

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SAMSUNG ELECTRONICS CO., LTD.
Petitioner,

v.

BLACK HILLS MEDIA, LLC
Patent Owner.

Case No. To Be Assigned
Patent No. 7,835,689

**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,835,689
UNDER 35 U.S.C. §§ 311-319 AND 37 C.F.R. § 42.100 *et seq.***

TABLE OF CONTENTS

I.	MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1))	1
A.	Real Party-In-Interest (37 C.F.R. § 42.8(b)(1))	1
B.	Related Matters (37 C.F.R. § 42.8(b)(2))	1
C.	Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3))	1
D.	Service Information (37 C.F.R. § 42.8(b)(4))	2
II.	FEES (37 C.F.R. § 42.103)	2
III.	REQUIREMENTS FOR INTER PARTES REVIEW UNDER 37 C.F.R. § 42.104	2
A.	Grounds for Standing (37 C.F.R. § 42.104(a))	2
B.	Citation of Prior Art	3
C.	Claims and Statutory Grounds (37 C.F.R. §§ 42.104(b)(1) & (b)(2))	4
D.	Claim Construction (37 C.F.R. § 42.104(b)(3))	4
E.	Person of Ordinary Skill in the Art	8
F.	Unpatentability of the Construed Claims (37 C.F.R. § 42.104(b)(4))	8
G.	Supporting Evidence (37 C.F.R. § 42.104(b)(5))	8
IV.	SUMMARY OF THE ‘689 PATENT	9
A.	Overview of the ‘689 Patent	9
B.	Prosecution History Summary of the ‘689 Patent	9
V.	THERE IS A REASONABLE LIKELIHOOD THAT PETITIONER WILL PREVAIL WITH RESPECT TO AT LEAST ONE CLAIM OF THE ‘689 PATENT	13
A.	Prior Art	13

1.	State of the Art in 2001	13
2.	The Yeager Patent (Ex. 1003).....	18
3.	The <i>P2P Networking</i> Reference (Ex. 1005)	20
4.	The Busam Application (Ex. 1006)	21
5.	The Phillips Patent (Ex. 1007).....	23
6.	The Abecassis Patent (Ex. 1008)	24
7.	The Ganesan Patent (Ex. 1009)	26
B.	Ground I: The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103	27
C.	Ground II: The Combination of the Busam Application and the Phillips Patent Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103	36
D.	Ground III: The Combination of the Abecassis and Ganesan Patents Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103	49
VI.	CONCLUSION	56

LIST OF EXHIBITS

Exhibit	Description
Ex. 1001	U.S. Patent No. 7,835,689
Ex. 1002	File History for U.S. Patent No. 7,835,689
Ex. 1003	U.S. Patent No. 7,383,433 to Yeager <i>et al.</i>
Ex. 1004	U.S. Patent Prov. App. No. 60/308,932
Ex. 1005	Manoj Parameswaran <i>et al.</i> , <i>P2P Networking: An Information-Sharing Alternative</i> , Computer 31-38 (July 2001)
Ex. 1006	U.S. Patent Application Publication No. 2002/0087887 to Busam <i>et al.</i>
Ex. 1007	U.S. Patent No. 7,058,696 to Phillips <i>et al.</i>
Ex. 1008	U.S. Patent No. 6,192,340 to Abecassis
Ex. 1009	U.S. Patent No. 5,535,276 to Ganesan
Ex. 1010	Black Hills Media, LLC's Disclosure of Asserted Claims and Preliminary Infringement Contentions and Document Production Accompanying Disclosure Under L.R. 3-1 and 3-2, <i>Black Hills Media, LLC v. Samsung Elecs. Co., Ltd. et al.</i> , Civil Action No. 2-13-cv-00379 (E.D. Tex. Aug. 22, 2013)
Ex. 1011	Declaration of Kevin Almeroth, Ph.D. ("Almeroth Declaration")
Ex. 1012	<i>Curriculum vitae</i> of Kevin Almeroth, Ph.D.
Ex. 1013	Savetz <i>et al.</i> , <i>MBONE: Multicasting Tomorrow's Internet</i> (1996)
Ex. 1014	Kevin C. Almeroth, <i>The Evolution of Multicast: From the MBone to Interdomain Multicast to Internet2 Deployment</i> , IEEE Network 10-20 (Jan./Feb. 2000)
Ex. 1015	Gong & Shacham, <i>Multicast Security and Its Extension to a Mobile Environment</i> , 1 Wireless Networks 281-295 (1995)
Ex. 1016	Neil Strauss, <i>Rolling Stones Live on Internet</i> , The New York Times, Nov. 22, 1994
Ex. 1017	Karl T. Greenfeld, <i>Meet the Napster</i> , TIME 60-68 (October 2, 2000)
Ex. 1018	Gene Kan, <i>Gnutella</i> , pp. 97-100, in <i>Peer-to-Peer: Harnessing the Power of Disruptive Technologies</i> (Andy Oram ed., 2001)
Ex. 1019	John Schwartz, <i>File-Swapping Is New Route for Pornography on Internet</i> , The New York Times, July 28, 2001
Ex. 1020	David Kushner, <i>The Digital Beat: The Instant Message Music War</i> , Rolling Stone, June 13, 2001

I. MANDATORY NOTICES (37 C.F.R. § 42.8(A)(1))**A. Real Party-In-Interest (37 C.F.R. § 42.8(b)(1))**

The real parties in interest for this petition for Inter Partes Review (“IPR”) are Samsung Electronics Co., Ltd.; Samsung Electronics America, Inc.; and Samsung Telecommunications America, LLC.

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

U.S. Patent No. 7,835,689 (“the ‘689 Patent”) is currently the subject of litigation against Samsung in the Eastern District of Texas in the action captioned *Black Hills Media, LLC v. Samsung Elecs. Co., Ltd. et al.* (Civil Action No. 2-13-cv-00379 (E.D. Tex.); the “Samsung Litigation”).

C. Lead and Backup Counsel (37 C.F.R. § 42.8(b)(3))

Lead Counsel	Back-up Counsel
Andrea G. Reister (Reg. No. 36,253) areister@cov.com	Gregory S. Discher (Reg. No. 42,488) gdischer@cov.com
<u>Postal and Hand-Delivery Address:</u> Covington & Burling LLP 1201 Pennsylvania Avenue, NW Washington, DC 20004 T: (202)662-5141; F: (202)778-5141	<u>Postal and Hand-Delivery Address:</u> Covington & Burling LLP 1201 Pennsylvania Avenue, NW Washington, DC 20004 T: (202)662-5485; F: (202)778-5485

D. Service Information (37 C.F.R. § 42.8(b)(4))

Service information for lead and back-up counsel is provided in the designation of lead and back-up counsel above.

II. FEES (37 C.F.R. § 42.103)

The undersigned authorizes the Office to charge \$23,000 (\$9,000 request fee; and \$14,000 post-institution fee) to Deposit Account No. 50-0740 for the fees set forth in 37 C.F.R. § 42.15(a) for this Petition for *Inter Partes* Review. The undersigned further authorizes payment for any additional fees that might be due in connection with this Petition to be charged to the above referenced Deposit Account.

III. REQUIREMENTS FOR INTER PARTES REVIEW UNDER 37 C.F.R. § 42.104

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

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the ‘689 Patent is available for *inter partes* review and that Petitioner is not barred or estopped from requesting an *inter partes* review challenging the ‘689 Patent on the grounds identified in the present petition.

B. Citation of Prior Art

Exhibit	Reference	Publication or Filing Date	Availability as Prior Art
Ex. 1003	U.S. Patent No. 7,383,433 to Yeager <i>et al.</i> (“Yeager”)	July 31, 2001	35 U.S.C. § 102(e)
Ex. 1005	Manoj Parameswaran <i>et al.</i> , <i>P2P Networking: An Information- Sharing Alternative</i> , Computer 31- 38 (July 2001) (“ <i>P2P Networking</i> ”).	July 2001	35 U.S.C. § 102(a)
Ex. 1006	U.S. Patent Application Publication No. 2002/0087887 to Busam <i>et al.</i> (“Busam”)	September 19, 2001	35 U.S.C. § 102(e)
Ex. 1007	U.S. Patent No. 7,058,696 to Phillips <i>et al.</i> (“Phillips”)	November 1, 2000	35 U.S.C. § 102(e)
Ex. 1008	U.S. Patent No. 6,192,340 to Abecassis (“Abecassis”)	February 20, 2001	35 U.S.C. § 102(b)
Ex. 1009	U.S. Patent No. 5,535,276 to Ganesan (“Ganesan”)	July 9, 1996	35 U.S.C. § 102(b)

C. Claims and Statutory Grounds (37 C.F.R. §§ 42.104(b)(1) & (b)(2))

The relief requested by Petitioner is that claims 9 and 10 of the ‘689 Patent be found unpatentable and cancelled from the ‘689 Patent on the following grounds:

Ground	Claims	Basis
I	9, 10	Obvious under 35 U.S.C. § 103(a) in view of Yeager and <i>P2P Networking</i>
II	9, 10	Obvious under 35 U.S.C. § 103(a) in view of Busam and Phillips
III	9, 10	Obvious under 35 U.S.C. § 103(a) in view of Abecassis and Ganesan

D. Claim Construction (37 C.F.R. § 42.104(b)(3))

A claim subject to IPR is given its “broadest reasonable construction in light of the specification of the patent in which it appears.” 37 C.F.R. § 42.100(b). Should patent owner, in an effort to avoid the prior art, contend that the claims have a construction different from their broadest reasonable construction, the appropriate course is for patent owner to seek to amend the claims to expressly correspond to its contentions in this proceeding. *See* Office Patent Trial Practice Guide, 77 Fed. Reg. 48756, 48764 (August 14, 2012). Of course, any such

amendment would only be permissible if the proposed amended claims comply with 35 U.S.C. § 112. Petitioner has included below a discussion of the “broadest reasonable construction consistent with the specification” (“BRC”) for a number of claim terms of the ‘689 Patent.

