRIAN: cya
POWERQUALITY CJBOUTCHER: bye
POWERQUALITY BRIAN: hi jenny
POWERQUALITY JOSH: hello?
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: hi dan
POWERQUALITY BRIAN: are you awake yet?
POWERQUALITY BRIAN: just giving present this a.m.
POWERQUALITY BRIAN: :)
POWERQUALITY BRIAN: who is guest96
POWERQUALITY GUEST96: test

While a particular embodiment of the present invention has been disclosed, it is to be understood that various different modifications are possible and are within the true spirit of the invention, the scope of which is to be determined with reference to the claims set forth below. There is no intention, therefore, to limit the invention to the exact disclosure presented herein as a teaching of one embodiment of the invention.

I claim:

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

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

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

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

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

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

if the first user identity is censored from the receiving of the data, not allowing the data that is censored to be presented from the second participator computer to the output device.

**2**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer.

**3**. The method of claim **2**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**4**. The method of claim **3**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**5**. The method of claim **2**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**6**. The method of claim **5**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**7**. The method of claim **2**, further including determining whether at least one of the communications is censored based on content.

**8**. The method of claim **7**, further including determining a user age corresponding to each of the user identities.

**9**. The method of claim **8**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**10**. The method of claim **7**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**11**. The method of claim **2**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**12**. The method of claim **11**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**13**. The method of claim **2**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**14**. The method of claim **13**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**15**. The method of claim **2**, further including determining a user age corresponding to each of the user identities.

**16**. The method of claim **15**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**17**. The method of claim **2**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**18**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the video.

**19**. The method of claim **18**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**20**. The method of claim **18**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**21**. The method of claim **18**, further including determining whether at least one of the communications is censored based on content.

**22**. The method of claim **21**, further including determining a user age corresponding to each of the user identities.

**23**. The method of claim **18**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**24**. The method of claim **23**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**25**. The method of claim **18**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**26**. The method of claim **18**, further including determining a user age corresponding to each of the user identities.

**27**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the audio.

**28**. The method of claim **27**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**29**. The method of claim **27**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**30**. The method of claim **27**, further including determining whether at least one of the communications is censored based on content.

**31**. The method of claim **30**, further including determining a user age corresponding to each of the user identities.

**32**. The method of claim **27**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**33**. The method of claim **27**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**34**. The method of claim **27**, further including determining a user age corresponding to each of the user identities.

**35**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the graphic.

**36**. The method of claim **35**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**37**. The method of claim **35**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**38**. The method of claim **35**, further including determining whether at least one of the communications is censored based on content.

**39**. The method of claim **38**, further including determining a user age corresponding to each of the user identities.

**40**. The method of claim **35**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**41**. The method of claim **35**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**42**. The method of claim **35**, further including determining a user age corresponding to each of the user identities.

**43**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the multimedia.

**44**. The method of claim **43**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**45**. The method of claim **43**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia:

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**46**. The method of claim **43**, further including determining whether at least one of the communications is censored based on content.

**47**. The method of claim **46**, further including determining a user age corresponding to each of the user identities.

**48**. The method of claim **43**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**49**. The method of claim **43**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**50**. The method of claim **43**, further including determining a user age corresponding to each of the user identities.

**51**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the video.

**52**. The method of claim **51**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**53**. The method of claim **52**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**54**. The method of claim **51**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**55**. The method of claim **54**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**56**. The method of claim **51**, further including determining whether at least one of the communications is censored based on content.

**57**. The method of claim **56**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**58**. The method of claim **51**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**59**. The method of claim **58**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**60**. The method of claim **51**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**61**. The method of claim **60**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**62**. The method of claim **51**, further including determining a user age corresponding to each of the user identities.

**63**. The method of claim **62**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**64**. The method of claim **51**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**65**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the audio.

**66**. The method of claim **65**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**67**. The method of claim **66**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**68**. The method of claim **65**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**69**. The method of claim **68**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**70**. The method of claim **65**, further including determining whether at least one of the communications is censored based on content.

**71**. The method of claim **70**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**72**. The method of claim **65**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**73**. The method of claim **72**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**74**. The method of claim **65**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**75**. The method of claim **74**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**76**. The method of claim **65**, further including determining a user age corresponding to each of the user identities.

**77**. The method of claim **76**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**78**. The method of claim **65**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**79**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the graphic.

**80**. The method of claim **79**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**81**. The method of claim **80**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**82**. The method of claim **79**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**83**. The method of claim **82**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**84**. The method of claim **79**, further including determining whether at least one of the communications is censored based on content.

**85**. The method of claim **84**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**86**. The method of claim **79**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**87**. The method of claim **86** wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**88**. The method of claim **79**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**89**. The method of claim **88**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**90**. The method of claim **79**, further including determining a user age corresponding to each of the user identities.

**91**. The method of claim **90**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**92**. The method of claim **79**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**93**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the video and the audio.

**94**. The method of claim **93**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**95**. The method of claim **93**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**96**. The method of claim **93**, further including determining whether at least one of the communications is censored based on content.

**97**. The method of claim **93**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**98**. The method of claim **93**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**99**. The method of claim **93**, further including determining a user age corresponding to each of the user identities.

**100**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the video and the graphic.

**101**. The method of claim **100**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**102**. The method of claim **100**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**103**. The method of claim **100**, further including determining whether at least one of the communications is censored based on content.

**104**. The method of claim **100**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**105**. The method of claim **104**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**106**. The method of claim **100**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**107**. The method of claim **100**, further including determining a user age corresponding to each of the user identities.

**108**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the audio and the graphic.

**109**. The method of claim **108**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**110**. The method of claim **108**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**111**. The method of claim **108**, further including determining whether at least one of the communications is censored based on content.

**112**. The method of claim **108**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**113**. The method of claim **108**, further including determining a user age corresponding to each of the user identities.

**114**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the video and the audio.

**115**. The method of claim **114**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**116**. The method of claim **115**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**117**. The method of claim **114**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**118**. The method of claim **117**, wherein each said user identity is associated with a respective particular user's stored and rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**119**. The method of claim **114**, further including determining whether at least one of the communications is censored based on content.

**120**. The method of claim **119**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**121**. The method of claim **114**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**122**. The method of claim **121**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**123**. The method of claim **114**, further including determining a user age corresponding to each of the user identities.

