IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of: Farber et al.	§	
	§	Petition for *Inter Partes* Review
U.S. Patent No. 6,928,442	§	
	§	Attorney Docket No.: 47015.137
Issued: Aug. 9, 2005	§	
	§	Customer No.: 116298
Title: ENFORCEMENT AND POLICING OF LICENSED CONTENT USING CONTENT-BASED IDENTIFIERS	§	
	§	Real Parties
	§	in Interest: Rackspace US, Inc. and
	§	Rackspace Hosting, Inc.
	§	

PETITION FOR INTER PARTES REVIEW

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Pursuant to the provisions of 35 U.S.C. §§ 311-319, Rackspace US, Inc. and Rackspace Hosting, Inc. ("Petitioners") hereby petition the Patent Trial and Appeal Board to institute *inter partes* review of claims 1, 2, 4, 7, 23, 27, 28, and 30 of U.S. Patent No. 6,928,442 to Faber *et al*. ("the '442 Patent," RACK-1001). PersonalWeb Technologies, LLC and Level 3 Communications, LLC have stated, in filings in the United States District Court for the Eastern District of the Texas that they each own an undivided fifty percent (50%) interest in the '442 Patent.

TABLE OF CONTENTS

I. Mandatory Notices by Petitioner (37 C.F.R. § 42.8(a)(1))

A. Real Parties-in-Interest (37 C.F.R. § 42.8(b)(1))

The real parties in interest are Rackspace US, Inc. and Rackspace Hosting, Inc.

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

The '442 Patent has been asserted in related judicial matter *PersonalWeb Tech. LLC et al v. Rackspace US, Inc. et al*., No. 6-12-cv-00659 (E.D. Tex., filed Sep. 17, 2012).

As of the filing date of this petition, to the best of petitioners' knowledge additional 3rd party judicial matters asserting claims of patent infringement under the '442 patent are: *PersonalWeb Techs. LLC et al v. EMC Corp. et al.*, No. 5-13 cv-01358 (N.D. Ca., filed Mar. 26, 2013); *PersonalWeb Techs. LLC et al v. Facebook Inc.*, No. 5-13-cv-01356 (N.D. Ca., filed Mar. 26, 2013); *PersonalWeb Techs. LLC et al v. NetApp, Inc.*, No. 5-13-cv-01359 (N.D. Ca., filed Mar. 26, 2013); *PersonalWeb Techs. LLC v. Google, Inc. et al*, No. 5-13-cv-01317 (N.D. Ca., filed Mar. 25, 2013); *PersonalWeb Techs. LLC et al v. Int'l Bus. Mach. Corp.*, No. 6-12-cv-00661 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC et al v. NetApp, Inc.*, No. 6-12-cv-00657 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC et al v. Facebook, Inc.*, No. 6-12-cv-00662 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC et al v. Apple Inc.*, No. 6-12-cv-

00660 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC et al v. Microsoft Corp.*, No. 6-12-cv-00663 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC et al v. Yahoo! Inc.*, No. 6-12-cv-00658 (E.D. Tex., filed Sep. 17, 2012); *PersonalWeb Techs. LLC v. Autonomy, Inc.*, No. 6-11-cv-00683 (E.D. Tex., filed Dec. 19, 2011); *PersonalWeb Techs. LLC v. Google, Inc. et al*, No. 6-11-cv-00656 (E.D. Tex., filed Dec. 8, 2011); *PersonalWeb Techs. LLC v. NEC Corp. of America, Inc.*, No. 6-11-cv-00655 (E.D. Tex., filed Dec. 8, 2011); *PersonalWeb Techs. LLC v. NetApp, Inc.*, No. 6-11-cv-00657 (E.D. Tex., filed Dec. 8, 2011); *PersonalWeb Techs. LLC v. Caringo, Inc.*, No. 6-11-cv-00659 (E.D. Tex., filed Dec. 8, 2011); *PersonalWeb Techs. LLC v. Amazon Web Svcs. LLC et al*, No. 6-11-cv-00658 (E.D. Tex., filed Dec. 8, 2011); *PersonalWeb Techs. LLC v. EMC Corp. et al*, No. 6-11-cv-00660 (E.D. Tex., filed Dec. 8, 2011); and *Akamai Techs, Inc. v. Digital Island, Inc.*, No. 1-00-cv-11851 (D. Mass., filed Sep. 13, 2000).

In addition, the following instituted trials and/or 3rd party petitions for *inter partes* review are related:

- IPR2013-00082 (instituted for related patent 5,978,791, May 17, 2013)
- IPR2013-00083 (instituted for related patent 6,415,280, May 17, 2013)
- IPR2013-00084 (instituted for related patent 7,945,544, May 17, 2013)
- IPR2013-00085 (instituted for related patent 7,945,539, May 17, 2013)

- IPR2013-00086 (instituted for related patent 7,949,662, May 17, 2013)
- IPR2013-00087 (instituted for related patent 8,001,096, May 17, 2013)
- IPR2013-00319 (petition for related patent 5,978,791, May 30, 2013)
- IPR2013-00596 (petition for related patent 7,802,310, Sept. 18, 2013)

Finally, Petitioners themselves are also seeking *inter partes* review of related U.S. Patents 5,978,791, 6,415,280, 7,802,310, and 8,099,420, and request that, if possible, they be assigned to the same panel for administrative efficiency.

C. Identification of Lead and Back-Up Counsel (37 C.F.R. § 42.8(b)(3)) and Service Information (37 C.F.R. § 42.8(b)(4))

Lead Counsel J. Andrew Lowes HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: (972) 680-7557 Fax: (214) 200-0853 andrew.lowes.ipr@haynesboone.com USPTO Reg. No. 40,706
Back-up Counsel David W. O'Brien HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: (512) 867-8457 Fax: (214) 200-0853 david.obrien.ipr@haynesboone.com USPTO Reg. No. 40,107
John Russell Emerson HAYNES AND BOONE, LLP 2323 Victory Ave., Suite 700 Dallas, TX 75219	Phone: (972) 739-6923 Fax: (214) 200-0853 russell.emerson.ipr@haynesboone.com USPTO Reg. No. 44,098

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

Petitioners certify pursuant to 37 C.F.R. § 42.104(a) that the '442 Patent is available for *inter partes* review and that Petitioners are not barred or estopped from requesting *inter partes* review challenging the patent claims on the grounds identified herein.

III. Statement of Precise Relief Requested (37 C.F.R. § 42.22(a))

Petitioners ask that the Board review the accompanying prior art and analysis, institute a trial for *inter partes* review of claims 1, 2, 4, 7, 23, 27, 28, and 30 of the '442 Patent, and cancel those claims as unpatentable.

IV. Overview of Challenges

A. Identification of Challenges (37 C.F.R. § 42.104(b))

The prior art references relied upon are as follows:

- U.S. Patent No. 5,649,196 to Woodhill, et al. (hereinafter "Woodhill") issued on July 15, 1997 as a continuation of 08/085,596 filed July 1, 1993. (RACK-1004.) Woodhill is prior art to the '442 Patent under 35 U.S.C. § 102(e).
- U.S. Patent No. 4,845,715 to Francisco (hereinafter "Francisco") issued on July 4, 1989. (RACK-1005.) Francisco is prior art to the '442 Patent under 35 U.S.C. §102(b).

- U.S. Patent No. 6,135,646 to Kahn et al. (hereinafter "Kahn") issued on October 24, 2000 as a continuation of 08/808,050 filed Oct. 22, 1993. (RACK-1006.) Kahn is prior art to the '442 Patent under 35 U.S.C. § 102(e).
- Albert Langer, "Re: dl/describe (File descriptions)," post to the "alt.sources" newsgroup on August 7, 1991, (hereinafter "Langer"). (RACK-1007.) As explained by Dr. Reddy, Langer was available as a printed publication more than one year before the priority date of the '442 Patent. (Reddy Decl., RACK-1011.) Therefore, Langer is prior art to the '442 Patent under 35 U.S.C. § 102(b).

For each challenge the table below identifies: (i) the specific statutory grounds of unpatentability and the prior art patents or printed publications relied upon, and (ii) the applicable claim(s).