Each of independent claim 9 and dependent claim 10 recites “media player device.” Petitioner submits that the BRC for “media player device” is “a device that is capable of playing media, including audio content, video content, or a combination of both.” As explained below, this construction is supported by the broadest reasonable understanding of the term “media player device” consistent with the specification, which states that the disclosed embodiments “are merely illustrations of a few of the many specific embodiments of the present invention.” Ex. 1001, 60:25-28.

In particular, the specification of the ‘689 Patent discloses both mobile device embodiments for sharing audio entertainment, *see, e.g.*, Ex. 1001, 3:31-48, 5:19-31, and other embodiments for sharing audio entertainment that need not be mobile, *see, e.g.*, Ex. 1001, 3:15-30, 3:49-58, 4:4-22, 4:23-40. Accordingly, the BRC of “media player device” includes within its scope mobile as well as non-mobile devices. In addition, the specification of the ‘689 Patent discloses that the units of its invention may “comprise video or audio/visual players” and, as such, the BRC of “media player device” includes within its scope devices that play video

as well as those that play audio. Ex. 1001, 56:17-38. Based on such disclosures, one skilled in the art would appreciate that the BRC for “media player device” is “a device that is capable of playing media, including audio content, video content, or a combination of both”. Almeroth Dec., ¶¶ 31-32.

Independent claim 9 also recites “information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.” Petitioner submits that the BRC for this “information” includes within its scope information that the trusted user makes available to a requesting user if that information helps the requesting user gain admission to a sharing group. Such “information” would include, for example, credentials, such as a sharing group password or a security certificate, provided by a trusted user to the “user of a requesting media player device,” if the requesting user submits those credentials with its request to join the sharing group. Almeroth Dec., ¶ 33. This construction accords with the broadest reasonable understanding of “made available by,” because the information is “made available by” the trusted user to the requesting user. Further, nothing in the specification requires that the trusted user make the information directly available to the user decision maker making the determination whether to admit the requesting media player device to the sharing group.

This construction is also consistent with the prosecution history, when viewed through the lens of the BRC standard. Although, as explained below, the applicant distinguished information “supplied by” a requesting user from “information, made available by a trusted user,” Ex. 1002, p. 164, the BRC of the term “information, made available by a trusted user” would still include information that the trusted user makes available to a requesting user, even if the decision maker ultimately receives that information from the requesting user.

Moreover, Patentee has asserted in its infringement contentions in litigation that a sharing group password submitted with a requesting user’s join request meets the limitation “information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group” because that sharing group password was obtained from a trusted user. *See* Ex. 1010, at 3, 7. Given the broader claim construction standard that applies in this proceeding, the BRC must also include such a “sharing group password” within its scope.

E. Person of Ordinary Skill in the Art

A person of ordinary skill in the art of the ‘689 Patent at the time of the alleged invention (“POSA”) would typically have had a M.S. degree in computer science in addition to two or more years of work experience relating to the distribution of multimedia content over networks. Almeroth Dec., ¶ 4.

F. Unpatentability of the Construed Claims (37 C.F.R. § 42.104(b)(4))

An explanation of how claims 9 and 10 of the ‘689 Patent are unpatentable under the statutory grounds identified above is provided in Section V. below.

G. Supporting Evidence (37 C.F.R. § 42.104(b)(5))

The exhibit numbers of the supporting evidence relied upon to support the challenge and the relevance of the evidence to the challenge raised, including identifying specific portions of the evidence that support the challenge, are provided below in the form of explanatory text and claim charts. An Exhibit List with the exhibit numbers and a brief description of each exhibit is set forth above.

IV. SUMMARY OF THE ‘689 PATENT

A. Overview of the ‘689 Patent

The ‘689 Patent discloses, among other things, embodiments of mobile devices for sharing audio entertainment. *See, e.g.*, Ex. 1001, 3:31-48, 5:19-31. In other embodiments, the ‘689 Patent discloses audio entertainment devices that need not be mobile. *See, e.g.*, Ex. 1001, 3:15-30, 3:49-58, 4:4-22, 4:23-40. The ‘689 Patent also discloses that the player units of its invention may “comprise video or audio/visual players.” Ex. 1001, 56:17-19.

The ‘689 Patent discloses an embodiment in which a number of units within communication range may share, for example, audio content. *See, e.g.*, Ex. 1001, 17:35-67 and 21:44-55. The ‘689 Patent further discloses that decisions on admitting a requesting user to such a sharing group may be made based on, for example, rating information regarding the requesting member, the duration of the requesting member’s association with other sharing groups, and the popularity of such other sharing groups. Ex. 1001, 37:64 – 38:10. Moreover, the ‘689 Patent discloses that the decision of whether to admit the requesting user to the sharing group may be based on information on the reputation or desirability of the requesting user as retrieved from trusted people. Ex. 1001, 38:11–24.

B. Prosecution History Summary of the ‘689 Patent

The ‘689 Patent was filed on December 4, 2006, as application number 11/566,552. The ‘552 application was a divisional of application number

10/513,702, which was the national stage of international application PCT/US03/14154, filed May 6, 2003. The international application claimed priority to three provisional applications, the earliest of which was filed on May 6, 2002.

A number of responses, amendments, and interview summaries are present in the file history of the '689 Patent. Petitioner summarizes here the ones most relevant to the grounds of unpatentability set forth in the present Petition.

In the Office Action dated December 19, 2008, certain pending claims were rejected under 35 U.S.C. § 102(e) as being anticipated by Chang (U.S. Pat. App. Pub. No. 2002/0168938) and the remaining rejected claims were rejected under 35 U.S.C. § 103(a) as being unpatentable over the combination of Chang and Iyer (U.S. Pat. App. Pub. No. 2001/0037367). Ex. 1002, pp. 148-59. In particular, claim 59 (which issued as claim 9 of the '689 Patent) was rejected in light of the combination of Chang and Iyer. Claims 53, 55, 57-58 were indicated as being allowable. *Id.* at p. 156.

Applicants filed a Response dated March 5, 2009, to the Office Action dated December 19, 2008. Ex. 1002, pp. 133-46. In this Response, applicants pointed out that a password supplied by a visitor, that is, a user of a device requesting admission to a group, could not satisfy the recited element of “wherein the information associated with the user of the requesting media player device

comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.”

Id. at p. 142. Applicants explained that the user of the device requesting admission could not be considered to be a “trusted user,” as recited:

Iyer teaches a system and method for sharing information via a virtual shared area. Paragraph [0025] of Iyer teaches that the system includes a server (18) that includes an authentication and management area (20) that manages ownership and access to a shared area (SA) (16). More specifically, as discussed in lines 3-6 of paragraph [0036] of Iyer, an authentication mechanism, such as a password, may be used to authenticate a visitor before allowing access to the SA (16). However, Iyer fails to teach or suggest information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group. In Iyer, even if the password supplied by the visitor is attempted to be read as the claimed information, the password in Iyer is supplied by the visitor (i.e., the user of the requesting device) rather than a trusted user. Chang fails to correct this deficiency. As such, the combination of Chang and Iyer fails to teach or suggest all of the features of claim 59. Further, the Patent Office has failed to show how the features of claim 59 that are not taught or suggested by the combination of Chang and Iyer would have otherwise been obvious to one of ordinary skill in the art at the time of the invention. As such, claim 59 is allowable.

Ex. 1002, p. 142. Applicants also added new claim 68, which issued as claim 10 of the ‘689 Patent. *Id.* at p. 139.

In response, claim 59 was allowed in the Final Office Action dated April 14, 2009. Ex. 1002, p. 126. Despite this, dependent claim 68, which depends from claim 59, was rejected in light of the Chang application. *Id.* at p. 124. Applicants filed a Response on June 16, 2009, pointing out that, among other things, claims 59 and 68 should both be allowed, and made amendments to some of the rejected claims. *Id.* at pp. 103-109.

In an Office Action dated August 3, 2009, the Examiner rejected (i) certain claims as being anticipated under 35 U.S.C. § 102(e) by Goto (U.S. Pat. App. Pub. No. 2002/0160824), (ii) certain other claims as being rendered obvious under 35 U.S.C. § 103(a) by the combination of Goto and Mourad (U.S. Pat. App. Pub. No. 2003/0135464), and (iii) yet certain other claims, including claims 59 and 68, as being rendered obvious under 35 U.S.C. § 103(a) by the combination of Goto and Kalpakian (U.S. Pat. App. Pub. No. 2003/0073494). *Id.* at pp. 73-81. In particular, the Examiner found that the Kalpakian application's disclosures of a client-server system for playing a game in which the game server, to reduce security risks to the user, does not store the user's credit card information, but rather uses a third party secure financial transaction provider, disclosed the recited element of "wherein the information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of

the user of the requesting media player device as a member of the sharing group.”
Id. at pp. 77-78.

Applicants, in their Response dated October 12, 2009, argued, without any substantive explanation, that the cited portions of the Kalpakian application (as well as the other cited references) failed to disclose the “wherein” element of claim 59. Ex. 1002, pp. 47-48. A Notice of Allowance issued on December 7, 2009. *Id.* at pp. 23-28. The Examiner, in his Statement for Reasons for Allowance, stated that claim 59 had been allowed for the reasons stated in the applicants’ Response dated October 12, 2009.

V. THERE IS A REASONABLE LIKELIHOOD THAT PETITIONER WILL PREVAIL WITH RESPECT TO AT LEAST ONE CLAIM OF THE ‘689 PATENT

The subject matter of claims 9 and 10 of the ‘689 Patent is disclosed and taught in the prior art as explained below. As set forth in § V.A. to V.D., the references and combinations utilized in Grounds I - III render obvious each of claims 9 and 10 pursuant to 35 U.S.C. §103, and provide a reasonable likelihood that the Petitioner will prevail on at least one claim. 35 U.S.C. § 314(a).