**124**. The method of claim **123**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**125**. The method of claim **114**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**126**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the video and the graphic.

**127**. The method of claim **126**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**128**. The method of claim **127**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**129**. The method of claim **126**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**130**. The method of claim **129**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**131**. The method of claim **126**, further including determining whether at least one of the communications is censored based on content.

**132**. The method of claim **131**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**133**. The method of claim **126**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**134**. The method of claim **133**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**135**. The method of claim **126**, further including determining a user age corresponding to each of the user identities.

**136**. The method of claim **135**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**137**. The method of claim **126**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**138**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the a pointer and the audio and the graphic.

**139**. The method of claim **138**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**140**. The method of claim **139**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**141**. The method of claim **138**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**142**. The method of claim **141**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**143**. The method of claim **138**, further including determining whether at least one of the communications is censored based on content.

**144**. The method of claim **143**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**145**. The method of claim **138**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**146**. The method of claim **145**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**147**. The method of claim **138**, further including determining a user age corresponding to each of the user identities.

**148**. The method of claim **147**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**149**. The method of claim **138**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**150**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the video and the audio and the graphic.

**151**. The method of claim **150**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**152**. The method of claim **150**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**153**. The method of claim **150**, further including determining whether at least one of the communications is censored based on content.

**154**. The method of claim **150**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**155**. The method of claim **150**, further including determining a user age corresponding to each of the user identities.

**156**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the data presenting the pointer and the video and the audio and the graphic.

**157**. The method of claim **156**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**158**. The method of claim **157**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**159**. The method of claim **157**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**160**. The method of claim **159**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**161**. The method of claim **157**, further including determining whether at least one of the communications is censored based on content.

**162**. The method of claim **161**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**163**. The method of claim **157**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**164**. The method of claim **163**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**165**. The method of claim **157**, further including determining a user age corresponding to each of the user identities.

**166**. The method of claim **165**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**167**. The method of claim **157**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**168**. The method of claim **1**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**169**. The method of claim **168**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**170**. The method of claim **1**, further including:

determining whether the first user identity is censored from sending in the communications data presenting at least one of a pointer, video, a graphic, and multimedia;

facilitating sending the communications that are not censored from the sending, from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network; and

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

**171**. The method of claim **170**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**172**. The method of claim **1**, further including determining whether at least one of the communications is censored based on content.

**173**. The method of claim **172**, further including determining a user age corresponding to each of the user identities.

**174**. The method of claim **173**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**175**. The method of claim **172**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**176**. The method of claim **1**, wherein the determining whether the first user identity is censored includes determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities.

**177**. The method of claim **176**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**178**. The method of claim **1**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**179**. The method of claim **178**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**180**. The method of claim **1**, further including determining a user age corresponding to each of the user identities.

**181**. The method of claim **180**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**182**. The method of claim **1**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**183**. The method of claim **1**, wherein receiving the communications includes causing presentation of some of the communications by one of the plurality of participator computers in the group.

**184**. The method of claim **1**, wherein, if the first user identity is censored, not allowing the communications that include the data that is censored.

**185**. The method of claim **1**, wherein the computer system comprises an Internet service provider computer.

**186**. The method of claim **1**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitating presentation of the graphical multimedia at an output device corresponding to the second user identity.

**187**. The method of claim **1**, further including:

providing the first user identity with access to a member-associated image corresponding to the second user identity.

**188**. The method of claim **1**, further including:

determining whether the first user identity is censored from access to a member-associated image corresponding to the second user identity;

if the first user identity is censored, not allowing access to the member-associated image; and

if the first user identity is not censored, allowing access to the member-associated image.

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

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

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

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

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

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

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

**190**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer.

**191**. The method of claim **190**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**192**. The method of claim **191**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**193**. The method of claim **190**, further including determining whether at least one of the communications is censored based on content.

**194**. The method of claim **193**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**195**. The method of claim **190**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**196**. The method of claim **195**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**197**. The method of claim **190**, further including determining a user age corresponding to each of the user identities.

**198**. The method of claim **197**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**199**. The method of claim **190**, wherein at least one of the communications includes data presenting a human communication of sound.

**200**. The method of claim **199**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**201**. The method of claim **190**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**202**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video.

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

**204**. The method of claim **202**, further including determining whether at least one of the communications is censored based on content.

**205**. The method of claim **202**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**206**. The method of claim **202**, further including determining a user age corresponding to each of the user identities.

**207**. The method of claim **202**, wherein at least one of the communications includes data presenting a human communication of sound.

**208**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the audio.

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

**210**. The method of claim **208**, further including determining whether at least one of the communications is censored based on content.

**211**. The method of claim **208**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**212**. The method of claim **208**, further including determining a user age corresponding to each of the user identities.

**213**. The method of claim **208**, wherein at least one of the communications includes data presenting a human communication of sound.

**214**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the graphic.

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

**216**. The method of claim **214**, further including determining whether at least one of the communications is censored based on content.

**217**. The method of claim **214**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**218**. The method of claim **214**, further including determining a user age corresponding to each of the user identities.

**219**. The method of claim **214**, wherein at least one of the communications includes data presenting a human communication of sound.

**220**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the multimedia.

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

**222**. The method of claim **220**, further including determining whether at least one of the communications is censored based on content.

**223**. The method of claim **220**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**224**. The method of claim **220**, further including determining a user age corresponding to each of the user identities.

**225**. The method of claim **220**, wherein at least one of the communications includes data presenting a human communication of sound.

**226**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the video.

**227**. The method of claim **226**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**228**. The method of claim **227**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**229**. The method of claim **226**, further including determining whether at least one of the communications is censored based on content.

**230**. The method of claim **229**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**231**. The method of claim **226**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**232**. The method of claim **231** wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**233**. The method of claim **226**, further including determining a user age corresponding to each of the user identities.

**234**. The method of claim **233**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**235**. The method of claim **226**, wherein at least one of the communications includes data presenting a human communication of sound.

**236**. The method of claim **235**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**237**. The method of claim **226**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**238**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the audio.

**239**. The method of claim **238**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**240**. The method of claim **239**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**241**. The method of claim **238**, further including determining whether at least one of the communications is censored based on content.