Challenge	Grounds and Reference(s)	Challenged claim(s)
1	§ 103(a), Woodhill in view of Francisco	1, 2, 4, 23, 27 and 30
2	§ 103(a), Woodhill in view of Kahn	7
3	§ 103(a), Woodhill in view of Francisco and Langer	28

Challenged claims are to be construed as indicated in Section V below. For each challenge, the unpatentability of the applicable claims is established with reference to particular claim elements and with reference to specific disclosure found in the

relied upon prior art. Supporting evidence is referenced by exhibit number and with particular reference to specific portions of the evidence that support the challenges. In particular, a Declaration of Dr. Melvin Ray Mercer, Professor Emeritus of Electrical and Computer Engineering at Texas A&M University (Mercer Decl., RACK-1010.) is included to establish a record for factual positions and matters of opinion testimony relied upon herein. In addition, a Declaration of Dr. Narasimha Reddy, Professor of Electrical and Computer Engineering at Texas A&M University is included to establish facts related to the Langer publication (Reddy Decl., RACK-1011.). Petitioners' Exhibit List is appended hereto.

B. Summary of Central Argument that Challenged Claims are Unpatentable

The '442 Patent relates generally to methods of distributing files across a data processing network and providing copies of the files based, at least in part, on unique identifiers based on the contents of a data file. The '442 Patent uses these identifiers in an access control method to prevent unauthorized access to files. The '442 Patent contends that "all of the prior data processing systems" used names or identifiers that were "always defined relative to a specific context," such as the file or directory containing the file. (RACK-1001, 1:66-2:12.) As explained below, this characterization of the prior art is inaccurate.

The Woodhill, Francisco, and Langer references all disclose data processing systems that utilize file identifiers that are based, at least in part, on a function of

the contents of the file. Both Woodhill and Langer use the content based identifiers to obtain copies of the files from other servers on a network. Francisco discloses an additional feature in that it uses content based identifiers to verify that files are authentic and provided only to authorized users. The Kahn reference discloses a digital image rights management method that distributes files on a network of computers and prevents copies from being distributed to unauthorized users. The Langer reference is provided to show that the MD5 hash was a well-known hash function used to generate a unique identifier for a data file at the time the '442 Patent was filed. The application of each of these references to the specific elements of the challenged claims of the '442 Patent is set forth in detail below.

C. Threshold Showing of Reasonable Likelihood That Petitioner Would Prevail With Respect To At Least One Challenged Claim (35 U.S.C. § 314(a)) Has Been Met; Institution of *Inter Partes* Review on Multiple Grounds is Proper (37 C.F.R. § 42.108)

Information presented in this Petition, including unpatentability grounds detailed in Section VI, below, establishes a reasonable likelihood that Petitioner will prevail with respect to at least one of the challenged claims. *See* 35 U.S.C. § 314(a). Indeed, Section VI, supported by the Mercer Declaration (Mercer Decl., RACK-1010) demonstrates multiple grounds on which the challenged claims are obvious in view of the relied upon prior art patents and printed publication.

V. The Challenged '442 Patent

A. Overview of the Patent

The '442 Patent is directed to data storage systems that use names to identify data files, where the names are based, at least in part, on the contents of the data in a data file. (RACK-1001, Title, Abstract, 1:14-19.) The '442 Patent uses these names in an access control method to only provide copies of a requested file to an authorized or licensed user. (RACK-1001, 11:66-12:10.) The content dependent names are also used in a method to determine if an unauthorized copy of a data file is present on a computer. (RACK-1001, 32:42-33:7.)

According to the '442 Patent, prior art systems identified data items based on their location or address within the data processing system. (RACK-1001, 1:24-31.) For example, files were often identified by their context or "pathname," i.e., information specifying a path through the computer directories to the particular file (e.g., C:\MyDocuments\classes\EE350\lecture1.ppt). (*See* RACK-1001, 1:36-43.) The '442 Patent contends that all prior art systems operated in this manner, stating that "[i]n all of the prior data processing systems[,] the names or identifiers provided to identify data items … are always defined relative to a specific context," and "there is no direct relationship between the data names and the data item." (RACK-1001, 1:66–2:4, 2:13-14.)

According to the '442 Patent, this prior art practice of identifying a data item by its context or pathname had certain shortcomings. For example, with pathname identification, the same data name may refer to different data items, or conversely, two different data names may refer to the same data item. (RACK-1001, 2:13-17.) Moreover, because there is no correlation between the contents of a data item and its pathname, there is no a priori way to confirm that the data item is in fact the one named by the pathname. (RACK-1001, 2:18- 21.) Furthermore, context or pathname identification may more easily result in the creation of unwanted duplicate data items, e.g., multiple copies of a file on a file server. (RACK-1001, 2:48-59.)

The '442 Patent purports to address these shortcomings. It suggests that "it is therefore desirable to have a mechanism … to determine a common and substantially unique identifier for a data item, using only the data in the data item and not relying on any sort of context." (RACK-1001, 3:7-12.) Moreover, "[i]t is further desirable to have a mechanism for reducing multiple copies of data items … and to have a mechanism which enables the identification of identical data items so as to reduce multiple copies." (RACK-1001, 3:13-16.)

To do so, the '442 Patent provides substantially unique identifiers that "depend[] on all of the data in the data item …." (RACK-1001, 1:14-19; *see also* 3:30-33.) The '442 Patent uses the terms "True Name" and "data identifier" to

refer to the substantially unique identifier for a particular data item (RACK-1001, 6:7-11.) and explains that a True Name is computed using a message digest function. (RACK-1001, 12:58-13:17.) Preferred embodiments use either of the MD5 or SHA message digest functions to calculate a substantially unique identifier from the contents of the data item. (RACK-1001, 13:18-13:22.)

The '442 patent calls these context- or location-independent, content-based identifiers "True Names"–a phrase apparently coined by the inventors. With these identifiers, the patent asserts, "data items can be accessed by reference to their identities (True Names) independent of their present location." (RACK-1001, 34:35-37.) The actual data item corresponding to these location-independent identifiers may reside anywhere, e.g., locally, remotely, offline. (RACK-1001, 34:37-39.) "[T]he identity of a data item is independent of its name, origin, location, address, or other information not derivable directly from the data, and depends only on the data itself." (RACK-1001, 3:34-36.)

In the preferred embodiments, the substantially unique identifiers are used to "augment" standard file management functions of an existing operating system. (*See* RACK-1001, 6:12-20.) For example, a local directory extensions (LDE)

table[1] is indexed by a pathname or contextual name of a file and also includes True Names for most files. (RACK-1001, 8:21-28.) A True File registry (TFR) lists True Names, and stores "location, dependency, and migration information about True Files." (RACK-1001, 8:29-36.) True Files are identified in the True File registry by their True Names, and can be looked up in the registry by their True Names. (RACK-1001, 8:29-36, 24:1–4.) This look-up provides, for each True Name, a list of the locations, such as file servers, where the corresponding file is stored. (*See*, RACK-1001, 34:35–55; *see also* 16:14–17.)

When a data item is to be "assimilated" into the data processing system, its substantially unique identifier (True Name) is calculated and compared to the True File Registry to see if the True Name already exists in the Registry. (RACK-1001, 14:45-64.) If the True Name already exists, this means that the data item already exists in the system and the to-be-assimilated data item (i.e., the scratch file) need not be stored. (RACK-1001, 14:55-64.) Conversely, if the True Name does not exist in the Registry, then a new entry is created in the Registry which is then set to the just-calculated True Name value, and the data items can be stored. (RACK-1001, 14:65-15:4.)

[1] The patent describes an LDE table as a data structure which provides information about files and directories in the system and includes information in addition to that provided by the native file system. (*See* RACK-1001, 8:21-28.)

The ‘442 Patent describes a “mechanism that ensures that licensed files are not used by unauthorized parties.” (RACK-1001, 32:43-44.) The disclosed technique includes recording a file identifier in a license table along with the identity of each user or system which is authorized/licensed to have a copy of the file. (RACK-1001, 8:53-56, 11:66-12:10, and 32:56-64.) The license table information is used to compare the contents of a user’s system with the license table data. (RACK 1001, 32:65-33:7.) The system can also deny access to the file without proper authorization. (RACK-1001, 32:48-51.)

Dr. Mercer confirms the foregoing overview of the challenged ‘442 patent. (*See* Mercer Decl., RACK-1010, ¶¶24-32.)