A. Prior Art

1. State of the Art in 2001

Paragraphs 14 to 27 of the Almeroth Declaration describe the state of the art regarding creating and managing media sharing groups of media player devices in the 2001 time frame.

By 2001, numerous software applications were available that could turn general purpose computers into devices capable of playing media content. Almeroth Dec., ¶ 15. Portable media players were also available for playing digital media, such as mp3 music files. *Id.*

Media sharing amongst these computer users had also become widespread by 2001. Almeroth Dec., ¶ 22. Especially well-known were peer-to-peer file sharing programs that allowed computer users to share media files, such as mp3s, across both local and wide-area networks. *Id.* The most famous of these programs, Napster, was released in 1999. *Id.* By 2000, Napster had over 25 million users and was featured on the cover of Time Magazine. *Id.* Napster allowed users to locate songs in mp3 format on other users' computers by searching a central server that contained information about these songs. *Id.* After locating each other through the central server, Napster users could share songs on a peer-to-peer basis (*i.e.*, directly from one user's computer to another user's computer). *Id.* Other fully decentralized peer-to-peer file sharing systems like Gnutella, which was released in 2000, allowed users to search for media on other users' computers without a central server. *Id.* ¶ 23.

These famous peer-to-peer systems followed earlier media-sharing applications that involved videoconferencing. Almeroth Dec., ¶ 16. A popular early internet videoconferencing application called CU-SeeMe was released in

1993. *Id.* CU-SeeMe allowed users to engage in two-way videoconferencing with real-time interactive video and voice communications over the Internet. *Id.* ¶¶ 16-17. CU-SeeMe also used a server-like component called a “reflector,” that would enable group videoconferencing, in which some users would only receive retransmissions, as seen below:

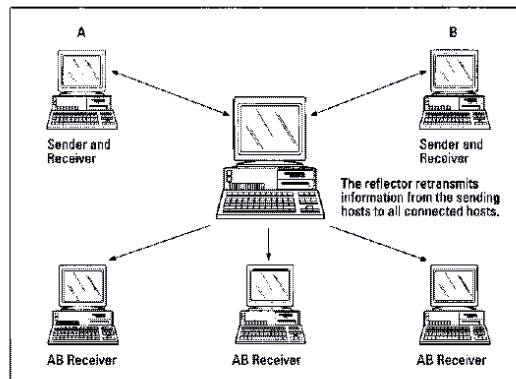


Figure 2-5: How a reflector works.

Internet users quickly recognized that the technology in CU-SeeMe could be used for more than simply “talking-heads style videoconferencing.” *Id.* ¶ 17. By 1996, CU-SeeMe had been used to broadcast speeches, lectures, and the Internet’s first full-length movie (an indie comedy called *Party Girl* starring Parker Posey). *Id.*

One drawback with CU-SeeMe’s architecture was that the reflector required tremendous bandwidth because it would need to send a separate stream of IP packets to each user who wanted to receive the signal. *Id.* at ¶ 18. Thus, a five-person videoconference would require five times the bandwidth of a single signal. *Id.* Bandwidth constraints led others to implement videoconferencing technology using a more efficient multicasting protocol. *Id.*

In many ways, multicasting is similar to television or radio broadcasting because it involves transmission from one source to many users. *Id.* ¶ 19. However, instead of a broadcast medium, multicasting uses a network like the Internet. *Id.* By 1995, it was well known that media content could be efficiently distributed over a network through the use of multicast trees. *Id.* ¶ 20. A multicast tree begins with traffic from a content source that is injected at the root switch of the tree. *Id.* The root sends this traffic to its child switches. *Id.* These switches then replicate that traffic to their children. *Id.* Each subsequent switch receives traffic from its parent switch and replicates that traffic to its child switches. *Id.* A popular multicast system called M-Bone (short for “multicast backbone”) was created in 1992. *Id.* ¶ 21. By 1994, the Rolling Stones had used M-Bone to broadcast a live concert over the Internet. *Id.* By 1996, M-Bone had been used for video teleconferences. *Id.*

By 2001, both peer-to-peer file sharing users and multicast videoconferencing users had demonstrated a need for secure private group sharing. Almeroth Dec., ¶ 24. Decentralized peer-to-peer file sharing networks like Gnutella could be disrupted if either malicious users or too many users joined a network. *Id.* There was also a need to provide secure file sharing amongst political activists in repressive countries. *Id.* And there was a well-known desire to use multicast videoconferencing for highly confidential applications, such as a meeting between geographically dispersed corporate executives. *Id.* By 2001, both peer-to-peer file sharing systems and

multicast videoconferencing systems had been created to meet these needs for secure private group sharing. *Id.* ¶¶ 25-27.

For example, by 2001, Gnutella clients allowed users to create private sharing groups that could be joined only by users that knew the group's secret handshake or password. *Id.* ¶ 26. These private Gnutella groups ensured a high quality of service by controlling the size of the network and the type of users on the network. *Id.*

Similarly, multicast videoconferencing technology allowed users to create private sessions both through controlling the multicast tree and through encryption. *Id.* ¶ 25. As described above, multicast trees begin with a root source, where traffic is injected into the tree. *Id.* ¶ 20. By 1995, a multicast protocol existed that would allow new recipients to join the multicast tree only with approval from the source. *Id.* ¶ 25. Encrypted multicast protocols also existed that would provide for secure multicast groups. *Id.* Admission to a secure group could require either all existing members of the group to approve the new member or an elected, trusted group leader to approve the new member. *Id.*

It is with this background and understanding that one skilled in the art would consider the following references and grounds for unpatentability.

2. The Yeager Patent (Ex. 1003)

The Yeager patent (U.S. Pat. No. 7,383,433) was filed in the U.S. on June 7, 2002, and issued on June 3, 2008. As explained below, the relevant disclosure of Yeager is also disclosed in priority provisional Application No. 60/308,932, which was filed on July 31, 2001. The Yeager patent therefore qualifies as prior art to the ‘689 Patent under 35 U.S.C. § 102(e) as of July 31, 2001. The Yeager patent is not cited on the face of the ‘689 Patent.

Yeager discloses several improvements to prior art peer-to-peer networks, such as Napster and Gnutella, that were famously used to share media content. *See, e.g.*, Ex. 1003, 2:18-40, 34:16-31; Almeroth Dec. ¶ 34. First, Yeager discloses that peer groups can be formed on these peer-to-peer networks to share protected content in a secure environment. Ex. 1003, 28:1-6, 37:9-20, 37:35-50. Although “new peers . . . may not initially belong to any peer group,” Ex. 1003, 7:20-21, peers can request to join existing peer groups. Ex. 1003, 35:59-61, 52:15-51. These peer groups can be used to share media content, such as mp3 music files. *See* Ex. 1003, 34:16-37.

Second, Yeager discloses methods for determining whether to trust another user based on content quality and risk. *See, e.g.*, Ex. 1003, 7:6-8. Yeager recognized that prior art methods for assessing trust were “too biased toward personal risk and not content.” Ex. 1003, 1:47-50. Yeager describes prior art

rating systems that rated trust based on “parameters such as performance, honesty, reliability, etc.,” so that, for example, a peer who cheats at playing cards “might be deprived of his ability to authenticate and join another card game.” Ex. 1003, 1:41-45. But Yeager recognized that other users, such as a “group of people interested in cooking,” might find it “desirable that trust be biased towards data relevance,” so a “cooking peer group” could focus on “the quality of recipes.” Ex. 1003, 1:46-50, 5:30-32. Thus, Yeager disclosed improved methods for assessing content quality in addition to personal risk. Ex. 1003, 11:27-14:67; Almeroth Dec., ¶ 37.

Third, Yeager discloses multiple ways to allow trusted users to provide information regarding whether a user’s request to join a peer group should be granted. In one method, one or more trusted users will directly make a decision about whether the requesting user should be allowed to join the group based on information about the requesting user. Ex. 1003, 35:59-36:3, 57:25-29 (“Each peer group policy may permit some members to be trusted to the extent that they have the authority to . . . add new members, and remove or revoke membership.”). The decision about whether to cooperate in a peer group with the requesting user is based on, among other things, an assessment of the peer’s content quality and personal risk. Ex. 1003, 10:14-18, 11:23-26, 27:63-28:8, 40:4-9; Almeroth Dec. ¶ 38. Another method disclosed by Yeager involves allowing trusted users to sign

security certificates that the requesting user submits to authenticate her identity during a join request. Ex. 1003, 17:12-33, 18:40-65, 52:23-51.

As all three of the features explained above are also disclosed in the priority provisional application, Yeager qualifies as prior art as of the July 31, 2001 filing date of that application. See Ex. 1004, at 5-13 (disclosing peer groups as an improvement to prior art peer-to-peer systems like Napster); 37 (disclosing that an elected representative member is trusted to accept or reject new member applications to a peer group); 77-81 (disclosing that new users can request to join peer groups); 96-107 (disclosing user trust ratings based on content quality and risk); 12, 94, 99 (disclosing that trust ratings may be used to determine whether a peer should be trusted to cooperate with other peers in a peer group); 77-79, 108-114 (disclosing that a join request will include credentials, such as a security certificate signed by a trusted user).

3. The *P2P Networking* Reference (Ex. 1005)

The *P2P Networking* reference was published in July 2001. Accordingly, the reference qualifies as prior art to the '689 patent under 35 U.S.C. § 102(a).

The *P2P Networking* reference discloses why it is desirable to set up peer-to-peer networks with controlled memberships. *P2P Networking* discloses that the extreme flexibility of open peer-to-peer networks is disadvantageous because it leads to a great variance in content quality and connection speeds. Ex. 1005, p. 34.

Open peer-to-peer networks also suffer from malicious users that can distribute undesirable content. *Id.* at 35.

P2P Networking also discloses a solution to the problems of open networks: private peer-to-peer networks with controlled memberships that can classify content and exclude undesirable users using feedback scores “similar to the scores that eBay provides for auctioneers.” Ex. 1005, p. 34. Further, *P2P Networking* discloses that by restricting participation to exclude free riders, a private network would discourage copyright infringement prevalent on other peer-to-peer networks. *Id.* at 35.