**242**. The method of claim **241**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**243**. The method of claim **238**, wherein the determining whether the first user identity and the second user identity are

able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**244**. The method of claim **243**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**245**. The method of claim **238**, further including determining a user age corresponding to each of the user identities.

**246**. The method of claim **245**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**247**. The method of claim **238**, wherein at least one of the communications includes data presenting a human communication of sound.

**248**. The method of claim **247**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**249**. The method of claim **238**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**250**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the graphic.

**251**. The method of claim **250**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**252**. The method of claim **251**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**253**. The method of claim **250**, further including determining whether at least one of the communications is censored based on content.

**254**. The method of claim **253**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**255**. The method of claim **250**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**256**. The method of claim **255**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**257**. The method of claim **250**, further including determining a user age corresponding to each of the user identities.

**258**. The method of claim **257**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**259**. The method of claim **250**, wherein at least one of the communications includes data presenting a human communication of sound.

**260**. The method of claim **259**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**261**. The method of claim **250**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**262**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video and the audio.

**263**. The method of claim **262**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**264**. The method of claim **262**, further including determining whether at least one of the communications is censored based on content.

**265**. The method of claim **262**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**266**. The method of claim **262**, further including determining a user age corresponding to each of the user identities.

**267**. The method of claim **262**, wherein at least one of the communications includes data presenting a human communication of sound.

**268**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video and the graphic.

**269**. The method of claim **268**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**270**. The method of claim **268**, further including determining whether at least one of the communications is censored based on content.

**271**. The method of claim **268**, wherein the determining whether the first user identity and the second user identity are

able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**272**. The method of claim **268**, further including determining a user age corresponding to each of the user identities.

**273**. The method of claim **268**, wherein at least one of the communications includes data presenting a human communication of sound.

**274**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the audio and the graphic.

**275**. The method of claim **274**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**276**. The method of claim **274**, further including determining whether at least one of the communications is censored based on content.

**277**. The method of claim **274** wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**278**. The method of claim **274**, further including determining a user age corresponding to each of the user identities.

**279**. The method of claim **274**, wherein at least one of the communications includes data presenting a human communication of sound.

**280**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the video and the audio.

**281**. The method of claim **280**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**282**. The method of claim **281**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**283**. The method of claim **280**, further including determining whether at least one of the communications is censored based on content.

**284**. The method of claim **283**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**285**. The method of claim **280**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**286**. The method of claim **285**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**287**. The method of claim **280**, further including determining a user age corresponding to each of the user identities.

**288**. The method of claim **287**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**289**. The method of claim **280**, wherein at least one of the communications includes data presenting a human communication of sound.

**290**. The method of claim **289**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**291**. The method of claim **280**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**292**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the video and the graphic.

**293**. The method of claim **292**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**294**. The method of claim **293**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**295**. The method of claim **292**, further including determining whether at least one of the communications is censored based on content.

**296**. The method of claim **295**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**297**. The method of claim **292**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**298**. The method of claim **297**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**299**. The method of claim **292**, further including determining a user age corresponding to each of the user identities.

**300**. The method of claim **299**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**301**. The method of claim **292**, wherein at least one of the communications includes data presenting a human communication of sound.

**302**. The method of claim **301**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**303**. The method of claim **292**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**304**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the audio and the graphic.

**305**. The method of claim **304**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**306**. The method of claim **305**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**307**. The method of claim **304**, further including determining whether at least one of the communications is censored based on content.

**308**. The method of claim **307**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**309**. The method of claim **304**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**310**. The method of claim **309**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**311**. The method of claim **304**, further including determining a user age corresponding to each of the user identities.

**312**. The method of claim **311**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**313**. The method of claim **304**, wherein at least one of the communications includes data presenting a human communication of sound.

**314**. The method of claim **313**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**315**. The method of claim **304**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**316**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the video and the audio and the graphic.

**317**. The method of claim **316**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**318**. The method of claim **316**, further including determining whether at least one of the communications is censored based on content.

**319**. The method of claim **316**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**320**. The method of claim **316**, further including determining a user age corresponding to each of the user identities.

**321**. The method of claim **316**, wherein at least one of the communications includes data presenting a human communication of sound.

**322**. The method of claim **189**, wherein the determining whether the first user identity is censored includes determining that the first user identity is censored from the sending of the data presenting the pointer and the video and the audio and the graphic.

**323**. The method of claim **322**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**324**. The method of claim **323**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**325**. The method of claim **322**, further including determining whether at least one of the communications is censored based on content.

**326**. The method of claim **325**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**327**. The method of claim **322**, wherein the determining whether the first user identity and the second user identity are

able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**328**. The method of claim **189**, wherein the determining whether the first user identity and the second user identity are able to form a group includes determining from access rights stored by user in the database that neither of the user identities is censored.

**329**. The method of claim **322**, further including determining a user age corresponding to each of the user identities.

**330**. The method of claim **329**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**331**. The method of claim **322**, wherein at least one of the communications includes data presenting a human communication of sound.

**332**. The method of claim **331**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**333**. The method of claim **322**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**334**. The method of claim **189**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**335**. The method of claim **334**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**336**. The method of claim **189**, further including determining whether at least one of the communications is censored based on content.

**337**. The method of claim **336**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**338**. The method of claim **327**, wherein each said user identity is associated with a respective user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**339**. The method of claim **328**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**340**. The method of claim **189**, further including determining a user age corresponding to each of the user identities.

**341**. The method of claim **340**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**342**. The method of claim **189**, wherein at least one of the communications includes data presenting a human communication of sound.

**343**. The method of claim **342**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**344**. The method of claim **189**, wherein the computer system is comprised of an Internet service provider computer.

**345**. The method of claim **344**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**346**. The method of claim **189**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitating presentation of the graphical multimedia at an output device corresponding to the second user identity.

**347**. The method of claim **346**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**348**. The method of claim **189**, further including:

providing the first user identity with access to a member-associated image corresponding to the second user identity.

**349**. The method of claim **348**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**350**. The method of claim **189**, further including:

determining whether the first user identity is censored from access to a member-associated image corresponding to the second user identity;

if the first user identity is censored, not allowing access to the member-associated image; and

if the first user identity is not censored, allowing access to the member-associated image.