B. Prosecution History

During the original prosecution of the application leading to the ‘442 Patent, the Examiner requested that the applicants identify support in the specification for the licensing aspects of the claims. The applicants directed the Examiner to the pages of the specification having a description of the “Track for Licensing Purposes” and a description of the license table. (‘442 Patent File History, RACK-1002, pp. 129-130, referring to specification pages found at pp. 371-372, 324, 329, and 330). Portions of the specification relating to the license table are reproduced below.

Each record 150 of the license table 136 records a relationship between a licensable data item and the user licensed to have access to it. Each license table record 150 includes the information summarized in the following table, with reference to FIGURE 9:

Field	Description
True Name	True Name of a data item subject to license validation.

Field	Description
licensee	identity of a user authorized to have access to this object.

(RACK-1002, pp. 329-330.)

After the claims were amended to include limitations relating to "licensed or authorized" users and copies, a Notice of Allowance was issued. (RACK-1002, pp. 76-84.)

During a subsequent reexamination proceeding, the patent Examiner rejected all of the claims based on U.S. Patent No. 4,658,093 to Hellman ("Hellman"). In seeking to maintain the claims, the patent owner distinguished claim 1 by suggesting that Hellman failed to disclose providing the content based name in a request and causing a copy of the file to be provided to the requester. (RACK-1003, pp. 230-231.) With respect to claim 23, the patent owner suggested that Hellman failed to provide a list of file names to determine whether

unauthorized or unlicensed copies of some of the plurality of data files are present on a particular computer. (RACK-1003, pp. 236-238.)

Although some claims were canceled, the patentability of the challenged claims was confirmed over the Hellman reference.

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

This petition presents claim analysis in a manner that is consistent with the broadest reasonable interpretation in light of the specification. *See* 37 C.F.R. § 42.100(b). Claim terms are given their ordinary and accustomed meaning as would be understood by one of ordinary skill in the art, unless the inventor, as a lexicographer, has set forth a special meaning for a term. *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1477 (Fed. Cir. 1998); *York Prods., Inc. v. Central Tractor Farm & Family Ctr.*, 99 F.3d 1568, 1572 (Fed. Cir. 1996).

"data file"

The term "data file" appears in all of the challenged claims. The term "data file" has been previously construed by the PTAB with respect to a parent patent of the '442 Patent, U.S. Patent No. 6,415,280, in IPR2013-00083. In IPR2013-00083, the PTAB construed the claim term "data file" to mean "a named data item, such as a simple file that includes a single, fixed sequence of data bytes or a compound file that includes multiple, fixed sequences of data bytes." (*see* Decision

to Institute *Inter Partes* Review, IPR-2013-00083 (RACK-1009)). Thus, Petitioners suggest that the Board adopt the same claim construction of "data file" for the '442 Patent.

"wherein some of the computers communicate with each other using a TCP/IP communication protocol."

The preamble of claim 7 includes the phrase "wherein some of the computers communicate with each other using a TCP/IP communication protocol." In general, a preamble is construed as a limitation "if it recites essential structure or steps, or if it is 'necessary to give life, meaning, and vitality' to the claim." *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*, 289 F.3d 801, 808 (Fed. Cir. 2002) (quoting *Pitney Bowes, Inv. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)). In this case, the body of claim 7 makes no reference to how the plurality of computers communicate with each other and do not specify any features unique to using a TCP/IP communication protocol. (Mercer Decl., RACK-1010, ¶ 46.) Thus, the feature set forth in the preamble of claim 7 does not add essential structure or steps to the claim and these terms are not necessary to give life, meaning, or vitality to the claim. (*Id.*) Therefore, Petitioners' assert that this portion of the preamble should not be entitled to patentable weight when considering the limitations of claim 7.

For avoidance of doubt, the foregoing proposed claim construction is presented by Petitioner in accordance with the broadest reasonable interpretation standard applied for purposes of *inter partes* review. Petitioner reserves the right to advocate a different claim interpretation in district court or any other forum in accordance with the claim construction standards applied in such forum.

VI. Unpatentability under Specific Grounds (37 C.F.R. 42.104(b)(4) and Evidence Relied Upon in Support of Challenge (37 C.F.R. 42.104(b)(5))

A. Challenge #1: Claims 1, 2, 4, 23, 27 and 30 are obvious under 35 U.S.C. § 103 based on Woodhill in view of Francisco

Claims 1, 2, 4, 23, 27 and 30 are obvious under 35 U.S.C. § 103 based on Woodhill in view of Francisco. Woodhill discloses use of context- and location-independent identifiers for purposes that are analogous to those disclosed in the '442 Patent. (RACK-1004; *see also* Mercer Decl., RACK-1010, ¶¶ 49-53.) As Woodhill explains, a "Binary Object Identifier 74 [of Fig. 3] … is a unique identifier for each binary object to be backed up." (RACK-1004, 4:45-47.) Woodhill's Binary Object Identifiers include three fields–a CRC value, a LRC value, and a hash value–each calculated from the contents of the binary object. (RACK-1004, 8:1-33.) As Woodhill emphasized, "[t]he critical feature to be recognized in creating a Binary Object Identifier 74 is that the identifier should be based on the contents of the binary object so that the Binary Object Identifier 74 changes when the contents of the binary object changes." (RACK-1004, 8:58-62.)

Woodhill uses these identifiers to identify binary objects that have changed since the most recent backup, so that "only those binary objects associated with the file that have changed must be backed up." (RACK-1004, 9:6-9.) "[D]uplicate binary objects, even if resident on different types of computers in a heterogeneous network, can be recognized from their identical Binary Object Identifiers 74." (RACK-1004, 8:62-65.)

Woodhill discloses that the method of distributed management of storage space and data using content based identifiers is implemented on a networked computer system having a plurality of local computers, work stations, local area networks, a wide area network, and at least one remote backup file server. (Mercer Decl., RACK-1010, ¶51.) "[T]he Distributed Storage Manager program 24 stores a compressed copy of every binary object it would need to restore every disk drive 19 on every local computer 20 somewhere on the local area network 16 other than on the local computer 20 on which it normally resides. At the same time, the Distributed Storage Manager program 24 transmits every new or changed binary object to the remote backup file server 12." (RACK-1004, 9:30-38.)

The local computers can act as clients when making requests for files and can act as servers when responding to requests for providing files served on their local storage devices. (Mercer Decl., RACK-1010, ¶¶51-53). Woodhill recognizes that "[s]ince most restores of files on a local area network 16 consist of requests to

restore the most recent backup version of a file, the local copies of binary objects serve to handle very fast restores for most restore requests that occur on the local area network 16. If the local backup copy of a file does not exist or a prior version of a file is required, it must be restored from the remote backup file server 12." (RACK-1004, 10:27-34.)

In order to better explain the description set forth in Woodhill, Dr. Mercer modified and annotated Fig. 1 of Woodhill to represent the description that "[e]ach local area network 16 includes multiple user workstations 18 and local computers 20 each in communication with their respective local area network 16 via data paths 17." (RACK-1004, 3:24-26, and Mercer Decl., RACK-1010, ¶ 53.) The modified portions of the figure set forth below are noted by the dashed box surrounding the feature.