4. The Busam Application (Ex. 1006)

The Busam application (U.S. Pat. App. Pub. No. 2002/0087887) was filed in the U.S. on September 19, 2001, and published on July 4, 2002. It therefore qualifies as prior art to the ‘689 Patent under 35 U.S.C. § 102(e). The Busam application is cited on the face of the ‘689 Patent; however, it was not used for a rejection by the Examiner during prosecution of the ‘689 Patent.

Busam discloses a device-to-device network in which users are organized in sharing groups so that their devices can share and stream media files to and from each other. Ex. 1006, [0008], [0028], [0032], Fig. 1. Busam further discloses an embodiment in which new devices must send requests to obtain access to shared devices on device-to-device networks. Ex. 1006, [0008]-[0009], [0025], [0028].

The sharing device described in Busam “can be a computer, a browser running on a computer, a digital music player running on a computer, a stand-alone music player, a video player, etc.” Ex. 1006, [0025]. And these devices can share music by either transferring or streaming music files. Ex. 1006, [0008].

Busam further discloses an embodiment in which two devices, Device A and Device B, set up a device-to-device network and authenticate with each other by exchanging usernames and passwords associated with each device. Ex. 1006, [0048], Fig. 12. If those usernames and passwords are from the same sharing group, those devices will be able to share media content with each other. Ex. 1006, [0028], [0048]. Busam further discloses that a third device, Device C, can request to join their device-to-device network if it is part of the same group. Ex. 1006, [0048], Fig. 12. After Device C authenticates with both devices by sharing a username and password, “all three devices are on the device-to-device network and can access each other.” Ex. 1006, [0048].

5. The Phillips Patent (Ex. 1007)

The Phillips patent (U.S. Patent No. 7,058,696) was filed in the U.S. on November 1, 2000,¹ and issued on June 6, 2006. It therefore qualifies as prior art to the ‘689 Patent under 35 U.S.C. § 102(e).

Phillips discloses a multi-user shared file access service in which users belong to user groups that can access shared files. Ex. 1007, 1:40-42, 5:66-6:9. The users can operate client nodes—such as computers, game consoles or internet receivers—and access file groups. Ex. 1007, 6:1-9, 8:43-46. The shared files are stored in virtual storage devices on a remote file server node, with each virtual storage device being accessible by a different group of users. Ex. 1007, 9:60 - 10:9.

These virtual storage devices are managed by a client manager node that is “able to designate new user accounts and to provide sufficient information to enable a client user to join one or more of the virtual storage devices.” Ex. 1007, 12:36-39. The user of the client manager node can invite new users to join by

¹ The Phillips patent claims priority under 35 U.S.C. §§ 120 and 119(e) to earlier-filed applications. Should patent owner attempt to remove the Phillips patent as a reference, Petitioner reserves the right to establish an earlier § 102(e) date for the Phillips patent.

sending them an emailed invitation containing a “one time password” (OTP). Ex. 1007, 16:22-28, 16:50-60. “The purpose of the client manager node is to provide the customer” with the ability to designate a trusted user that—in addition to designating new user accounts—can also “administer each of the [customer’s] virtual storage devices,” and “is provided with full access privileges for all of the files and directories on each virtual storage device.” Ex. 1007, 12:21-39. As explained by Dr. Almeroth, only trusted users would receive such extensive privileges. Almeroth Dec., ¶ 49.

New client users can then request to join a user group by initiating a “join process” in which the user clicks on an emailed invitation “at a particular client node.” Ex. 1007, 17:9-11, 18:16-18, Fig. 6B. A determination is then made as to whether the new client user’s node will be allowed to join the user group based on the user’s user ID and OTP. Ex. 1007, 16:50-51, 17:9-11, 18:16-18, 18:22-36, Fig. 6B.

6. The Abecassis Patent (Ex. 1008)

The Abecassis patent (U.S. Patent No. 6,192,340) was filed in the U.S. on October 19, 1999, and issued on February 20, 2001. It therefore qualifies as prior art to the ‘689 Patent under 35 U.S.C. § 102(b). The Abecassis patent is cited on the face of the ‘689 Patent; however, it was not used for a rejection by the Examiner during prosecution of the ‘689 Patent.

The Abecassis patent discloses a network of digital audio devices that can retrieve and transmit audio and information from each other. Ex. 1008, 7:16-22, 11:1-30 and Fig. 4. In particular, Abecassis discloses that devices in this network whose users correctly enter user identification and password information may access audio information, such as radio-on-demand. 19:38-20:16. One skilled in the art would understand such a set of network devices where users are granted access to share, for example, audio information, to be a “sharing group” as set forth in the ‘689 Patent. Almeroth Dec., ¶ 58.

The Abecassis patent discloses that the user of an audio device may enter user identification and password information into his/her audio device to access services from the network. Ex. 1008, 19:38-20:16. The Abecassis patent discloses embodiments in which such access control functionality is not necessarily located in the audio device of the user, indicating to one skilled in the art that it may reside in, for example, other audio devices already accessing the network. Ex. 1008, 26:66-27:4; Almeroth Dec., ¶ 60. Further, the Abecassis patent discloses access control in connection with “handshaking,” indicating to one skilled in the art that the access control routines may be based in an audio device of the network other than the audio device attempting access to the network (*e.g.*, an information provider). Ex. 1008, 19:53-55 and 26:57 – 27:10. Almeroth Dec., ¶ 60.

The Abecassis patent discloses that if login is successful, processing continues, ultimately allowing the audio device to obtain services from an information providing device (*i.e.*, receive and transmit audio and information from other audio devices of the network), and thus, join the sharing group. Ex. 1008, 11:1-8, 20:11-15, 27:11-18, Figs. 7 and 9.

Abecassis discloses that a plurality of audio devices may be part of the network, and that each may retrieve and transmit audio and information from any other participant. Ex. 1008, 11:1-8 and 22-43 (stating that a “radio-on-demand provider” system will “commercially service a substantial number of end users”). Figure 4 of Abecassis discloses a plurality of “Multimedia Player” devices 431-438 that may be available to a user, including a “smart Multimedia Player 431” and “a Multimedia Player in the vehicle 437.” Ex. 1008, 13:23-47, 14:8-10.

7. The Ganesan Patent (Ex. 1009)

The Ganesan patent (U.S. Patent No. 5,535,276) was filed in the U.S. on November 9, 1994, and issued on July 9, 1996. It therefore qualifies as prior art to the ‘689 Patent under 35 U.S.C. § 102(b). The Ganesan patent was neither cited nor considered during prosecution of the ‘689 Patent.

The Ganesan patent discloses systems for maintaining the privacy of information transmitted across a communications channel. Ex. 1009, 1:9-19. In one system, a transmitter sends a message that is encrypted to a receiver along with

a certificate that authenticates the identity of the transmitter to the receiver. Ex. 1009, 2:41-54. The authenticating certificate is generated by a trusted third party, such as a Certificate Authority (CA) that serves as a trusted intermediary. Ganesan, 2:48-54 and 1:58-2:20. Moreover, the trusted third party, could, for example, be another user, such as an authentication server. Ex. 1009, Abstract, claims 1, 2 and 4, 8:20-43. One skilled in the art would understand that the authenticating certificate corresponds to the “information associated with a user” that is “made available by a trusted user” as recited in claim 9 of the ‘689 Patent. Almeroth Dec., ¶ 62.

B. Ground I: The Combination of the Yeager Patent and the *P2P Networking* Reference Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103

The combination of the Yeager patent and the *P2P Networking* Reference discloses all of the limitations of Claims 9 and 10 of the ‘689 patent. The Yeager patent discloses “Peer Devices” and “Peer Members” (*see, e.g.*, FIGs. 1B, 12, and 13, and 2:18-40) that one skilled in the art would understand to be “media player devices” as claimed in the ‘689 patent. Almeroth Dec., ¶ 35. It discloses “sharing groups” in the form of “peer groups” that are used to publish content. Ex. 1003, 28:1-6, 37:9-20, 37:35-50. And it discloses that existing members of a peer group will receive requests to join the peer group from potential new members. *Id.* at 35:59-61, 52:26-41.

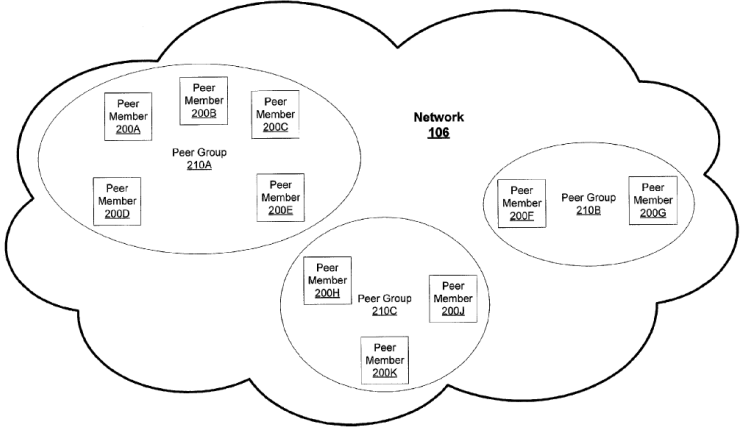
The Yeager patent further discloses making a determination about whether to admit that requesting peer based on two types of information associated with the user of that peer: credentials that may be signed by a trusted user (Ex. 1003, 17:12-33, 18:40-65, 52:23-51.); and trust levels that a trusted user will review to determine whether the join request should be granted (*Id.* at 10:14-18, 11:23-26, 27:63-28:8, 35:59-36:3, 40:4-9, 57:25-29). Additionally, Yeager discloses adding the requesting peer to the sharing group by distributing a full membership credential to the requesting device. *Id.* at 52:52-63.