**351**. The method of claim **350**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**352**. The method of claim **189**, wherein each said user identity is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**353**. A system to communicate over an Internet network, the system including:

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

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

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

if the user identities are determined to be able to form the group, forms the group and facilitates receiving the communications that are sent and not censored from the second participator computer to the first participator computer, wherein the receiving is in real time and via the Internet network, and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the first participator computer; and

if the first user identity is censored from the data, does not facilitate the data that is censored to be presented from the second participator computer to the output device.

**354**. The system of claim **353**, wherein the data presents the pointer.

**355**. The system of claim **354**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**356**. The system of claim **355**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**357**. The system of claim **354**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitating sending the communications that are not censored from the sending.

**358**. The system of claim **357**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**359**. The system of claim **354**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**360**. The system of claim **359**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**361**. The system of claim **354**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**362**. The system of claim **353**, wherein the data presents the video.

**363**. The system of claim **362**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**364**. The system of claim **362**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**365**. The system of claim **362**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**366**. The system of claim **353**, wherein the data presents the audio.

**367**. The system of claim **366**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**368**. The system of claim **366**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**369**. The system of claim **366**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**370**. The system of claim **353**, wherein the data presents the graphic.

**371**. The system of claim **370**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**372**. The system of claim **370**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and
facilitates sending the communications that are not censored from the sending.

**373**. The system of claim **370**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**374**. The system of claim **353**, wherein the data presents the multimedia.

**375**. The system of claim **374**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**376**. The system of claim **374**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and
facilitates sending the communications that are not censored from the sending.

**377**. The system of claim **374**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**378**. The system of claim **353**, wherein the data presents the pointer and the video.

**379**. The system of claim **378**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**380**. The system of claim **379**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**381**. The system of claim **378**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and
facilitates sending the communications that are not censored from the sending.

**382**. The system of claim **381**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**383**. The system of claim **378**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**384**. The system of claim **383**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**385**. The system of claim **378**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**386**. The system of claim **353**, wherein the data presents the pointer and the audio.

**387**. The system of claim **386**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**388**. The system of claim **387**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**389**. The system of claim **386**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and
facilitates sending the communications that are not censored from the sending.

**390**. The system of claim **389**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**391**. The system of claim **386**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**392**. The system of claim **391**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**393**. The system of claim **386**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**394**. The system of claim **353**, wherein the data presents the pointer and the graphic.

**395**. The system of claim **394**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**396**. The system of claim **395**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**397**. The system of claim **394**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**398**. The system of claim **397**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**399**. The system of claim **394**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**400**. The system of claim **399**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**401**. The system of claim **394**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**402**. The system of claim **353**, wherein the data presents the video and the audio.

**403**. The system of claim **402**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**404**. The system of claim **402**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**405**. The system of claim **402**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**406**. The system of claim **353**, wherein the data presents the video and the graphic.

**407**. The system of claim **406**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**408**. The system of claim **406**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**409**. The system of claim **406**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**410**. The system of claim **353**, wherein the data presents the audio and the graphic.

**411**. The system of claim **410**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**412**. The system of claim **410**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**413**. The system of claim **410**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**414**. The system of claim **353**, wherein the data presents the pointer and the video and the audio.

**415**. The system of claim **414**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**416**. The system of claim **415**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**417**. The system of claim **414**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**418**. The system of claim **417**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**419**. The system of claim **414**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**420**. The system of claim **419**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**421**. The system of claim **414**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**422**. The system of claim **353**, wherein the data presents the pointer and the video and the graphic.

**423**. The system of claim **422**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**424**. The system of claim **423**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**425**. The system of claim **422**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**426**. The system of claim **425**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**427**. The system of claim **422**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**428**. The system of claim **427**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**429**. The system of claim **422**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**430**. The system of claim **353**, wherein the data presents the pointer and the audio and the graphic.

**431**. The system of claim **430**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**432**. The system of claim **431**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**433**. The system of claim **430**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**434**. The system of claim **433**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**435**. The system of claim **430**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**436**. The system of claim **435**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**437**. The system of claim **430**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**438**. The system of claim **353**, wherein the data presents the video and the audio and the graphic.

**439**. The system of claim **438**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**440**. The system of claim **438**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**441**. The system of claim **438**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**442**. The system of claim **353**, wherein the data presents the pointer and the video and the audio and the graphic.

**443**. The system of claim **442**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**444**. The system of claim **443**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**445**. The system of claim **442**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**446**. The system of claim **445**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**447**. The system of claim **442**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**448**. The system of claim **447**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**449**. The system of claim **442**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**450**. The system of claim **353**, wherein the computer system is further programmed to determine whether at least one of the communications is censored based on content.

**451**. The system of claim **450**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**452**. The system of claim **353**, wherein the computer system determines whether at least one of the first user identity and the second user identity, individually, is censored from sending in the communications data presenting at least one of the pointer, the video, the graphic, and the multimedia, and

facilitates sending the communications that are not censored from the sending.

**453**. The system of claim **452**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**454**. The system of claim **353**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**455**. The system of claim **454**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**456**. The system of claim **353**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**457**. The system of claim **456**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**458**. The system of claim **353**, wherein the computer system is programmed to:

store, for the first user identity, an authorization associated with presentation of graphical data, and

based on the authorization, allow the graphical data to be presented at an output device corresponding to the second user identity.

**459**. The system of claim **458**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**460**. The system of claim **353**, wherein the computer system is programmed to:

provide the first user identity with access to a member-associated image corresponding to the second user identity.

**461**. The system of claim **460**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**462**. The system of claim **353**, wherein the computer system is programmed to:

determine whether the first user identity is censored from access to a member-associated image corresponding to the second user identity,

if the first user identity is censored, not allowing access to member-associated image, and

if the first user identity is not censored, allow access to the member-associated image.

**463**. The system of claim **462**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**464**. The system of claim **353**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

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

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

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

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

if the user identities are determined to be able to form the group, forms the group and facilitates sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network, and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer; and

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

**466**. The system of claim **465**, wherein the data presents the pointer.

**467**. The system of claim **466**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**468**. The system of claim **467**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**469**. The system of claim **466**, wherein the computer system determines whether at least one of the communications is censored based on content.