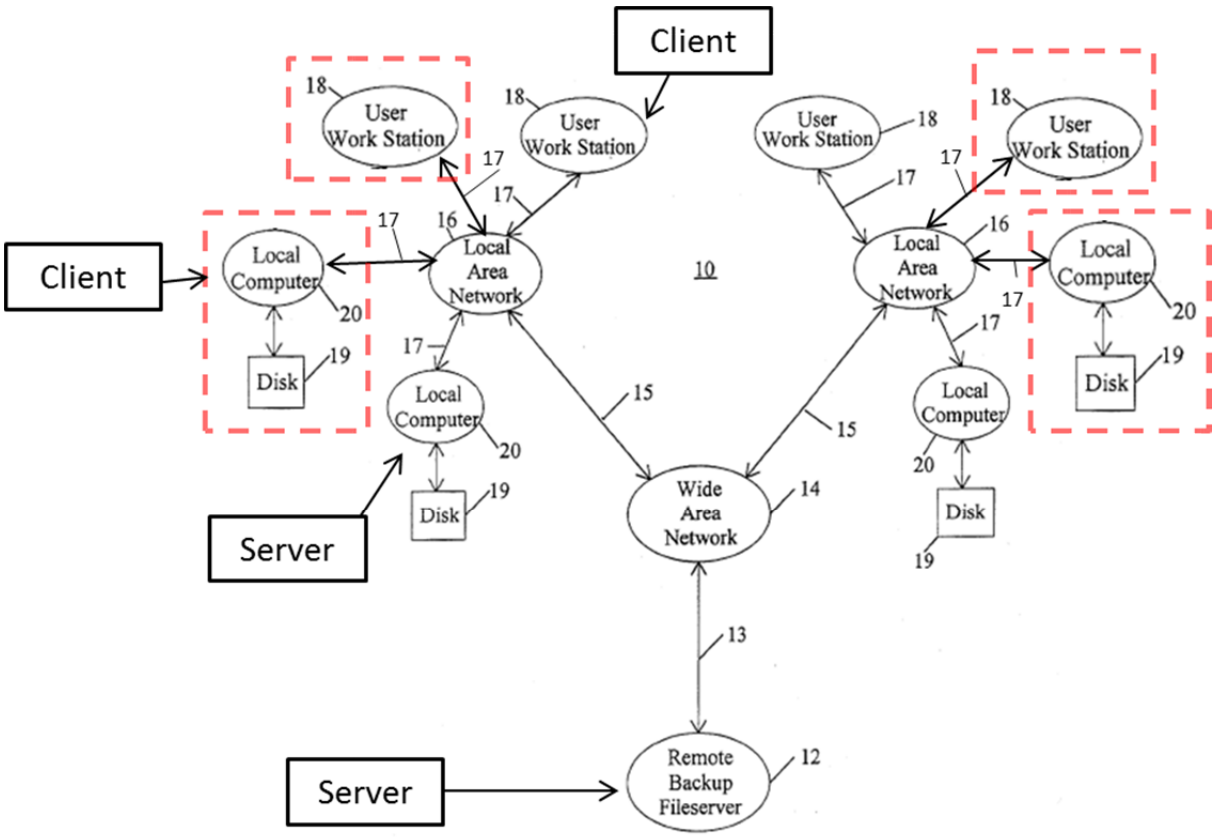

FIG. 1
Annotated

U.S. Patent No. 4,845,715 to Francisco issued on July 4, 1989 and is therefore prior art to the '442 Patent under 35 U.S.C. §102(b). (RACK-1005.) Francisco discloses "an improved method for maintaining the integrity of a data processing system through controlled authentication and subsequent authorization of both selected programs and potential users thereof. In its broader aspects, the invention includes the generation and storage of a selective electronic identification indicia, based upon the nature and content of the program itself, for each software program in the system together with a separately stored correlation of such

electronic identification indicia with user identity therewith in association with a regeneration of such electronic identification indicia each time the program is sought to be used and a checking of said regenerated electronic identification indicia against a stored catalog of such identification indicia and against a stored permitted user register therefore." (RACK-1005, 1:38-53 (emphasis added).)

Francisco further describes that "[a]mong the advantages of the subject invention is a markedly improved system security to ensure only utilization of authenticated programs, the utilization of such programs only by authorized users thereof and the immediate detection of any modifications or changes introduced into a software program." (RACK-1005, 1:54-59 (emphasis added).)

Woodhill and Francisco both disclose methods of managing data storage systems utilizing content based unique identifiers. Both references disclose using a function of the contents of the data file to determine a unique identifier. Woodhill discloses that file information can include access control data and therefore suggests that access control to the data files is already a part of the system set forth in the Woodhill patent. (Mercer Decl., RACK-1010, ¶61.) Although Woodhill does not expressly disclose how to use access control data to limit the provision of files to unauthorized/unlicensed parties, it was well known at the time to maintain a listing of authorized users and compare the requesting parties credentials against a listing of authorized users. (*Id*.) As an example, Francisco discloses "a method for

maintaining integrity through selectively coded preauthorized software program and user identification and subsequent automatic authentication of both a selected program and permitted user thereof when system resources are to be utilized." (RACK-1005, 1:10-15.)

It would have been obvious to combine Woodhill's suggested access control data with the user authentication techniques taught by Francisco to only provide copies of the requested file to an authorized party identified in a table and not provide copies of files to unauthorized parties. (Mercer Decl., RACK-1010, ¶62.)

Claim 1

[1a] ***In a system in which a plurality of files are distributed across a plurality of computers, a method comprising:***

Woodhill is titled "System and Method for Distributed Storage Management on Networked Computer Systems Using Binary Object Identifiers" and discloses a method of distributing files across a network of servers. (Mercer Decl., RACK-1010, p. 30.) Woodhill discloses a networked computer system including a remote backup file server and one or more local computers with data storage devices (clients and servers) connected to one or more local area networks. (*Id*.) A copy of Fig. 1 of Woodhill, modified to illustrate the additional computers described in the specification, is set forth above. Just like the disclosure in the '442 Patent, Woodhill discloses using content based data identifiers to name sequences of bytes, called "binary objects". (Mercer Decl., RACK-1010, p. 31.)

As explained in Woodhill, "The Distributed Storage Manager stores a compressed copy of every binary object it would need to restore every disk drive 19 on every local computer 20 somewhere on the local area network 15 other than on the local computer 20 on which it normally resides. At the same time, the Distributed Storage Manager program 24 transmits every new or changed binary object to the remote backup file server 12." (RACK-1004, 9:31-38). Thus, with reference to modified Fig. 1 above, Woodhill discloses distributing a set of data files across a network of computers. (Mercer Decl., RACK-1010, ¶¶51-53.)

[1b] ***obtaining a name for a data file, the name being based at least in part on a given function of the data, wherein the data used by the given function to determine the name comprises the contents of the data file***

The term "data file" has been previously construed by the PTAB as "a named data item, such as a simple file that includes a single, fixed sequence of data bytes or a compound file that includes multiple, fixed sequences of data bytes." (RACK-1009, pp. 10-11.) Just like the disclosure in the '442 Patent, Woodhill discloses using content based data identifiers to identify (name) sequences of bytes, called "binary objects." (Mercer Decl., RACK-1010, p. 31) In one example in Woodhill, if a file is less than 1 megabyte, then a single binary object represents a single file. (*Id.*)

As part of its creation of the Binary Object Identifier 74 of a Binary Object Identifier Record, Woodhill computes a hash against the contents of the binary

object to be identified. (RACK-1004, 7:60-8:32.) Specifically, relative to Binary Object Hash field 70 of Binary Object Identifier 74:

> **The Binary Object Hash field 70 is calculated against the contents of the binary object taken one (1) word (16 bits) at a time using the following algorithm:**
>
> ```
> HASH = (initialized value)
> for each word (16 bits) of the binary object:
>    rotate current HASH value by 5 bits
>    HASH = HASH + 1
>    HASH = HASH + (current word (16 bits) of binary object)
> end loop
> ```

(RACK-1004, 8:16-32.) Binary Object Identifier 74 is used to uniquely identify a particular binary object. (RACK-1004, 8:33-34.) Furthermore, duplicate binary objects, even if resident on different types of computers, can be recognized based on their identical Binary Object Identifiers 74. (RACK-1004, 8:62-65.) As shown in FIGS. 2 and 3 reproduced from Woodhill, each memory includes a file database 25 that includes a data file name comprising a Binary Object Identifier 74 based on the contents of the file. (RACK-1004, FIGS. 2 and 3, 7:60-8:65.)