P2P Networking discloses why the limitations in Yeager would be combined in the way that they are in Claims 9 and 10 of the '689 patent. *P2P Networking* discloses that it is desirable to create a “self-enforced, restricted membership social community like a neighborhood P2P network” so that “users can impose standards on the quality of content and service.” Ex. 1005, p. 36. *P2P Networking* further discloses that such a network can be established through rating users based on content contributions and connection speeds in order to exclude free riders, malicious users, and low-speed nodes. *Id.* at 34-35.

In addition, a person skilled in the art would have had reason to combine the elements disclosed in Yeager to achieve the purpose disclosed in *P2P Networking* because both references arise from the same narrow field of art: content sharing on peer-to-peer networks. Almeroth Dec., ¶ 44. Moreover, both references disclose

allowing users to rate peers and content quality in order create curated communities, like private peer-to-peer networks and peer groups focused on a particular interest. *Id.*

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
A method of operating a digital computing device associated with a sharing group, comprising:	<p>Yeager discloses a method for operating digital computing devices with a sharing group.</p> <p>“A peer may be anything with a digital heartbeat that supports the peer-to-peer platform core, including sensors, servers, PCs, computers up to and including supercomputers, PDAs, manufacturing and medical equipment, phones and cellular phones. In order to interact with other peers (e.g. to form or join peer groups), the peer needs to be connected to some kind of network (wired or wireless), such as IP, Bluetooth, or Havi, among others.</p> <p>The peer-to-peer platform may provide mechanisms through which peers may discover each other, communicate with each other, and cooperate with each other to form peer groups.” Ex. 1003, 27:54-66.</p> <p>“Each peer group may establish its own membership policy in a range from open (any peer can join) up to highly secure and protected (a peer may join only if it possesses sufficient credentials).” <i>Id.</i> at 35:55-58.</p> <p>“Peer group boundaries permit member peers to access and publish protected contents.” <i>Id.</i> at 37:10-11.</p> <p>“A peer group is a collection of peers connected by a network that share a common set of interests and that have agreed upon a common set of rules to publish, share and access any computer content (code, data, applications, or other collections of computer representable resources), and communicate among</p>

Claim 9	<p>The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)</p>
	<p>themselves.” <i>Id.</i> at 28:1-6.</p>  <p>FIG. 12</p> <p>Ex. 1003, Fig. 12.</p> <p><i>P2P Networking</i> discloses that “a private P2P network in which users exchange decision-making information can control membership, implement authentication schemes, and adopt standardized schemes to describe and classify content.” Ex. 1005, p. 34.</p> <p><i>P2P Networking</i> further discloses that a “self-enforced, restricted membership social community like a neighborhood P2P network” allows users to “impose standards on quality of content and service.” <i>Id.</i> at 36.</p>
<p>receiving a request to join the sharing group from a requesting media player device;</p>	<p>“FIG. 1B illustrates several peer devices 104 connected over the network 106 in a peer group.” Ex. 1003, 2:36-37.</p>

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
	<div data-bbox="618 317 1317 961" data-label="Diagram"> </div> <p data-bbox="1003 1052 1105 1087">FIG. 1B</p> <p data-bbox="581 1142 1414 1262">“In one embodiment, peers wishing to join a peer group may first locate a current member, and then request to join the peer group.” <i>Id.</i> at 35:59-61.</p> <p data-bbox="581 1310 1373 1472">“A peer membership protocol apply message may be sent by a potential new group member to the group membership application authenticator.” <i>Id.</i> at 52:26-29.</p> <p data-bbox="581 1520 1419 1640">“A peer membership protocol join message may be sent by a peer to the peer group membership authenticator to join a group.” <i>Id.</i> at 52:39-41.</p>
making a determination as to whether to permit the requesting media player device to join	<p data-bbox="581 1696 1386 1858">Yeager discloses making a determination about whether to accept or reject the join request based on information (credentials) associated with a user of the requesting media player device.</p>

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
<p>the sharing group based on information associated with a user of the requesting media player device; and</p>	<p>“The application to join may be rejected or accepted by the collective set of current members in accordance with the peer group’s membership policy. In one embodiment, a peer group core membership service may be used to enforce a vote among one or more group members. Alternatively, one or more group representative member peers may be elected or appointed to accept or reject new membership applications.” Ex. 1003, 35:63-36:3.</p> <p>“[T]he apply message may include, but is not limited to, the current credential of the candidate group member and the peer endpoint for the peer group membership authenticator to respond to with an acknowledgement (ACK) message.” <i>Id.</i> at 52:34-38.</p> <p>“[A] successful response from the group’s authenticator may include an application credential and a group advertisement that may list, at a minimum, the group’s membership service.” <i>Id.</i> at 52:31-34.</p> <p>“The [join] message may include a credential (application credential of the applying peer: see ACK message). This credential may be used as the application form when joining.” <i>Id.</i> at 52:47-49.</p> <p>“A credential is a token that when presented in a message body is used to identify a sender and can be used to verify that sender’s right to send the message to the specified endpoint and other associated capabilities of the sender. The credential is an opaque token that must be presented each time a message is sent. The sending address placed in the message envelope may be crosschecked with the sender’s identity in the credential.” <i>Id.</i> at 59:49-58.</p> <p>“Mobile Credentials. Some embodiments may provide the ability to move a peer’s private security</p>

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
	<p>environment from device to device. Having multiple identities, for example, may be confusing and may add unwanted complexity to a security model.” <i>Id.</i> at 24:1-5.</p> <p>Yeager further discloses using a requesting user’s credentials, such as a security certificate, to calculate a “level of trust” for that user that will determine whether the user can be admitted to the peer group.</p> <p>“[A]ny peer, including a recognized Certificate Authority, may join a peer group and offer its services (assuming it meets membership requirements, if any). The peer group members may assign a level of trust or peer confidence to that peer, as well as to each other. Mobile credentials, e.g. how to make a system’s private security credentials securely available, may also be provided.” <i>Id.</i> at 3:48-54.</p> <p>“[U]ser input [may] set trust confidence values on a certificate for a peer received from the peer and for certificates received for a peer from a different peer with the different peer’s recommendation. This recommendation may be measured.” <i>Id.</i> at 16:51-54.</p>
adding the requesting media player device to the sharing group if the determination is made to permit the requesting media player device to join the sharing group;	<p>Yeager discloses that a requesting media player device is added as a member of a peer group if the determination is made to permit it to join the peer group.</p> <p>“[T]he process of joining a peer group may include obtaining a credential that is used to become a group member.” Ex. 1003, 52:15-17.</p> <p>“[A]ll messages include, at a minimum, a peer group credential that identifies the sender of the message as a full member peer in the peer group in good standing.” <i>Id.</i> at 59:63-66.</p>

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
	<p>“[A] successful response from the group’s authenticator may include an application credential and a group advertisement that may list, at a minimum, the group’s membership service.” <i>Id.</i> at 52:31-34.</p> <p>“A successful response from the group’s authenticator may include a full membership credential and a full group advertisement that lists, at a minimum, the group’s membership configurations requested of full members in good standing.” <i>Id.</i> at 52:43-47.</p> <p><i>See also</i> Ex. 1003, 26:14-34.</p>
wherein the information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.	<p>Yeager discloses information associated with the user of the requesting media player device (credentials, such as security certificates) that comprises information made available by a trusted user (<i>e.g.</i>, “web of trust” and trust relationships between peers), regarding a desirability of the user of the requesting media player device as a member of the sharing group.</p> <p>“On a network comprising a plurality of peer nodes, each peer may build a trust relationship with one or more of the other peers to form a ‘web of trust.’” Ex. 1003, 6:56-59.</p> <p>“[U]ser input [may] set trust confidence values on a certificate for a peer received from the peer and for certificates received for a peer from a different peer with the different peer’s recommendation. This recommendation may be measured. Trust is not necessarily transitive. If a peer A trusts a peer B and peer B trusts peer C, it does not necessarily follow that peer A should trust peer C with the same degree of trust that peer B trusts peer C. The transitivity of the trust may be measured from the point of view of peer A. This transitivity may be referred to as ‘weak transitivity.’ These measurements of trust and transitivity consider which peers sign and/or cosign a</p>

Claim 9	The Combination of the Yeager Patent and the P2P Networking Reference (Exs. 1003 and 1005)
	<p>certificate from the recipient's point of view. Thus, using embodiments, real, 'human' trust may be modeled based on reputation. Thus, trust may be 'personal.'" <i>Id.</i> at 16:51-64; <i>see also id.</i> at 18:61-65.</p> <p>"The peer-to-peer platform security model may be implemented to provide a P2P web of trust. The web of trust may be used to exchange public keys among its members. Each peer group policy may permit some members to be trusted to the extent that they have the authority to sign public keys for other members as well as to do things like authenticate, add new members, and remove or revoke membership." <i>Id.</i> at 57:23-29.</p> <p>"Trust relationships between peers 200 thus may be based on content (the codat trust component) instead of or in combination with the risk trust component. Peers 200 may also propagate codat confidence and peer confidence information to other peers 200." <i>Id.</i> at 7:6-10.</p> <p>"[P]eer trust may be a function of peer confidence and risk. In one embodiment, peer 200 may also include one or more peer risk tables 412 which each may include one or more peer risks each associated with a particular peer. Peer risk for a particular peer may be determined using one or more factors including, but not limited to, codat integrity (e.g., did codat received from the peer contain a virus as noted by a virus pre-processor), peer accessibility (is the peer up most of the time?), and peer performance (e.g. are there long delays in retrieving data from the peer?). Entries in peer risk tables 412 may be used in evaluating a peer's risk trust component. In one embodiment, the peer confidence and risk tables may be used in determining if a target peer is able to cooperate and is thus trustworthy." <i>Id.</i> at 10:4-18.</p>

Claim 9	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
	<p>“[T]he peer confidence and risk classes may be used in determining if another peer, for example a peer offering to provide codat in a particular area of interest, is able to cooperate and is thus trustworthy.” <i>Id.</i> at 11:23-26.</p> <p>Yeager further discloses that requesting users with a sufficient trust level, such as those users who present a credential signed by a particularly trusted user (<i>e.g.</i>, a Certificate Authority) will be allowed to join the group. <i>See, e.g.</i>, Ex. 1003, 17:17-30.</p>
Claim 10	The Combination of the Yeager Patent and the <i>P2P Networking</i> Reference (Exs. 1003 and 1005)
10. The method of claim 9 wherein the digital computing device is one of at least two media player devices in the sharing group.	Yeager discloses peer groups that are composed of two or more devices. Ex. 1003, FIGs. 1B, 12, and 13.

