IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC, ***Plaintiff,*** v. **HITACHI LTD.; HITACHI DATA SYSTEMS CORPORATION; HITACHI VANTARA CORPORATION; AND HITACHI ID SYSTEMS, INC.** ***Defendant.***	**Civil Action No. 2:16-cv-1055-JRG** **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Marking Object Virtualization Intelligence, LLC ("MOV Intelligence" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos.: 6,802,006 ("the '006 patent"); 7,650,504 ("the '504 patent"); and 7,124,114 ("the '114 patent") (collectively, the "patents-in-suit" or the "MOV Intelligence Patents"). Defendants Hitachi Ltd. ("HL"); Hitachi Data Systems Corporation ("HDS"); Hitachi Vantara Corporation (HDS and Hitachi Vantara Corporation are collectively referred to herein as "Vantara"); and Hitachi ID Systems, Inc. ("HID") (collectively, "Hitachi" or "Defendant") infringe one or more of the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

INTRODUCTION

1. MOV Intelligence and its wholly-owned subsidiary, MOV Global Licensing LLC ("MOV Global Licensing") pursues the reasonable royalties owed for Hitachi's unauthorized use of patented groundbreaking technology both here in the United States and throughout Europe.

MOV Intelligence and its subsidiaries were assigned the rights to these patented technologies by Rovi Corporation ("Rovi").[1]

2. Rovi Corporation was a pioneer and leader in protecting computer technology, including digital rights management ("DRM") and digital watermarking systems. Rovi assigned MOV Intelligence rights to over 233 patents including many of John O. Ryan's, the founder of Rovi predecessor Macrovision, groundbreaking patents.[2]

THE PARTIES

MARKING OBJECT VIRTUALIZATION INTELLIGENCE, LLC

3. Marking Object Virtualization Intelligence, LLC ("MOV Intelligence") is a Texas limited liability company with its principal place of business located at 903 East 18th Street, Suite 217, Plano, Texas 75074. MOV Intelligence is committed to advancing the current state of DRM and watermarking technologies.

4. MOV Intelligence Global Licensing, LLC ("MOV Global Licensing") is a wholly-owned subsidiary of MOV Intelligence and assists in the licensing of MOV Intelligence's patents in territories outside the United States with a focus on the European Union (and the United Kingdom).[3] MOV Intelligence Global Licensing, LLC is a corporation organized under the laws of Delaware.

5. Rovi assigned the following patents to MOV Intelligence: U.S. Patent Nos. 7,299,209; 6,510,516; 6,802,006; 7,650,504; 6,813,640; 7,650,418; 7,200,230; 7,124,114; 6,381,367; 6,374,036; 6,360,000; 6,553,127; 6,701,062; 6,594,441; 7,764,790; 8,014,524; 6,931,536; and International Patent Nos. DE60047794; DE60148635.8; DE60211372.5; DE69901231.7-08; DK1047992; EP1047992; EP1303802; EP1332618; EP1444561;

[1] On April 29, 2016, Rovi Corporation acquired TiVo, Inc. The combined company operates under the name TiVo, Inc.

[2] *See* U.S. Patent Nos. 6,381,367; 7,764,790; 6,701,062; 8,014,524; German Patent Nos. DE60001837 and DE60001837D1; Chinese Patent No. CN1186941C; Canadian Patent No. CA2379992C; European Patent No. EP1198959B1; and Japanese Patent No. JP4387627B2.

[3] Wolfram Schrag, *EU-Patent steht auf der Kippe*, BR.COM NACHRICHTEN (August 2016).

ES1047992; FR1047992; FR1303802; FR1332618; FR1444561; GB1047992; GB1303802; GB1332618; GB1444561; GR3040059; IE1047992; IE1444561; IT1047992; NL1047992; NL1444561; PT1047992; and SE1047992.

6. MOV Intelligence has the right to sublicense the following international patent assets: AT1020077; AT1198959; AT1080584; ATE232346; AT1020077; AU729762; AU741281; AU753421; AU743639; AU714103; AU729762; AU2002351508; AU765747; AU2000263715; BE1020077; BE1198959; BE1020077; BE1080584; BE900498; BRPI 9812908-2; BR9709332.7; BRPI 9812908-2; CA2305254; CA2332546; CA2379992; CA2305254; CA2332548; CA2557859; CA2252726; CA2462679; CA2315212; CA2416304; CA2425115; CH1020077; CH1080584; CH900498; CH1020077; CH1047992; CNZL98809610.2; CNZL99806376.2; CNZL00811179.0; CNZL98809610.2; CNZL99806377.0; CNZL97194746.5; CNZL02820738.6; CNZL99802008.7; CNZL00819775.X; CNZL200510089437; DE69807102.608; DE60001837.7; DE69908352.4-08; DE69718907.4-08; DE69807102.608; DK1020077; DK1080584; DK1198959; DK1020077; DK900498; EP1020077; EP1198959; EP1080584; EP900498; EP1020077; ES1020077; ES1198959; ES1080584; ESES2191844; ES1020077; FI1020077; FI1080584; FI1020077; FI900498; FR1020077; FR1198959; FR1080584; FR900498; FR1020077; GB1020077; GB1198959; GB1080584; GB900498; GB1020077; GR3041381; GR3045620; GR3043304; GR3041381; HK1028696; HKHK1035625; HK1028696; HK1035282; HK1018562; HKHK1069234; HKHK1057115; HK1083653B; IE1020077; IE1198959; IE1020077; IE1080584; IE900498; IL135498; IL139543; IL148002; IL135498; IL139544; IN201442; IN220504; IN201442; IN207829; IT1020077; IT1080584; IT900498; IT1020077; JP4139560; JP4263706; JP4387627; JP4551617; JP4139560; JP4263706; JP3542557; JP4627809; JP4698925; JP4366037; JP4307069; KR374920; KR422997; KR761230; KR374920; KR362801; KR478072; KR689648; KR539987; KR752067; KR728517; KR593239; MX223464; MX231725; MX226464; MX223464; MX212991; MX214637; MX237690; MX240845; MYMY-123159-A; MYMY-123159-A; NL1020077; NL1198959; NL1080584;