**470**. The system of claim **469**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**471**. The system of claim **466**, wherein at least one of the communications includes a human communication of sound.

**472**. The system of claim **471**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**473**. The system of claim **466**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**474**. The system of claim **473**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said

user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**475**. The system of claim **466**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**476**. The system of claim **465**, wherein data presents the video.

**477**. The system of claim **476**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**478**. The system of claim **476**, wherein the computer system determines whether at least one of the communications is censored based on content.

**479**. The system of claim **476**, wherein at least one of the communications includes a human communication of sound.

**480**. The system of claim **476**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**481**. The system of claim **465**, wherein the data presents the audio.

**482**. The system of claim **481**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**483**. The system of claim **481**, wherein the computer system determines whether at least one of the communications is censored based on content.

**484**. The system of claim **481**, wherein at least one of the communications includes a human communication of sound.

**485**. The system of claim **481**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**486**. The system of claim **465**, wherein the data presents the graphic.

**487**. The system of claim **486**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**488**. The system of claim **486**, wherein the computer system determines whether at least one of the communications is censored based on content.

**489**. The system of claim **486**, wherein at least one of the communications includes a human communication of sound.

**490**. The system of claim **486**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**491**. The system of claim **465**, wherein the data presents the multimedia.

**492**. The system of claim **491**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**493**. The system of claim **491**, wherein the computer system determines whether at least one of the communications is censored based on content.

**494**. The system of claim **491**, wherein at least one of the communications includes a human communication of sound.

**495**. The system of claim **491**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**496**. The system of claim **465**, wherein the data presents the pointer and the video.

**497**. The system of claim **496**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**498**. The system of claim **496**, wherein the computer system determines whether at least one of the communications is censored based on content.

**499**. The system of claim **498**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**500**. The system of claim **496**, wherein at least one of the communications includes a human communication of sound.

**501**. The system of claim **500**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**502**. The system of claim **496**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**503**. The system of claim **502**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**504**. The system of claim **496**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**505**. The system of claim **465**, wherein the data presents the pointer and the audio.

**506**. The system of claim **505**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**507**. The system of claim **506**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**508**. The system of claim **505**, wherein the computer system determines whether at least one of the communications is censored based on content.

**509**. The system of claim **508**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**510**. The system of claim **505**, wherein at least one of the communications includes a human communication of sound.

**511**. The system of claim **510**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**512**. The system of claim **505**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**513**. The system of claim **512**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**514**. The system of claim **505**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**515**. The system of claim **465**, wherein the data presents the pointer and the graphic.

**516**. The system of claim **515**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**517**. The system of claim **516**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**518**. The system of claim **515**, wherein the computer system determines whether at least one of the communications is censored based on content.

**519**. The system of claim **518**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**520**. The system of claim **515**, wherein at least one of the communications includes a human communication of sound.

**521**. The system of claim **520**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**522**. The system of claim **515**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**523**. The system of claim **522**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**524**. The system of claim **515**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**525**. The system of claim **465**, wherein the data presents the video and the audio.

**526**. The system of claim **525**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**527**. The system of claim **525**, wherein the computer system determines whether at least one of the communications is censored based on content.

**528**. The system of claim **525**, wherein at least one of the communications includes a human communication of sound.

**529**. The system of claim **525**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**530**. The system of claim **465**, wherein the data presents the video and the graphic.

**531**. The system of claim **530**, wherein the computer wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**532**. The system of claim **530**, wherein the computer system determines whether at least one of the communications is censored based on content.

**533**. The system of claim **530**, wherein at least one of the communications includes a human communication of sound.

**534**. The system of claim **530**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**535**. The system of claim **465**, wherein the data presents the pointer and the video and the audio.

**536**. The system of claim **535**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**537**. The system of claim **536**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**538**. The system of claim **535**, wherein the computer system determines whether at least one of the communications is censored based on content.

**539**. The system of claim **538**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**540**. The system of claim **535**, wherein at least one of the communications includes a human communication of sound.

**541**. The system of claim **540**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**542**. The system of claim **535**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**543**. The system of claim **542**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**544**. The system of claim **535**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**545**. The system of claim **465**, wherein the data presents the pointer and the video and the graphic.

**546**. The system of claim **545**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**547**. The system of claim **546**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**548**. The system of claim **545**, wherein the computer system determines whether at least one of the communications is censored based on content.

**549**. The system of claim **548**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**550**. The system of claim **545**, wherein at least one of the communications includes a human communication of sound.

**551**. The system of claim **550**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**552**. The system of claim **545**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**553**. The system of claim **552**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**554**. The system of claim **545**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said

user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**555**. The system of claim **465**, wherein the data presents the pointer and the audio and the graphic.

**556**. The system of claim **555**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**557**. The system of claim **556**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**558**. The system of claim **555**, wherein the computer system determines whether at least one of the communications is censored based on content.

**559**. The system of claim **558**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**560**. The system of claim **555**, wherein at least one of the communications includes a human communication of sound.

**561**. The system of claim **560**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**562**. The system of claim **555**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**563**. The system of claim **562**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**564**. The system of claim **555**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**565**. The system of claim **465**, wherein the data presents the video and the audio and the graphic.

**566**. The system of claim **565**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**567**. The system of claim **565**, wherein the computer system determines whether at least one of the communications is censored based on content.

**568**. The system of claim **565**, wherein at least one of the communications includes a human communication of sound.

**569**. The system of claim **565**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**570**. The system of claim **465**, wherein the data presents the pointer and the video and the audio and the graphic.

**571**. The system of claim **570**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**572**. The system of claim **571**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**573**. The system of claim **570**, wherein the computer system determines whether at least one of the communications is censored based on content.

**574**. The system of claim **573**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**575**. The system of claim **570**, wherein at least one of the communications includes a human communication of sound.

**576**. The system of claim **575**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**577**. The system of claim **570**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**578**. The system of claim **577**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**579**. The system of claim **570**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said

user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**580**. The system of claim **465**, wherein the computer system provides access via any of two client software alternatives, wherein both of the client software alternatives allow respective user identities to be recognized and allow at least some of the participator computers to form at least one group in which members can send communications and receive communications.

**581**. The system of claim **580**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**582**. The system of claim **465**, wherein the computer system determines whether at least one of the communications is censored based on content.