C. Ground II: The Combination of the Busam Application and the Phillips Patent Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103

The Busam application discloses a device-to-device network for sharing and streaming media. Devices on this network can be any kind of media player device, ranging from a web browser to a portable music player to a car stereo. Ex. 1006, [0025], [0027]. These devices are associated with users, who are organized into sharing groups. Ex. 1006, [0028]. Devices can only see (and hence share media with) other devices in their sharing group. Ex. 1006, [0028]; [0034]. The only aspect of claims 9 and 10 of the '689 patent that is not clearly disclosed by the

Busam application is an indication of how new devices can join an existing sharing group.

This aspect is disclosed by the Phillips patent, which teaches a method for allowing a trusted user to screen members of a file sharing group in which users receive access to a virtual storage device. Ex. 1007, 12:21-39, Almeroth Dec., ¶¶ 49-50. Users will access the virtual storage devices through client nodes, which can be a variety of computers, including game consoles and internet receivers. Ex. 1007, 8:43-46. New users can request to join an existing user group, but they will only be allowed to join if the user of the client manager node has sent them a one-time password to indicate that they are allowed to join the group. Ex. 1007, 16:50-17:5, 17:9-11, 18:16-18, 18:22-36, FIG. 6B. If a new user does not know the one-time password, the new user will not be able to join the group. Ex. 1007, 18:28-36. The user of the client manager node is a trusted user because she is given extensive privileges over system security that could easily be misused by an untrustworthy user. *See id.* 12:21-39; Almeroth Dec. ¶ 49.

A person of ordinary skill in the art would have had reason to combine the teachings of the Busam application with the teachings of the Phillips patent because both references teach ways for devices to securely share content amongst users in a group. Almeroth Dec., ¶ 55. A person of ordinary skill in the art would also have had reason to use Phillips' method of generic file sharing to share media

content, as is disclosed in Busam, because it was famously known at the time that file sharing systems could be used to share media (*e.g.*, Napster). Almeroth Dec., ¶ 54.

Further, a person of ordinary skill in the art would have had reason to combine Busam's media sharing group with Phillips' method for screening new group members with a password from a trusted user because Busam's media sharing group was designed to avoid the problem in the prior art that "[a] consumer who exposes content to the network, must do so for all to access." Ex. 1006, [0006]. Thus, as explained by Dr. Almeroth, a person skilled in the art would understand from the Busam application the need to limit which users would be able to access content to be shared on a network, and that the Phillips patent simply teaches one of several known ways of doing that. Almeroth Dec., ¶ 55. Another well-known way to do this was to choose a shared password for the group and distribute that password to group members, and this method was used to form private media sharing groups such as on the Gnutella peer-to-peer network. *Id.* A person skilled in the art would have found reason in Busam to use the Phillips method of sharing one-time passwords, which prevents users from re-sharing a group password, thus giving more control to the user sharing content over who can access that content. *Id.*

Moreover, the combination of the Phillips patent and the Busam application provides the teaching that applicants argued was missing from the prior art regarding the “wherein” clause present in claim 9 - “wherein the information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.” In particular, the Phillips patent discloses that a requesting user can join an existing user group if the user is able to provide an OTP that it received from a trusted user. Ex. 1007, 16:50-51, 17:9-11, 18:16-18, 18:22-36, FIG. 6B.

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
A method of operating a digital computing device associated with a sharing group, comprising:	<p>Busam and Phillips disclose digital computing devices associated with a sharing group.</p> <p>“One feature of the device-to-device network is that any particular device can only see other devices on the network for which that device is authorized to communicate with. In one embodiment, a device can only access other devices on the network that have been authenticated with the same username. In another embodiment, groups can be set up. When a device logs into the device-to-device network, it can only see other devices that have been logged in by users in the same group.” Ex. 1006, [0028]; <i>see also</i> [0008], [0032].</p>

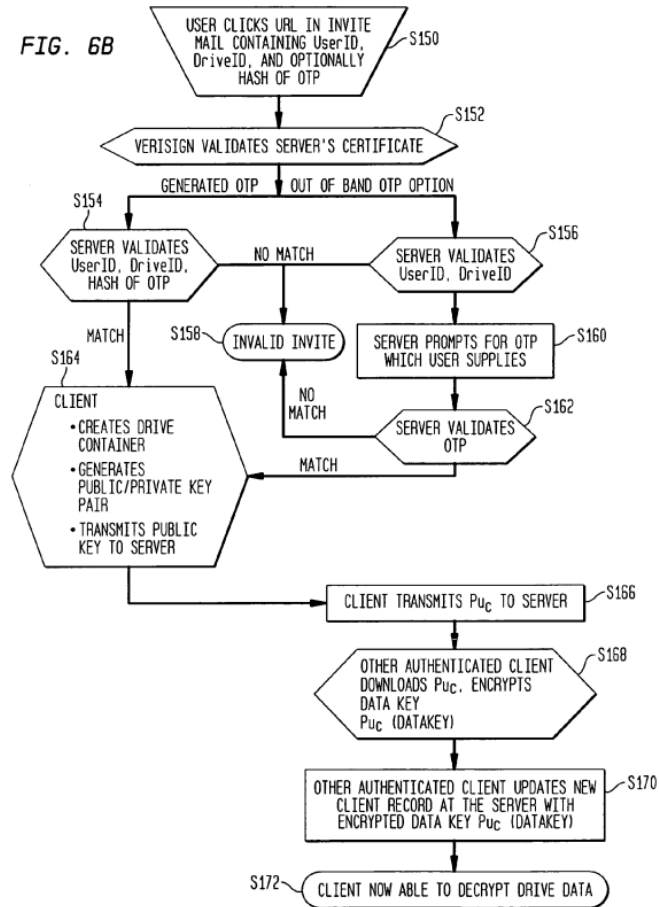
Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
	<p style="text-align: center;">Fig. 1</p> <p>The diagram illustrates a network architecture where multiple client devices connect to a central D2D Server (2) through a Network (4). The clients are categorized into three groups: Joe's devices (10, 12, 14), Lisa's devices (20, 22, 24), and Sam's devices (26, 28). A commercial service (18) and a proxy server (40) are also connected to the network. The network is secured by two firewalls (30, 32, 34, 36). The diagram shows various types of devices including A/V devices, handheld devices, home computers, wireless devices, laptops, and work computers.</p> <p>“Illustratively, the remote file server nodes can implement several virtual storage devices. For example, a group F1 of one or more virtual storage devices can be provided for a single group of users G1. A group F2 of one or more additional virtual storage devices can be provided for an entirely contained subset of users of that group G2 G1. . . . It is also possible for one specific user g1 to be part of two different groups, say G1 and G4” Ex. 1007, 9:60-10:9; <i>see also</i> 1:40-42, 5:66-6:9, 6:1-9, 8:43-46.</p>
receiving a request to join the sharing group from a requesting media player device;	<p>Busam discloses that media player devices can form sharing groups for sharing content on device-to-device networks.</p> <p>“For example, a device can be a computer, a browser running on a computer, a digital music player running on a computer, a stand-alone music player, a video player, etc.” Ex. 1006, [0025].</p>

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
	<p>“While using the device-to device network, an entity can transfer files, stream files, create and use playlists, send commands to various devices and explore the contents of various devices.” <i>Id.</i> at [0008].</p> <p>“In another embodiment, groups can be set up. When a device logs into the device-to-device network, it can only see other devices that have been logged in by users in the same group.” <i>Id.</i> at [0028].</p> <p>“The method includes the step of receiving a request to access a network of devices, where the network of devices includes a set of devices the user is authorized to access and a set of devices that the user is not authorized to access.” <i>Id.</i> at [0009].</p> <p>“In step 152, the server sends a list of accessible devices to the requesting device. That is, after a user is authenticated, server 2 will determine which devices the user may access. In one embodiment, the user may access all devices that are logged into the device-to-device network using the same username. Additionally, the user can access any device for which the user is a member of a group that is allowed to access the device. Step 152 includes determining this list of accessible devices and sending that list to the requesting device.” <i>Id.</i> at [0034].</p> <p>“FIG. 12 is a flowchart describing the process for starting the device-to-device network without a server. This process is called self-discovery. The example described in FIG. 12 includes three devices that attempt to create a device-to-device network. For example purposes, the devices will be called device A, device B and device C (e.g., Joe’s home computer 10, Joe’s handheld device 12, Joe’s AV device 14). In step 470, device A starts and broadcasts a message on the network. Since no one else is on the network, nobody responds. In step 472, device A begins to listen for broadcasts. In step 474, device B starts</p>

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
	<p>and broadcasts on the network. This time, device A is listening so device A will receive device B's broadcast in step 476. In step 478, device B starts listening for broadcasts. In step 480, device A attempts to connect to device B. The attempt to connect includes informing device B of the instance of device A and authenticating with device B. By authenticating, it is meant that device A sends a username and password associated with the instance of device A. If device B is using the same username and password or a username and password from the same group (depending on the embodiment), then device A will be authenticated with device B. Device B authenticates to device A on the same socket in step 482. In step 484, device C starts and broadcasts on the network. In step 486, device A and device B receive device C's broadcast. In step 488, device C starts listening for broadcasts on the network. In step 490, device A connects to device C, informing device C of its instance and authenticating with device C. In step 492, device C authenticates with device A on the same socket that device A authenticated with device C. In step 494, device B connects to device C, informs device C of the instance of device B that is logging in and authenticates with device C. In step 496, device C authenticates with device B on the same socket that device B authenticated with device C. After step 496, all three devices are on the device-to-device network and can access each other. In some embodiments, a device is accessible on the device level. That is if the user is authenticated with a device, the user can access anything on the device. In other embodiments, different items on the device can have different access levels so that different sets of users can access different items." <i>Id.</i> at [0048].</p> <p>Phillips discloses a process in which a new client user can, from a variety of client node devices, request to join a user group by clicking on an emailed invitation.</p> <p>"Herein, the invention is illustrated using PC computers,</p>