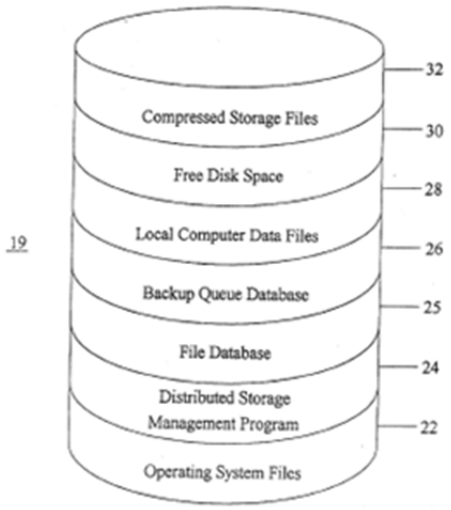

FIG. 2

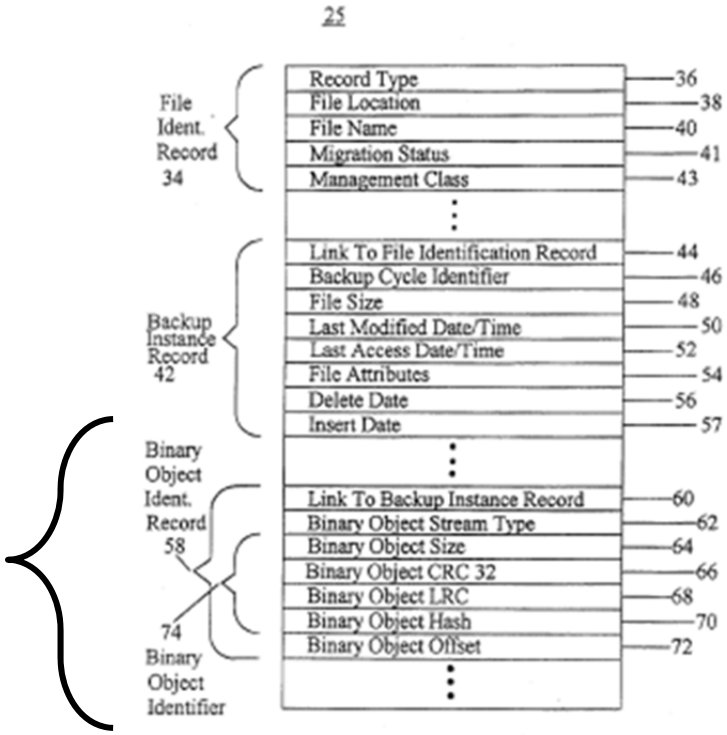

FIG. 3

Binary Object Identification Record 58 is created in File Database 25 of Woodhill

Dr. Mercer confirms that Binary Object Identifier 74 and, indeed Binary Object Hash field 70, Binary Object LRC field 68, and Binary Object CRC32 field 66, are all determined using and depending on the data in the data item. (Mercer Decl., RACK-1010, ¶50.) Dr. Mercer further confirms that, based on Woodhill's description of its binary object identifier fields and computations, two identical data items will have the same identifier. (*Id.*)

[1c] ***and in response to a request for the a data file, the request including at least the name of the particular file, causing a copy of the file to be provided from a given one of the plurality of computers,***

Woodhill discloses, responsive to a client request for the data file, the request including a hash of the contents of the data file, causing the data file to be provided to the client. (Mercer Decl., RACK-1010, p. 32.) For example, the data processing system of Woodhill allows restores (client request) of binary objects (data files) using their Binary Object Identifiers during the Backup/Restore Routine. (*Id.*) As set forth as an example in Woodhill, "the Distributed Storage Manager program 448 transmits an "update request" to the remote backup file server 12 which includes the Binary Object Identification Record 58 for the previous version of each binary object as well as the list of "contents identifiers" calculated in step 444…. If the Distributed Storage Manager program 24 determines, in step 452, that the "contents identifiers" do not match, program control continues with step 454 where the Distributed Storage Manager program 24 transmits the "granule" to the local computer 20. " (RACK-1004, 17:18-18:11 (emphasis added)).

As another example, the data processing system of Woodhill performs periodic self-audits by initiating a restore of a randomly selected binary object, identified by its Binary Object Identification Record, which includes its Binary Object Identifier. (Mercer Decl., RACK-1010, p. 32.) The program initiates a

restore by requesting a binary object identified by a Binary Object Identification Record 58 stored in File Database 25. (*See* FIGS. 2 and 3 reproduced above.) (RACK-1004, 18:16-19.) As shown in FIG. 3 of Woodhill, Binary Object Identifier includes a hash value, calculated by a hash function of the contents of the binary object that it identifies, that is sent as part of the request to restore the binary object. (Mercer Decl., RACK-1010, pp. 32-33.) "[T]he selected binary object is restored from either a compressed storage file 32 residing on one of the disk drives 19 of one of the local computers 20 or from the remote backup file server." (RACK-1004, 8:20-23.) Thus, Woodhill discloses, responsive to a client request for the data file including a name, causing the file to be provided to the client.

[1d] ***wherein a copy of the requested file is only provided to licensed parties.***

Woodhill discloses that access control data may be included with the content of data files. (RACK-1004, 7:40 and Mercer Decl., RACK-1010, p. 35.) Access control data is understood by those skilled in the art to provide information concerning which users are entitled to access the particular data file. (Mercer Decl., RACK-1010, p. 35.) Thus, Woodhill suggests that access control to the data files is already a part of the system set forth in the patent. (*Id.*) Although Woodhill does not expressly disclose how to use access control data to limit the provision of files to unauthorized/unlicensed parties, it was well known at the time

to maintain a listing of authorized users and compare the requesting party's credentials against a listing of authorized users. (*Id.*) As an example, U.S. Patent 4,845,714 to Francisco, discloses "a method for maintaining integrity through selectively coded preauthorized software program and user identification and subsequent automatic authentication of both a selected program and permitted user thereof when system resources are to be utilized." (RACK-1005, 1:10-15 (emphasis added).) Francisco discloses using a library of all authorized profiles correlating authorized user identifications with all programs that each user is entitled to use. (RACK-1005, 2:56-64 and Mercer Decl., RACK-1010, pp. 35-36.) FIG. 1 of Francisco is reproduced below.

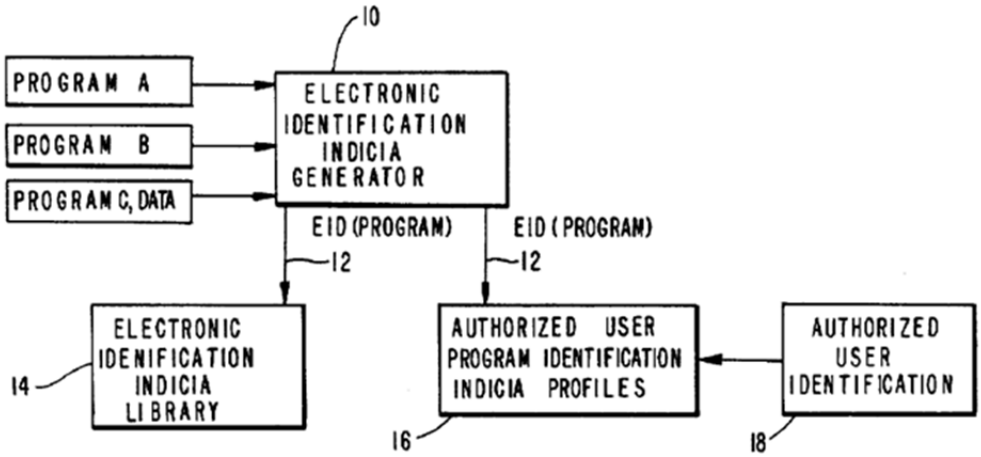

FIG. 1

As illustrated in FIG. 2 reproduced and annotated below, Francisco discloses first checking to see if the requested program is the "true program" requested, if so, then a second comparison is made to the user profile to determine if the user is

authorized to receive the program. (Mercer Decl., RACK-1010, pp. 37-38.) As shown graphically in the annotated copy of Francisco FIG. 2, reproduced below, if the user's profile does not match any authorized user profiles, then the file will not be released to the user. (Mercer Decl., RACK-1010, ¶ 57.)