**583**. The system of claim **582**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**584**. The system of claim **465**, wherein at least one of the communications includes a human communication of sound.

**585**. The system of claim **584**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**586**. The system of claim **465**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**587**. The system of claim **586**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**588**. The system of claim **465**, wherein the computer system determines from access rights stored by user that neither of the first user identity and the second user identity is censored from the group.

**589**. The system of claim **588**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**590**. The system of claim **465**, wherein the computer system is programmed to:

store, for the first user identity, an authorization associated with presentation of graphical data; and

based on the authorization, allow the graphical data to be presented at the output device corresponding to the second user identity.

**591**. The system of claim **590**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**592**. The system of claim **465**, wherein the computer system is programmed to:

provide the first user identity with access to a member-associated image corresponding to the second user identity.

**593**. The system of claim **592**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**594**. The system of claim **465**, wherein the computer system is programmed to:

determine whether the first user identity is censored from access to a member-associated image corresponding to the second user identity,

if the first user identity is censored, not allow access to the member-associated image, and

if the first user identity is not censored, allow access to the member-associated image.

**595**. The system of claim **594**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**596**. The system of claim **465**, wherein the computer system associates each said user identity in the group with a respective particular user's stored access rights, and determines whether the corresponding said user identity is censored from receiving, and whether the corresponding said user identity is censored from sending, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**597**. An Internet network communication system, the system including:

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

respond to one of the participator computers communicating a pointer in real time and via the Internet, wherein the pointer produces a pointer-triggered message on demand, by determining whether the first user identity is individually censored from content in the pointer-triggered message, by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities, if the content is censored, disallow the pointer-triggered message from being presented at an output device of the participator computer corresponding to the first user identity, and

if the content is not censored, allow the pointer-triggered message to be presented, wherein the computer system facilitates handling an Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the pointer-triggered message at the output device.

**598**. The system of claim **597**, wherein the computer system is further programmed to:

send and receive communications between members in a group, the communications including data presenting at least one of video, sound, a graphic, and multimedia, the communications being sent and received in real time via the Internet network.

**599**. The system of claim **598**, wherein the data includes data presenting sound.

**600**. The system of claim **599**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**601**. The system of claim **598**, wherein the data includes data presenting video.

**602**. The system of claim **601**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**603**. The system of claim **598**, wherein the data includes data presenting sound and video.

**604**. The system of claim **603**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**605**. The system of claim **598**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

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

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

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

responsive to the first of the participator computers communicating a pointer in real time and via the Internet, the pointer producing a pointer-triggered message on demand, determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities so that the first user identity is individually censored from content in the pointer-triggered message; and

if the content is censored, disallowing the pointer-triggered message to be presented at an output device of the first of the participator computers, and

if the content is not censored, allowing the pointer-triggered message to be presented, wherein the computer system facilitates handling an Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the pointer-triggered message at the output device.

**607**. The method of claim **606**, further including sending and receiving communications between members in a group, the communications including data presenting at least one of video, sound, a graphic, and multimedia, the receiving in real time via the Internet network.

**608**. The method of claim **607**, wherein the data presents sound.

**609**. The method of claim **608**, further including:

store, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitate presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**610**. The method of claim **607**, wherein the data presents video.

**611**. The method of claim **610**, further including:

store, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitate presentation of the graphical multimedia the participator computer corresponding to the second user identity.

**612**. The method of claim **607**, wherein the data presents sound and video.

**613**. The method of claim **607**, further including:

store, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitate presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**614**. The method of claim **606**, further including sending and receiving communications between members in a group, the communications including data presenting a member-associated image, sound, and video.

**615**. The method of claim **606**, further including:

store, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, facilitate presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

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

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

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

determining whether at least one of the first user identity and the second user identity is individually censored, by determining whether a parameter corresponding to said at least one has been determined by an other of the user identities, from receiving data comprising a pointer in communications that include at least one of text or ascii, the pointer being a pointer that produces a pointer-triggered message on demand;

determining whether the first and the second of the user identities are able to form a group; and

if the first and the second user identities are able to form the group, then forming the group and facilitating receiving the communications that are sent and not censored from one of the participator computers to another of the participator computers, wherein the computer system facilitates handling an Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content specified by the Internet URL at an output device of the other of the participator computers, and not allowing the data that is censored to be presented at the output device.

**617**. The method of claim **616**, wherein at least one of the communications includes data presenting sound.

**618**. The method of claim **617**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**619**. The method of claim **616**, wherein at least one of the communications includes data presenting video.

**620**. The method of claim **619**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**621**. The method of claim **616**, wherein at least one of the communications includes data presenting sound and video.

**622**. The method of claim **616**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**623**. The method of claim **622**, wherein the graphical data includes graphical multimedia data.

**624**. The method of claim **616**, based on the authorization, presenting the graphical multimedia data at the output device corresponding to the second user identity, and wherein one of the determining steps includes determining whether a parameter corresponding to the first user identity has been determined by a user corresponding to another of the user identities.

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

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

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

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

determining whether at least one of the first user identity and the second user identity is individually censored, by determining whether a parameter corresponding to said at least one has been determined by an other of the user identities, from sending a pointer in the communications including at least one of text or ascii, the pointer being a pointer that produces a pointer-triggered message on demand; and

if the first and the second user identities are able to form the group, then forming the group and facilitating sending the communications that are not censored from one of the participator computers to another of the participator computers in real time over the Internet network, wherein the computer system facilitates handling an Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and not facilitating sending a pointer that is censored.

**626**. The method of claim **625**, wherein at least one of the communications includes data presenting sound.

**627**. The method of claim **626**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**628**. The method of claim **625**, wherein at least one of the communications includes data presenting video.

**629**. The method of claim **628**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**630**. The method of claim **625**, wherein at least one of the communications includes data presenting sound and video.

**631**. The method of claim **630**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical data; and

based on the authorization, allowing presentation of the graphical data at the participator computer corresponding to the second user identity.

**632**. The method of claim **625**, further including:

storing, for the first user identity, an authorization associated with presentation of graphical multimedia; and

based on the authorization, allowing presentation of the graphical multimedia at the participator computer corresponding to the second user identity.