Claim 9	<p>The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)</p> <p>such as desktops, laptops and file servers, as nodes. However, the invention is also applicable for other types of nodes such as game consoles and Internet receivers.” Ex. 1007, 8:43-46.</p> <p>“Illustratively, the client manager node can email the invitation to the new client user node via the Internet, by addressing the email message to an Internet address of the client user.” <i>Id.</i> at 16:57-60.</p> <p>“In regard to FIG. 6A, assume that the new client user receives the above-described invitation, e.g., as an encrypted email message, at a particular client node.” <i>Id.</i> at 17:9-11.</p> <p>“In the alternative process of FIG. 6B, the user, upon receipt of an email invitation, activates the join process in step S150 by clicking on the email message.” <i>Id.</i> at 18:16-18, Fig. 6B.</p>
<p>making a determination as to whether to permit the requesting media player device to join the sharing group based on information associated with a user of the requesting media player device; and</p>	<p>Phillips discloses that a new client user’s node is allowed to join a user group based on the user’s user ID and OTP (“one time password”).</p> <p>“Next, in step S108, the client manager node creates a one time password (‘OTP’). Preferably, the OTP is a bidirectional encryption/decryption key. In addition, the client manager node communicates to the new client user an invitation to join the group of user permitted to access the virtual storage device, which invitation includes the user name (‘user id’), the identifier of the virtual storage device (‘drive id’), and optionally the OTP.” Ex. 1007, 16:50-57.</p> <p>“In regard to FIG. 6A, assume that the new client user receives the above-described invitation, e.g., as an encrypted email message, at a particular client node.” <i>Id.</i> at 17:9-11.</p> <p>“In the alternative process of FIG. 6B, the user, upon receipt</p>

Claim 9	<p>The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)</p> <p>of an email invitation, activates the join process in step S150 by clicking on the email message. The email message includes the user id, the drive id, and optionally a hash of the OTP. In step S152, a trusted third party, such as Verisign™, validates the “certificate” or authenticity of the remote file server identified by the drive id. If the hash of the OTP was included in the email invitation, the process proceeds to step S154 and the remote file server validates the user id, drive id, and the hash of the OTP. If there is a match, i.e., the remote server validates the above, then the process proceeds to step S164 which will be described below.</p> <p>Referring back to step S152, if the hash of the OTP was not included in the email invitation, then the remote file server validates only the user id and drive id. As stated above, the new client user obtains the OTP separate from the invitation email. If there is a match, then in step S160 the remote file server prompts the client user to supply the OTP which is validated in step S162. If there is no match in either step S156 or step S162, then the invite is invalidate in step 158. Otherwise, the process proceeds to step S164.” <i>Id.</i> at 18:16-36, Fig. 6B.</p>
----------------	--

Claim 9**The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)**

Busam discloses that a third device can request to join an existing device-to-device network based on its username and password. Ex. 1006, [0048], Fig. 12.

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
	<p style="text-align: center;">Fig. 12</p> <pre> graph TD 470[A starts and broadcasts, nobody responds] --> 472[A starts listening for broadcasts] 472 --> 474[B starts and broadcasts] 474 --> 476[A receives B's broadcast] 476 --> 478[B starts listening for broadcasts] 478 --> 480[A connects to B, adds instance and authenticates] 480 --> 482[B Authenticates to A on same socket] 482 --> 484[C starts and broadcasts] 484 --> 486[A and B receive C's broadcast] 486 --> 488[C starts listening for broadcasts] 488 --> 490[A connects to C, adds instance and authenticates] 490 --> 492[C authenticates with A on same socket] 492 --> 494[B connects to C, adds instance and authenticates] 494 --> 496[C authenticates with B on same socket] </pre> <p>The username and password are associated with a user of the device. <i>See, e.g., Ex. 1006, [0033].</i></p>
adding the requesting media player device to	Phillips discloses that the client node is added to the virtual storage device on the remote file server node after a determination is made to permit the client node to access

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
<p>the sharing group if the determination is made to permit the requesting media player device to join the sharing group;</p>	<p>the virtual storage device. Ex. 1007, 9:60-61, 18:37-19:5, Fig. 6B.</p> <p>“Illustratively, the remote file server nodes can implement several virtual [sic] storage devices. For example, a group F1 of one or more virtual storage devices can be provided for a single group of users G1. A group F2 of one or more additional virtual storage devices can be provided for an entirely contained subset of users of that group G2 G1.” Ex. 1007, 9:60-65.</p> <p>“The process described in this section is only used once to join a client node to a virtual storage device. Subsequently, all accesses by that client node to the virtual storage device which it has joined are achieved using the authentication and secure file transfer processes described below. Moreover, each OTP can be used only once.” <i>Id.</i> at 19:4-9; <i>see also id.</i> at 18:16-19:3, Fig. 6B.</p> <p>Busam discloses adding a third device to an existing device-to-device network after authentication.</p> <p>“In step 484, device C starts and broadcasts on the network. In step 486, device A and device B receive device C’s broadcast. In step 488, device C starts listening for broadcasts on the network. In step 490, device A connects to device C, informing device C of its instance and authenticating with device C. In step 492, device C authenticates with device A on the same socket that device A authenticated with device C. In step 494, device B connects to device C, informs device C of the instance of device B that is logging in and authenticates with device C. In step 496, device C authenticates with device B on the same socket that device B authenticated with device C. After step 496, all three devices are on the device-to-device network and can access each other.” Ex. 1006, [0048], Fig. 12.</p>
<p>wherein the</p>	<p>As described above, Phillips discloses that the</p>

Claim 9	The Combination of the Busam Application and the Phillips Patent (Exs. 1006 and 1007)
information associated with the user of the requesting media player device comprises information, made available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.	<p>determination to add the user depends on a one-time password or OTP sent from the “client manager node” to the new client user. Ex. 1007, 16:50-60, Fig. 6B.</p> <p>“[A]t least one client node is provided with client manager software, which enables this node to function as the client manager node. The purpose of the client manager node is to provide the customer who uses the service to manage and administer each of the virtual storage devices of that customer. . . . [T]he client manager node is provided with full access privileges for all of the files and directories on each virtual storage device Furthermore, the client manager node is able to designate new user accounts and to provide sufficient information to enable a client user to join one or more of the virtual storage devices managed by the client manager node.” <i>Id.</i> at 12:21-39.</p> <p>“[A] manger node which chooses which users may join the group, transmits a message to an Internet email address of a user inviting the user to join the user group. Using the information in the message, a client node operated by the user issues a message to join the user group. The message is usable only once to join the user group.” <i>Id.</i> at 6:42-48.</p>
Claim 10	The Combination of the Phillips Patent and the Busam Application (Exs. 1005 and 1006)
10. The method of claim 9 wherein the digital computing device is one of at least two media player devices in the sharing group.	<p>Busam discloses that the sharing group consists of three media player devices.</p> <p>“The example described in FIG. 12 includes three devices that attempt to create a device-to-device network. For example purposes, the devices will be called device A, device B and device C (e.g., Joe’s home computer 10, Joe’s handheld device 12, Joe’s AV device 14).” Ex. 1006, [0048].</p>

D. Ground III: The Combination of the Abecassis and Ganesan Patents Renders Obvious Each of Claims 9 and 10 Under 35 U.S.C. § 103

The Abecassis patent discloses that devices in a network whose users correctly enter user identification and password information may access audio information, such as radio-on-demand. Ex. 1008, 19:38-20:16. One skilled in the art would understand such a set of network devices where users are granted access to share, for example, audio information, to be a “sharing group” as set forth in the ‘689 Patent. Almeroth Dec., ¶ 58. The Abecassis patent also discloses an access control system that determines whether a user of a multimedia player device may obtain access to multimedia content. For example, in one embodiment, handshaking routines request user identification, and, if required, a corresponding password. Ex. 1008, 19:49-59.

The Ganesan patent discloses that a first user, to assure a second user of the first user’s identity, sends the second user a certificate issued by a trusted intermediary that attests to the identity of the first user. Ex. 1009, 2:48-54. The Ganesan patent further discloses a trusted intermediary that is another user of the system, such as an authentication server. Ex. 1009, 8:29-39.

Successful authentication of a user by a content distribution system based on a third-party’s statement or certificate vouching for the identity of the user indicates that the user is authorized to access content on the content distribution system. This

distinguishes such a user from a user that is not successfully authenticated, and who, as a result, is not able to access content on the content distribution system. For that reason, a third-party's statement or certificate vouching for the identity of an authorized user is an expression of desirability of the user as an entity that can access content from the content distribution system, *i.e.*, it is an expression of the desirability of the user as a member of the sharing group.

Based on the above disclosures, a person of ordinary skill in the art would have reason to implement the Ganesan patent's method of authenticating the identity of a first user to a second user (by using information from a trusted intermediary) in the access control system of the Abecassis patent in order to, for example, implement access to the sharing group based on the authenticated identities of members of the sharing group instead of, or in addition to, password-based access control. Almeroth Dec., ¶ 66. Among other things, combining such features is at most the mere combination of known elements according to a known method to yield predictable results, or simple substitution of one known element for another to obtain predictable results. Almeroth Dec. ¶ 67.