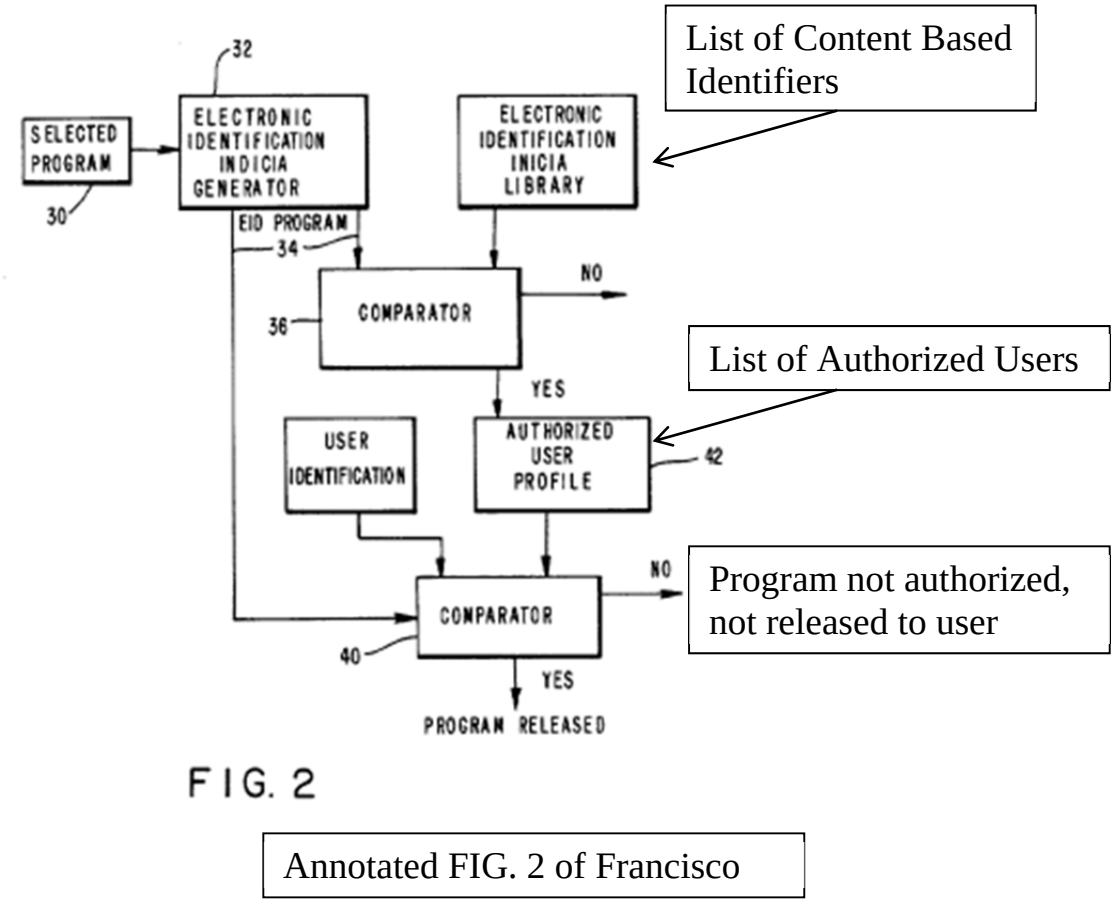

FIG. 2

Annotated FIG. 2 of Francisco

It would have been obvious to combine Woodhill's access control data with the user authentication techniques taught by Francisco to only provide copies of the requested file to an authorized party identified in a table as set forth in Francisco and not provide copies of files to unauthorized parties as set forth in Francisco. (Mercer Decl., RACK-1010, pp. 35-38.)

Claim 2

[2] ***A method as in claim 1 further comprising: determining, using at least the name, whether a copy of the data file is present on a particular one of said computers.***

Woodhill discloses a first computer using at least the file name (Binary Object Identification) to determine if the same binary object is present on a second computer. (Mercer Decl., RACK-1010, p. 38.) Woodhill discloses determining, based on content identifiers, whether a data file on a local computer matches a data file on a remote backup file server. (RACK-1004, 17:36-46 and Mercer Decl., RACK-1010, p. 38.) Thus, Woodhill discloses the additional limitation of claim 2.

Claim 4

[4] ***A method as in claim 1, further comprising: maintaining accounting information relating to the data files.***

The '442 Patent describes examples of accounting information relating to the data files to be the type of information associated with uses of the files, as well as the times when files are created, deleted, or copied. (RACK-1001, 31:57-32:24.)

Woodhill expressly discloses tracking this same information. (Mercer Decl., RACK-1010, p. 40.) For example, Woodhill discloses maintaining for each file, the date the file was last backed up, the last access date, the delete date and

creation date. (RACK-1004, 3:64-4:11 and Mercer Decl., RACK-1010, p. 40.) Thus, Woodhill discloses all of the features of claim 4.

Claim 23

[23a] ***A method comprising: obtaining a list of file names, at least one file name for each of a plurality of files, each of said file names having been determined, at least in part, by applying a function to the contents of the corresponding file***

As explained above in [1b], Woodhill discloses a system for determining unique identifiers based on the content of the file and then maintaining listings of those identifiers across a networked computer system. (RACK-1004, 3:7-5:11 and Mercer Decl., RACK-1010, pp. 40-42.) Francisco also discloses obtaining a list of file names by first determining a unique identifier for each file based on a function of the contents of the file and then storing a listing of the identifiers in a library. (Mercer Decl., RACK-1010, pp. 42-43.)

[23b] ***and using at least said list to determine whether unauthorized or unlicensed copies of some of the plurality of data files are present on a particular computer.***

As set forth above in [1b], Woodhill discloses determining file names, at least in part, based on the contents of the file. Woodhill also discloses maintaining a list of the file names, at least in part determined by a function of the contents of the file. (Mercer Decl., RACK-1010, pp. 40-42.) Woodhill suggests that access control can be a part of the system, but does not expressly disclose a technique for

accomplishing access control. (*See* Rack-1004, 7:40 and Mercer Decl., RACK-1010, p. 43.) Although Woodhill does not expressly disclose how to use access control data to limit the provision of files to unauthorized/unlicensed parties or to prevent unauthorized files from being used on the system, it was well known at the time to maintain a listing of authorized users and compare the requesting party's credentials against a listing of authorized users before providing a copy of the requested file. (Mercer Decl., RACK-1010, pp. 43-44.) As an example, Francisco discloses "a method for maintaining integrity through selectively coded preauthorized software program and user identification and subsequent automatic authentication of both a selected program and permitted user thereof when system resources are to be utilized." (RACK-1005, 1:10-15.)

Francisco discloses that a copy of a program residing on a computer being requested can be determined to be unauthorized if there have been any modifications or changes in the software program. (Mercer Decl., RACK-1010, pp.44-45.) As a further step, Francisco operates by checking a list of file names determined at least in part by the content of the file and then checking to see if that file is authorized for use by the requesting user. (Mercer Decl. RACK-1010, p. 45.) These steps are shown graphically in annotated FIG. 2 of Francisco shown below.

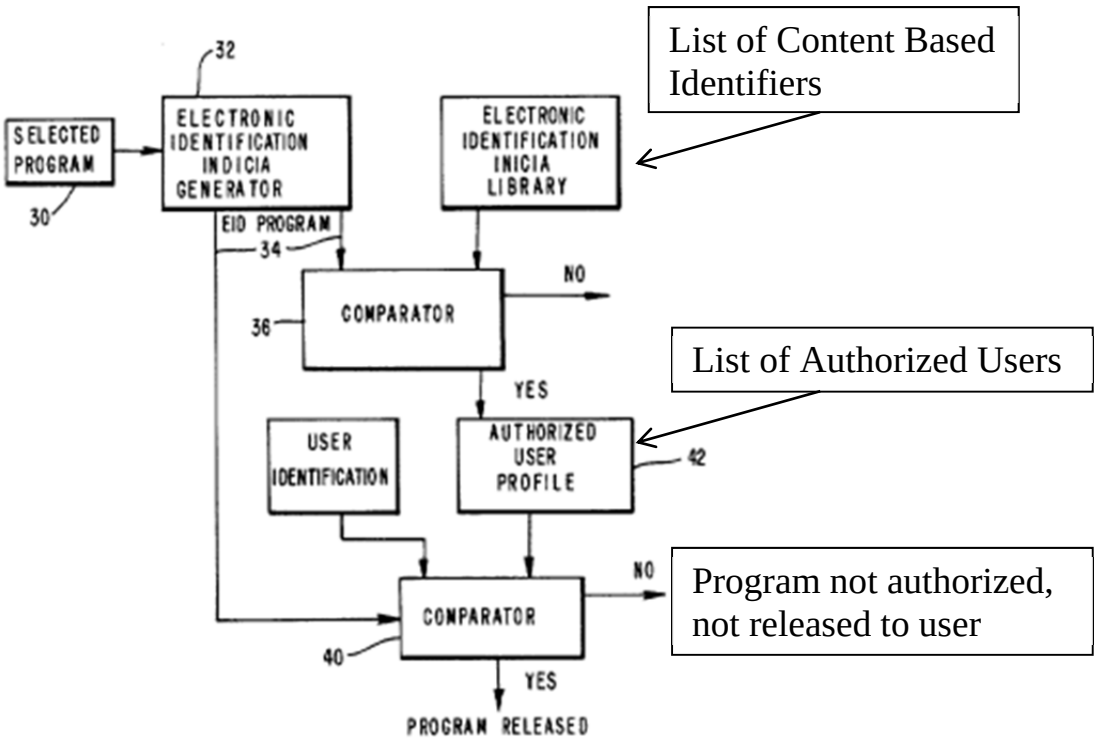

FIG. 2

Annotated FIG. 2 of Francisco

Thus, even if Francisco determines that the content of a file is authorized, the copy of the file residing on a computer may be unlicensed or unauthorized if the user is not authorized for use of the designated file. (Mercer Decl., RACK-1010, p. 45.)