**633**. A system to communicate via an Internet network, the system including:

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

determine whether at least one of the first user identity and the second user identity is individually censored, by determining whether a parameter corresponding to said at least one has been determined by an other of the user identities, from receiving, in communications, data comprising a pointer, the pointer producing a pointer-triggered message on demand, and

thereafter allow the participator computers to receive, in real time via the Internet network, and present the communications that are not censored, wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of one of the participator computers corresponding the user identity which presents the communications, and to not present the data that is censored at an output device corresponding to the user identity that is censored from receiving the data.

**634**. The system of claim **633**, wherein at least one of the communications includes data presenting sound.

**635**. The system of claim **634**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**636**. The system of claim **633**, wherein at least one of the communications includes data presenting video.

**637**. The system of claim **636**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**638**. The system of claim **633**, wherein at least one of the communications includes data presenting sound and video.

**639**. The system of claim **638**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**640**. The system of claim **633**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**641**. A system to communicate via an Internet network, the system including:

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

determine whether at least one of the first user identity and the second user identity is individually censored, by determining whether a parameter corresponding to said at least one has been determined by an other of the user identities, from sending, in communications, a pointer that produces a pointer-triggered message on demand, and

thereafter allow the participator computers to receive, in real time via the Internet network, and present the communications that are not censored based on the individual user identity, wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of one of the participator computers corresponding the user identity which presents the communications, and to not present the communications that are censored at an output device corresponding to the user identity that is censored from the sending.

**642**. The system of claim **641**, wherein at least one of the communications includes data presenting sound.

**643**. The system of claim **642**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**644**. The system of claim **641**, wherein at least one of the communications includes data presenting sound.

**645**. The system of claim **644**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**646**. The system of claim **641**, wherein at least one of the communications includes data presenting video.

**647**. The system of claim **646**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

**648**. The system of claim **641**, wherein the computer system provides the participator computer corresponding to the first user identity with access to a member-associated image corresponding to the second user identity.

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

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

storing a respective particular user's access rights corresponding to each said user identity;

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

determining whether at least one of the first user identity and the second user identity is individually censored by the corresponding user's stored access rights from receiving data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities; and

if the first and the second user identities are able to form the group, forming the group and facilitating receiving the communications, including receiving at least some of the communications with the data that is not censored, that are sent from one of the participator computers to another of the participator computers, wherein the receiving is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the participator computer which is receiving the communications, and not allowing the data that is censored by the corresponding user's stored access rights to be presented at an output device of the participator computer corresponding to the user identity that is censored.

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

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

determining whether the first user identity and the second user identity are able to form a group to send and to receive data in communications in real time by determining whether at least one of the first user identity and the second user identity is individually censored from receiving the data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities; and

if the first and the second user identities are determined to be able to form the group, forming the group and facilitating receiving the communications, including receiving at least some of the communications with the data that is not censored, that are sent from one of the participator computers to another of the participator computers, in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers; and

if the first and the second user identities are determined to not be able to form the group with respect to receiving the data that is censored, not forming the group.

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

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

storing a respective particular user's access rights corresponding to each said user identity;

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

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

if the first and the second user identities are able to form the group, forming the group and facilitating sending the communications, including sending at least some of the communications with the data that is not censored, from one of the participator computers to another of the participator computers, wherein the sending is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and not allowing sending the data that is censored by the corresponding user's stored access rights.

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

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

determining whether a first of the user identities and a second of the user identities are able to form a group to send and to receive communications in real time by determining whether at least one of the first user identity and the second user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities; and

if the first and the second user identities are determined to be able to form the group, forming the group and facilitating sending the communications, including sending at least some of the communications with the data that is not censored, from one of the participator computers to another of the participator computers in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers; and

if the first and the second user identities are determined to not be able to form the group with respect to sending the data that is censored, not forming the group.

**653**. A system to communicate via an Internet network, the system including:

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

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

determine whether at least one of the first user identity and the second user identity is individually censored by the corresponding user's stored access rights from receiving data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, and

if the first and the second user identities are able to form the group, form the group and facilitate receiving the communications that are sent and not censored from one of the participator computers to another of the participator computers, wherein the receiving is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and

not allow the data that is censored by the corresponding user's stored access rights to be presented at an output device of the participator computer corresponding to the user identity that is censored.

**654**. A system to communicate via an Internet network, the system including:

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

determine whether the first user identity and the second user identity are able to form a group to send and to receive real-time communications by determining whether at least one of the first user identity and the second user identity is individually censored from receiving data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, and

if the first and the second user identities are determined to be able to form the group, form the group and facilitate receiving the communications from one of the participator computers to an other of the participator computers, in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and

if the first and the second user identities are determined to not be able to form the group with respect to receiving the data that is censored, not form the group.

**655**. A system to communicate via an Internet network, the system including:

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

store a respective particular user's access rights corresponding to each said user identity,

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

determine whether at least one of the first user identity and the second user identity is individually censored by the corresponding user's stored access rights from sending data in the communications, the data including at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, and

if the first and the second user identities are able to form the group, and facilitate sending the communications that are not censored from one of the participator computers to another of the participator computers, wherein the sending is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and not allow sending the data that is censored by the corresponding user's stored access rights.

**656**. A system to communicate via an Internet network, the system including:

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

determine whether a first of the user identities and a second of the user identities are able to form a group to send and to receive communications in real time by determining whether at least one of the first user identity and the second user identity is individually censored from sending data in the communications, the data presenting at least one of a pointer, video, audio, a graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, and

if the first and the second user identities are determined to be able to form the group, form the group and facilitate sending the communications from one of the participator computers to another of the participator computers, wherein the sending is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and

if the first and the second user identities are determined to not be able to form the group with respect to sending the data that is censored, not form the group.

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

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

storing a respective particular user's access rights corresponding to each said user identity;

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

determining, based on the access rights of the first user identity by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities, whether the first user identity is individually censored from receiving content in the communications;

if the user identities are determined to be able to form the group, forming the group and facilitating receiving the communications that are sent and not censored from the second participator computer to the first participator computer, wherein the receiving is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and

if the first user identity is censored, not allowing the content that is censored to be presented from the second participator computer to a user of the first participator computer.