Moreover, the combination of the Abecassis and Ganesan patents provides the teaching that applicants argued was missing from the prior art regarding the "wherein" clause present in claim 9 - "wherein the information associated with the user of the requesting media player device comprises information, made available

by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.” In particular, the Ganesan patent (which was not before the Examiner during prosecution of the ‘689 Patent) discloses that a user may authenticate itself to another user, for purposes of receiving information from and transmitting information to the other user, by sending the other user a certificate authenticating the first user that was produced by a trusted third party. Ex. 1009, 1:48 - 2:54. Thus, the concept of a trusted third party’s authenticating the identity of a user so that the user can access information (*i.e.*, an indication of the desirability of the user for purposes of accessing the information) was disclosed in a prior-art reference that was not available to the Examiner during prosecution of the ‘689 Patent.

Claim 9	The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)
A method of operating a digital computing device associated with a sharing group, comprising:	<p>Abecassis discloses a sharing group of digital computing devices.</p> <p>“FIG. 4 is a schematic diagram of an audio and information network comprising a plurality of providers 411-413, and a plurality of end users 431-438. Participants in the network 400, however, whether classified as providers 411-413 or end user 431-438 are both providers and end users of audio, video, and information services. Analogous to a communications network, each participant is able to retrieve and transmit audio and information from any other participant. A radio-on-demand system, in general, and the delivery of radio-on-demand services, in particular, are herein intended to be deployable by a variety of possible networks and Multimedia Player</p>

Claim 9	The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)
	<p>configurations. . . . A provider may utilize one or more Multimedia Players 431 in delivering radio-on-demand services.” Ex. 1008, 11:1-30; <i>see also</i> FIG. 4 and 7:16-22.</p> <p>“A method of playing radio-on-demand is principally detailed with respect to the flow chart of FIG. 7. . . . If user identification and password are found acceptable 713, other restrictions 715 to a user access are checked. . . . If user control is not enabled 711, or if enabled and verification of the user 713 and verification of other restrictions permit usage 715, the radio-on-demand initialization routines continue with, in this example, the scheduling preferencing routines 721.” <i>Id.</i> at 19:38-20:16.</p>
receiving a request to join the sharing group from a requesting media player device;	<p>Abecassis discloses that a request by a media player device is received to join the sharing group.</p> <p>“A method of playing radio-on-demand is principally detailed with respect to the flow chart of FIG. 7. Upon selection of the play function or turning on the apparatus, as in, for example, a dedicated apparatus, software, firmware, and/or hardware processing capabilities begin a radio-on-demand session 701 with the object of instantaneously playing an audio 702 in response to a reception of a start/play command 701. The selection of, for example, an audio unit 702 from the user's audio library can be arbitrary, random, or in response to a preestablished preference, procedure, or by utilizing a previously identified audio item.</p> <p>The playing of a first audio item 702 can serve as background audio to, or be an integral element of, for example, the user access control routines which begin by issuing a command to read the user control setup to ascertain if user control is enabled 711. If enabled, the handshaking routines request user identification and, if required, a corresponding password 712. If the user</p>

Claim 9	The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)
	<p>identification and password are not found acceptable 713, the appropriate error message is provided 714, and the apparatus is returned to a state prior to the user play request 701. A first audio item 702 can comprise an audio requesting voice identification 712.</p> <p>If user identification and password are found acceptable 713, other restrictions 715 to a user access are checked. These additional restrictions include, for example, time of day restrictions and/or accumulated usage during specified time frames. If restrictions are enabled that prevent usage 715, an appropriate error message 716 is provided, and the apparatus is returned to a state prior to the user play request 701.” Ex. 1008, 19:38-20:16.</p> <p>“Access routines previously detailed with respect to FIG. 7 steps 711-716 are summarized in FIG. 9 as steps 903-904. In an embodiment, although not necessarily, these routines reside within a Multimedia Player and are executed prior to, or after, establishing a communications linkage with either a network administrator or directly with a provider.” <i>Id.</i> at 26:66-27:4.</p>
making a determination as to whether to permit the requesting media player device to join the sharing group based on information associated with a user of the requesting media player device; and	<p>Ganesan discloses that a determination is made regarding permitting the player device to join based on information associated with its user.</p> <p>“The present invention relates generally to securing communications using cryptography. More particularly, the present invention provides a method and system for enhancing the security of communications using asymmetric crypto-keys and is especially useful in enhancing communication security in conventional Kerberos authentication systems.</p> <p>2. Description of the Related Art</p> <p>Cryptosystems have been developed for maintaining the privacy of information transmitted across a</p>

Claim 9	<p>The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)</p> <p>communications channel.” Ex. 1009, 1:9-19.</p> <p>“In a typical mode of operation, i sends j, $M^{(di)} \bmod N_i$ along with M and a certificate $C=(i, e_i N_i)^{(dCA)} \bmod N_{CA}$, where C is generated by a Certificate Authority (CA) which serves as a trusted off-line intermediary. User j can recover i's public key from C, by performing $C^{(eCA)} \bmod N_{CA}$, as e_{CA} and N_{CA} are universally known. It should also be noted that in an RSA system the encryption and signatures can be combined.” <i>Id.</i> at 2:48-55; <i>see also id.</i> at 1:58-2:20.</p> <p>Abecassis discloses access control routines for access to audio information.</p> <p>“Access routines previously detailed with respect to FIG. 7 steps 711-716 are summarized in FIG. 9 as steps 903-904. In an embodiment, although not necessarily, these routines reside within a Multimedia Player and are executed prior to, or after, establishing a communications linkage with either a network administrator or directly with a provider.” Ex. 1008, 26:66-27:4; <i>see also id.</i> at 26:57-61 and 27:11-24.</p>
adding the requesting media player device to the sharing group if the determination is made to permit the requesting media player device to join the sharing group;	<p>Abecassis discloses adding the player device to the sharing group if a determination is made to do so.</p> <p>“If access is permitted 903, retrieval routines are enabled 905 to permit the remote retrieval of audio and/or information.” Ex. 1008, 27:11-13; <i>see also id.</i> at 11:1-8, 20:11-15, Figs. 7, 9.</p>
wherein the information associated with the user of the requesting media player device comprises information, made	<p>Ganesan discloses that the information associated with the requesting player device is made available by a trusted user.</p> <p>“In a typical mode of operation, i sends j, $M^{(di)} \bmod N_i$ along with M and a certificate $C=(i, e_i N_i)^{(dCA)} \bmod N_{CA}$, where C is generated by a Certificate Authority (CA)</p>

Claim 9	The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)
<p>available by a trusted user, regarding a desirability of the user of the requesting media player device as a member of the sharing group.</p>	<p>which serves as a trusted off-line intermediary. User j can recover i's public key from C, by performing $C^{(e_{CA})} \bmod N_{CA}$, as e_{CA} and N_{CA} are universally known. It should also be noted that in an RSA system the encryption and signatures can be combined.” Ex. 1009, 2:48-55.</p> <p>“Another user, preferably an authentication server, applies the second private key portion and the public key portion of the first user crypto-key to the first encrypted message to decrypt the second temporary key portion and thereby authenticate the first user to the security server.” <i>Id.</i> at Abstract; <i>see also id.</i> at claim 4 and 8:29-33.</p> <p>Abecassis discloses access control routines for access to audio information.</p> <p>“Access routines previously detailed with respect to FIG. 7 steps 711-716 are summarized in FIG. 9 as steps 903-904. In an embodiment, although not necessarily, these routines reside within a Multimedia Player and are executed prior to, or after, establishing a communications linkage with either a network administrator or directly with a provider.” Ex. 1008, 26:66-27:4; <i>see also id.</i> at 26:57-61 and 27:11-24.</p>

Claim 10	The Combination of the Abecassis Patent and the Ganesan Patent (Exs. 1008 and 1009)
<p>10. The method of claim 9 wherein the digital computing device is one of at least two media player devices in the sharing group.</p>	<p>Abecassis discloses that there can be at least two media player devices in a sharing group.</p> <p>“FIG. 4 is a schematic diagram of an audio and information network comprising a plurality of providers 411-413, and a plurality of end users 431-438. Participants in the network 400, however, whether classified as providers 411-413 or end user 431-438 are both providers and end users of audio, video, and</p>

	information services. Analogous to a communications network, each participant is able to retrieve and transmit audio and information from any other participant.” Ex. 1008, 11:1-8; <i>see also id.</i> at 11:22-43, 13:23-47, 14:8-10, Fig. 4.
--	---

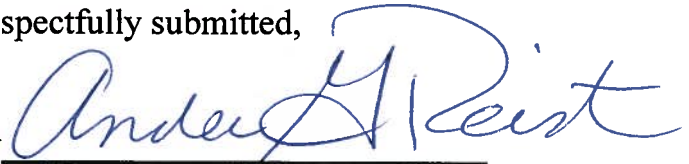
VI. CONCLUSION

Petitioner respectfully submits that, for the reasons set forth above, there is a reasonable likelihood that Petitioner will prevail on at least one claim. Accordingly, Petitioner respectfully requests that this Petition be granted and claims 9 and 10 of the ‘689 Patent be found to be unpatentable.

Date: May 1, 2014

Respectfully submitted,

By



Andrea G. Reister

Registration No.: 36,253

Gregory S. Discher

Registration No. 42,488

COVINGTON & BURLING LLP

1201 Pennsylvania Avenue, NW

Washington, DC 20004-2401

(202) 662-6000


Attorneys for Petitioner

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. §§ 42.6 and 42.105, I hereby certify that on this 1st day of May 2014, the foregoing Petition for *Inter Partes* Review of U.S. Patent No. 7,835,689 Under 35 U.S.C. §§ 311-319 and 37 C.F.R. § 42.100 *et seq.*, together with Petitioner's Exhibits Nos. 1001-1020, was served via overnight courier on the following counsel of record for patent owner:

Concert Technology Corporation
5400 Trinity Road, Suite 303
Raleigh NC 27607

Date: May 1, 2014


Andrea G. Reister, Esq.
Registration No.: 36, 253