It would have been obvious to combine the method of determining content based file identifiers and distributed storage of Woodhill with Francisco's method for maintaining a library of authorized files identifiers and comparing those identifiers to other files to determine if they are authorized files. (Mercer Decl., RACK-1010, p. 46.) Woodhill already suggests access control within the system

and Francisco provides a known technique of determining which files are authorized based on a comparison of content based identifiers such that the addition of Francisco's access control would utilize a known element to obtain a predictable result. (*Id.* at pp. 46-47.)

Claim 27

[27] ***A method as in claim 23 wherein the function is a message digest function or a hash function.***

As set forth above in [1b], Woodhill discloses that the function is a hash function. (Mercer Decl., RACK-1010, p. 47.)

Claim 30

[30] ***A method as in claim 23 wherein the function produces a substantially unique value based on the data comprising the data file.***

Woodhill discloses using four different functions, including a hash function calculated against the contents of the binary object to generate substantially unique values. (RACK-1004, 7:60-8:65 and Mercer Decl., RACK-1010, p. 47.) These functions, including the hash function value, are included in the Binary Object Identifier, that "is used to uniquely identify a particular binary object." (RACK-1004, 8:33-36, FIG. 3 and Mercer Decl., RACK-1010, p. 47.)

As shown above and as confirmed by Dr. Mercer, each and every element of the claims 1, 2, 4, 23, 27, and 30 is disclosed in or obvious in view of Woodhill

and Francisco. (Mercer Decl., RACK-1010, pp. 21-47.) Thus, these claims are obvious over Woodhill in combination with Francisco.

B. Challenge #2: Claim 7 is obvious under 35 U.S.C. § 103 based on Woodhill in view of Kahn

Woodhill creates unique file identifiers based on a hash of the contents of the data file and further discloses that file information can include access control data. Thus, Woodhill suggests that access control to the data files is already a part of the system set forth in the Woodhill patent. (Mercer Decl., RACK-1010, ¶66.) Although Woodhill does not expressly disclose that the data file represents a digital image, it does not exclude the possibility that the data files being stored within the system would include digital images. (*Id.*) Digital images were a common file type at the time of filing of the '442 Patent and as Dr. Mercer explains, a person of ordinary skill in the art would understand that the Woodhill reference contemplates that the data files would include digital images. (*Id.*)

U.S. Patent No. 6,135,646 to Kahn et al. (RACK-1006) issued on October 24, 2000 based on an application claiming priority to Oct. 22, 1993, which is before the earliest priority, April 11, 1995, of the '442 Patent. Therefore, Kahn is prior art to the '442 Patent under 35 U.S.C. § 102(e). Kahn discloses an example of a system for storing and controlling delivery of digital objects to authorized users of the system. (RACK-1006, 2:17-32.) The digital objects can include, among other things, digital image files. (RACK-1006, 1:17-21.) Still further,

users can be authorized to receive delivery of the digital objects if their certificates match the information on file with the system. (*see* RACK-1006, 22:26-26:38.) However, users requesting digital objects that do not have authorization to receive a digital object will not be sent a copy of the requested digital object. (RACK-1006, 25:1-3 and 54-57.) Digital objects can be requested between system components communication via direct connections such as TCP/IP. (RACK-1006, 10:39-48, and Mercer Decl., RACK-1010, ¶¶ 68-69.)

A person of ordinary skill in the art would have found it obvious to combine the method of Woodhill in view of Kahn because it would have been a use of known techniques to improve a similar methodology in the same way. (Mercer Decl., RACK-1010, ¶¶ 70-77.)

Woodhill recognizes that the data streams within its system include access control data. (RACK-1004, 7:40.) Access control data is understood by those skilled in the art to provide information concerning which users are entitled to access the particular data file. (Mercer Decl., RACK-1010, ¶73.) For example, a person of ordinary skill in the art would understand that the access control data of Woodhill refers to controlling access to certain files to system administrators while restricting access to such files by regular users of the system. (*Id*.) Moreover, to a person of ordinary skill in the art, a data storage or archive system would not provide restricted files in response to client requests from unauthorized users. (*Id*.)

A person of ordinary skill in the art would have found it obvious to combine the method of Woodhill in view of Kahn because it would have been a use of known techniques to improve a similar methodology in the same way. (Mercer Decl., RACK-1010, ¶70.)

Kahn discloses a procedure for retrieving a digital object from the system after a user has set-up an account. (RACK-1006, 23:48-26:38.) When requesting a copy of a digital file, the system checks whether the requester is an authorized party and if they are not, rather than sending the requested object, the system sends "an invalid-random-value-tag response to the requesting system." (RACK-1006, 25:1-8 and 25:54-58.) Only after verifying that the requesting party is authorized to receive the requested file, does the system "transmit [] to the requesting system: …the [digital] object, signed by the repository." (RACK-1006, 23:48-26:38.)

Claim 7

[7a] ***A method, in a system in which a plurality of files are distributed across a plurality of computers, wherein some of the computers communicate with each other using a TCP/IP communication protocol, the method comprising:***

As explained in detail above in [1a] of Challenge #1, Woodhill discloses a method for distributing files across of a plurality of computers. The statement in the preamble that "wherein some of the computers communicate with each other using a TCP/IP communication protocol" appears to be extra verbiage that should

not be provided patentable weight as it is not referenced in the body of the claim. To the extent that this well-known communication protocol is determined to be important to the claimed method steps, it is respectfully submitted that the Kahn patent recognizes that "messages will be sent between system components via direct connections (e.g., "TCP/IP")." (RACK-1006, 10:44-46.) It would be obvious to have some computers in the network of Woodhill communicate with each other using a TCP/IP communication protocol as taught by Kahn. (Mercer Decl., RACK-1010, p. 53.)

[7b] ***obtaining a name for a data file, the contents of said data file representing a digital image, the name having been determined using at least a given function of the data in the data file, wherein the data used by the given function to determine the name comprises the contents of the data file***

As discussed in [1b] of Challenge #1 above, Woodhill discloses obtaining a name for a data file, the name being determined using at least a given function of the data in the data file. As explained by Dr. Mercer, it would have been obvious to a person of ordinary skill in the art at the time of filing of the'442 Patent that the data file could represent a digital image. (Mercer Decl., RACK-1010, p. 53.) However, to the extent that Woodhill is deemed to not disclose digital image file types to a person of ordinary skill in the art at the time of filing, the Kahn reference expressly discloses that files may be "digital objects that can be any set of sequences of bits or digits and an associated unique identifier." (*Id*.) As Kahn

explains, "[d]igital objects may include conventional digital representations of works (books, papers, images, sounds, software). . . ." (RACK-1006, 1:18-20.) Thus, Kahn expressly discloses that a data file can represent a digital image. Utilizing the distributed storage system of Woodhill to store Kahn's digital images would be an obvious use of a known system to achieve predictable results. (Mercer Decl., RACK-1010, ¶72.)

[7c] ***and in response to a request for the data file, the request including at least the name of the data file, providing a copy of the file from a given one of the plurality of computers,***

As discussed in [1c] of Challenge #1 above, Woodhill discloses this limitation. (Mercer Decl., RACK-1010, p. 54.)