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

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

storing a respective particular user's access rights corresponding to each said user identity;

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

determining, based on the access rights of the first user identity by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities, whether the first user identity is individually censored from sending content in the communications;

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

if the first user identity is censored, not allowing the content that is censored to be sent from the first participator computer the second participator computer.

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

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

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

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

if the user identities are determined to be able to form the group, forming the group and facilitating receiving the communications that are sent and not censored from the second participator computer to the first participator computer, wherein the receiving is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present the Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the first participator computer, and

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

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

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

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

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

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

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

**661**. A system to communicate via an Internet network, the system including:

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

determine whether the first user identity is individually censored from receiving content in the communications, by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities,

if the user identities are determined to be able to form the group, form the group and facilitate receiving the communications that are sent and not censored from the second participator computer to the first participator computer, wherein the receiving is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers at an output device of the first participator computer, and

if the first user identity is censored, not allow the content that is censored to be presented from the second participator computer at the first participator computer.

**662**. A system to communicate via an Internet network, the system including:

a computer system including a controller computer that is an Internet service provider computer and a database

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

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

determine whether the first user identity is individually censored from sending content in the communications, by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities,

if the user identities are determined to be able to form the group, form the group and facilitate sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers at an output device of the second participator computer, and

if the first user identity is censored, not allow the content that is censored to be sent from the first participator computer the second participator computer.

**663**. A system to communicate via an Internet network, the system including:

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

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

determine whether the first user identity is individually censored from sending content in the communications, by determining whether a parameter corresponding to the first user identity has been determined by an other of the user identities,

if the user identities are determined to be able to form the group, form the group and facilitate sending the communications that are not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers, and if the first user identity is censored, not allow the content that is censored to be sent from the first participator computer the second participator computer.

**664**. The method of claim **663**, wherein each said user identity in the group is associated with a respective particular user's stored access rights, which determine whether the corresponding said user identity is censored from receiving, in the communications, data presenting at least one of a pointer, video, audio, a graphic, and multimedia.

**665**. The method of claim **663**, further including:

determining whether the first user identity is censored from the data by determining whether a parameter corresponding to the first user identity has been determined by a user corresponding to an other of the user identities.

**666**. A system to communicate via an Internet network, the system including:

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

determine whether a first of the user identities and a second of the user identities are able to form a group to send and to receive communications in real time by determining whether at least one of the first user identity and the second user identity is individually censored from data in the communications, the data presenting at least one of a pointer, video, audio, graphic, and multimedia, by determining whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, and

if the first and the second user identities are determined to be able to form the group, form the group and facilitate receiving the communications that are sent and include said data that is not censored from one of the participator computers to another of the participator computers, wherein the receiving is in real time via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the other of the participator computers at an output device of the other of the participator computers, and

if the first and the second user identities are determined to not be able to form the group, not form the group.

**667**. A system to communicate via an Internet network, the system including:

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

allow the first user identity and the second user identity to send communications and to receive communications sent by another user identity on at least one of a plurality of channels, wherein at least some of the communications are received in real time via the Internet network, except that if at least one of the user identities is individually censored, from data in one of the channels, the data presenting at least one of a pointer, video, audio, graphic, or multimedia, and multimedia, by a determination of whether a respective at least one parameter corresponding to said at least one of the first user identity and the second user identity has been determined by an other of the user identities, the data that is censored is not presented by the participator computer corresponding to the user identity that is censored from the data, and otherwise allow the data to be presented at an output device corresponding to the participator computer which receives the data, wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at the output device.

**668**. A system to communicate via an Internet network, the system including:

a computer system including a controller computer that is an Internet service provider computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the computer system in communication with a first of the participator computers responsive to a first authenticated user identity and with a second of the participator computers responsive to a second authenticated user identity, wherein the computers are configured so as to censor communications based on:

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

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

if the user identities are able to form the group, form the group and facilitate receiving the communications that are sent and not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network and wherein the computer system facilitates handling an Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer;

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

**669**. A system to communicate via an Internet network, the system including:

a computer system including a controller computer that is an Internet service provider computer and a database which serves as a repository of tokens for other programs to access, thereby affording information to each of a plurality of participator computers which are otherwise independent of each other, the computer system in communication with a first of the participator computers responsive to a first authenticated user identity and with a second of the participator computers responsive to a second authenticated user identity, wherein the computers are configured so as to censor communications based on:

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

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

if the user identities are able to form the group, form the group and facilitate receiving the communications that are sent and not censored from the second participator computer to the first participator computer, wherein the receiving is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the first participator computer;

if the first user identity is censored, not allowing the data that is censored to be presented from the second participator computer at the output device.

**670**. A system to communicate via an Internet network, the system including:

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

store a respective particular user's access rights corresponding to each said user identity, and

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

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

if the user identities are determined to be able to form the group, form the group and facilitate receiving the communications that are sent and not censored from the first participator computer to the second participator computer, wherein the sending is in real time and via the Internet network and wherein the computer system facilitates, for the communications which are received and which present an Internet URL, handling the Internet URL via the computer system so as to find content specified by the Internet URL and facilitates presenting the content at an output device of the second participator computer, and

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

**671**. A system to communicate via an Internet network, the system including:

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

store a respective particular user's access rights corresponding to each said user identity, and

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

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

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

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

* * * * *

# CERTIFICATE OF SERVICE

I hereby certify that on May 21, 2018, I caused a copy of the foregoing Appellant's Opening Brief to be served on Appellee's counsel via electronic mail at the following addresses:

Vincent J. Rubino, III
vrubino@brownrudnick.com
Alfred R. Fabricant
afabricant@brownrudnick.com
Peter Lambrianakos
plambrianakos@brownrudnick.com
Shahar Harel
sharel@brownrudnick.com
Enrique W. Iturralde
eiturralde@brownrudnick.com
BROWN RUDNICK LLP

/s/ Heidi L. Keefe
Heidi L. Keefe

# CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Circuit Rule 32(a). Exclusive of the exempted portions of the brief, as provided in Federal Circuit Rule 32(a), the brief contains 11,203 words.

This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6). The brief has been prepared in proportionally spaced typeface using Microsoft Word in 14 point Times New Roman font.

Dated: May 21, 2018

By: /s/ Heidi L. Keefe
Heidi L. Keefe
Cooley LLP