[7d] ***wherein a copy of the requested file is not provided to unlicensed parties or to unauthorized parties***

Woodhill discloses that access control data may be included with the content of data files. (Mercer Decl., RACK-1010, ¶71.) Access control data is understood by those skilled in the art to provide information concerning which users are entitled to access the particular data file. (*Id*.) Thus, Woodhill suggests that access control to the data files is already a part of the system set forth in the patent. (*Id*.) Although Woodhill does not expressly disclose how to use access control data to limit the provision of files to unauthorized/unlicensed parties, it was well known at the time to maintain a listing of authorized users and compare the requesting

party's credentials against a listing of authorized users. (*Id*.) Moreover, to a person of ordinary skill in the art, a data storage or archive system would not provide restricted files in response to client requests from unauthorized users. (Mercer Decl., RACK-1010, p. 55.)

An example of a system for controlling access to digital image files is provided in Kahn. The Kahn reference provides a system that restricts access to digital image files, among other digital representations of works, to those that are authorized to obtain copies of the files. (Mercer Decl., RACK-1010, ¶ 72-74). The digital objects of Kahn are stored on a network that prevents unauthorized access and only provides a copy of the digital object to authorized users. (Mercer Decl., RACK-1010, ¶ 74). As Dr. Mercer explains, one of ordinary skill in the art would have been motivated to combine the digital rights management techniques of Kahn with Woodhill's distributed storage system to utilize two existing capabilities in order to realize the benefits of distributed storage while inhibiting unauthorized copying. (Mercer Decl., RACK-1010, ¶76.) It would have been obvious to combine Woodhill's access control data with the user authentication techniques taught by Kahn to only provide copies of the requested digital image file to an authorized party and not provide copies of files to unauthorized parties as set forth in Kahn. (Mercer Decl., RACK-1010, ¶77.)

As shown above and as confirmed by Dr. Mercer, each and every element of claim 7 is disclosed in or obvious in view of Woodhill and Kahn. (Mercer Decl., RACK-1010, pp. 47-57.) Thus, claim 7 is obvious over Woodhill in combination with Kahn.

C. Challenge #3: Claim 28 is obvious under 35 U.S.C. § 103 based on Woodhill in view of Francisco and Langer

The Woodhill and Francisco references are described above in greater detail in Challenge #1with respect to the claim elements of independent claim 23. Claim 28 depends from claim 23 and adds the additional limitation that the function is selected from MD4, MD5, and SHA.

Albert Langer, "Re: dl/describe (File descriptions)," post to the "alt.sources" newsgroup on August 7, 1991 ("Langer"), (RACK-1004) was published more than a year before the priority date of the '442 Patent and is therefore prior art to the '442 Patent under 35 U.S.C. § 102(b). (*See* Reddy Decl., RACK-1011.) The Langer reference identifies a problem in "uniquely identifying files which may have different name and/or be in different directories on different systems (and also of being sure that files with the same name are identical …)." (RACK-1007, p. 3.) The Langer reference discloses that a solution to this problem would be to create unique identifiers based on the contents of the file. (RACK-1007, p. 4.) The Langer reference discloses "[a] simple method of defining a unique identifier that

does NOT include a particular site identifier would be to use a hash function on the entire contents of the file. This can be generated locally without requiring a registration system and if long enough the chances of collision are negligible. I would suggest using a cryptographic hash function such as MD5 which generates a 16 byte result." (RACK-1007, p. 4.)

Claim 28

[28] ***A method as in claim 23 wherein the function is selected from the functions: MD4, MD5, and SHA.***

As discussed in [23] of Challenge #1, Woodhill in view of Francisco discloses all of the elements of claim 23. Woodhill expressly discloses performing a hash of the contents of the data file. Woodhill does not expressly disclose the type of hash function contemplated for use in determining the identifier. Woodhill does disclose that "[t]hose of ordinary skill in the art will recognize that there exist many different ways to generate the Binary Object Identifier 74 (e.g. . . . using different calculations) and that the procedures set forth above is only one way of establishing the Binary Object Identifier 74." (RACK-1004, 8:52-58.) Woodhill recognizes that it is important that "the possibility of two different binary objects being assigned the same Binary Object Identifier 74 be very small." (RACK-1004, 8:33-36.)

Thus, one would be motivated to utilize functions that enhance security and that limit the chance of collision between files based on the disclosure of Woodhill. (Mercer Decl., RACK-1010, ¶¶ 81-83.) The Langer reference discusses techniques for the generation of unique identifiers by performing a function over the contents of a file. "A simple method of defining a unique identifier that does NOT include a particular site identifier would be to use a hash function of the entire contents of the file. … I would suggest using a cryptographic hash function such as MD5 which generates a 16 byte result." (RACK-1007, p. 4)

A person of ordinary skill in the art would be motivated to utilize the "cryptographic hash function such as MD5" disclosed in Langer as the hash function in determining the Binary Object Identifier of Woodhill because, at a minimum, the combination would have used known techniques to improve a similar system in the same way. (Mercer Decl., RACK-1010, pp.59-61.)

As shown above and as confirmed by Dr. Mercer, each and every element of claim 28 is disclosed in or obvious in view of Woodhill, Francisco, and Langer. (Mercer Decl., RACK-1010, pp. 57-61.) Thus, claim 28 is obvious over Woodhill in combination with Francisco and Langer.

VII. Conclusion

For the reasons set forth above, Petitioner has established a reasonable likelihood of prevailing with respect to at least one claim of the ‘442 Patent. Therefore, Petitioner asks that the Patent Office order an *inter partes* review trial and then proceed to cancel claims 1, 2, 4, 7, 23, 27, 28, and 30 of the ‘442 Patent.

Respectfully submitted,

Dated: October 11, 2013

/J. Andrew Lowes/

J. Andrew Lowes
Registration No. 40,706
HAYNES AND BOONE, LLP
Telephone: (972) 680-7557
Facsimile: (214) 200-0853

PETITIONER'S EXHIBIT LIST

October 11, 2013

Exhibit	Description
RACK-1001	U.S. Patent No. 6,928,442
RACK-1002	USPTO File Wrapper for U.S. Patent No. 6,928,442, including the prosecution history of U.S. Application No.: 09/987,723.
RACK-1003	USPTO File Wrapper for Ex Parte Reexamination 90/010,260
RACK-1004	U.S. Patent No. 5,649,196, ("Woodhill")
RACK-1005	U.S. Patent No. 4,845,715, ("Francisco")
RACK-1006	U.S. Patent No. 6,135,646, ("Kahn")
RACK-1007	Albert Langer, "Re: dl/describe (File descriptions)," article <1991Aug7.225159.786@newshost.anu.edu.au> in Usenet newsgroups "alt.sources.d" and "comp.archives.admin" (August 7, 1991)
RACK-1008	Decision, Institution of *Inter Partes* Review, IPR2013-00082
RACK-1009	Decision, Institution of *Inter Partes* Review, IPR2013-00083
RACK-1010	Declaration of Dr. Melvin Ray Mercer in support of Petition for *Inter Partes* Review of U.S. Patent No. 6,928,442
RACK-1011	Declaration of Dr. Narasimha Reddy in support of Petition for *Inter Partes* Review of U.S. Patent No. 6,928,442
RACK-1012	B. Reid, "USENET READERSHIP SUMMARY REPORT FOR AUG 91" (Sept. 1, 1991)
RACK-1013	B. Reid, "USENET Readership report for Aug 91" (Sep. 1, 1991)
RACK-1014	J.S. Quarterman, The Matrix (1990)

Exhibit	Description
RACK-1015	G. Todino et al., Using UUCP and Usenet (1991)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent of: Farber et al.	§	
	§	Petition for *Inter Partes* Review
U.S. Patent No. 6,928,442	§	
	§	Attorney Docket No.: 47015.137
Issued: Aug. 9, 2005	§	
	§	Customer No.: 116298
Title: ENFORCEMENT AND POLICING OF LICENSED CONTENT USING CONTENT-BASED IDENTIFIERS	§	
	§	Real Parties in Interest: Rackspace US, Inc. and Rackspace Hosting, Inc.

CERTIFICATE OF SERVICE

The undersigned certifies, in accordance with 37 C.F.R. § 42.205, that service was made on the Patent Owner as detailed below.

Date of service	October 11 2013
Manner of service	FEDERAL EXPRESS
Documents served	Petition for *Inter Partes* Review Petitioner's Exhibit List Exhibits RACK-1001 through RACK-1015
Persons served	Davidson Berquist Jackson & Gowdey LLP 4300 Wilson Blvd., 7th Floor Arlington, VA 22203

/J. Andrew Lowes/
J. Andrew Lowes
Registration No. 40,706