NL900498; NL1020077; NZ503280; NZ507789; NZ503280; NZ532122; PT1010077; PT1198959; PT1080584; PT900498; PT1010077; RU2195084; RU2216121; RU2251821; RU2195084; RU2208301; RU2258252; SE1020077; SE1198959; SE1080584; SE900498; SE1020077; SG71485; SG76965; SG86547; SG76964; SG71485; TWNI117461; TWNI-124303; TWNI-130428; TWNI1600674; TWNI-162661; TWNI-202640; TWNI117461; TWNI-130754; and TWNI-184111.

HITACHI

7. On information and belief, Hitachi Data Systems Corporation was a Delaware corporation with a principal place of business located at 2845 Lafayette Street, Santa Clara, California 95050. Hitachi Data Systems Corporation can be served via its registered agent for service of process at Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, 211 E. 7th Street, Suite 620, Austin, Texas 78701. On information and belief, HDS has three offices in Texas, and is registered to do business in the state of Texas and has been since at least July 18, 1980.

8. On information and belief, Hitachi Data Systems Corporation has changed its name to Hitachi Vantara Corporation. On information and belief, on September 25, 2017, Hitachi Data Systems Corporation filed a "Certificate of Amendment of Certificate of Incorporation" with the State of Delaware effecting the change in name.

9. Plaintiff MOV Intelligence presently has no information on the roles, responsibilities, assets, and liabilities of Hitachi Vantara Corporation. For example, Hitachi, when requested, failed to provide a representation that the assets of Hitachi Data Systems Corporation are now the assets of Hitachi Vantara Corporation. Hitachi further failed to provide a stipulation agreeing that all pleadings and discovery requests previously served on HDS will be deemed served on Hitachi Vantara Corporation. Accordingly, with respect to this Second Amended Complaint, all allegations relating to "Vantara" shall be directed equally to Hitachi Data Systems Corporation and Hitachi Vantara Corporation. Plaintiff MOV Intelligence is

optimistic that any confusion relating to the name change from Hitachi Data Systems Corporation to Hitachi Vantara Corporation can be cleared up through agreement between the parties or through discovery.

10. On information and belief, Hitachi ID Systems, Inc. is a Canadian company with its principal place of business located at 500, 1401 1st Street S.E., Calgary, Alberta, Canada T2G 2J3. On information and belief, HID conducts business in Texas. For example, in a press release dated June 11, 2014 HID announced it was selected to provide identity management solutions for one of the world's largest energy companies, which is based in Texas. On information and belief, according to a job search advertisement posted on the website linkedin.com, HID is seeking to hire a senior account executive in the Houston, Texas area.

11. On information and belief, Hitachi Ltd. is a Japanese company with its principal place of business located at 6-6, Marunouchi 1-chome, Chiyoda-ku, Tokyo, 100-8280 Japan. According to its website, Hitachi Ltd. has 947 different consolidated subsidiaries, including Vantara and HID.

12. On information and belief, multiple Hitachi Ltd. subsidiaries have previously asserted patents in the Eastern District of Texas. *See, e.g., Hitachi Maxell, Ltd. v. Top Victory Electronics (Taiwan) Co. Ltd., et al.*, Case No. 2:14-cv-01121 (E.D. Tex. Dec. 16, 2014); *Hitachi Consumer Electronics Co. Ltd., et al. v. TPV Int'l (USA) Inc., et al.,* Case No. 2:13-cv-264 (E.D. Tex. April 8, 2013).

JURISDICTION AND VENUE

13. This action arises under the patent laws of the United States, Title 35 of the United States Code. Accordingly, this Court has exclusive subject matter jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338(a).

14. Upon information and belief, this Court has personal jurisdiction over Hitachi in this action because Hitachi has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Hitachi would not offend traditional notions of fair play and substantial justice.

Hitachi, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. In addition, at least HDS is registered to do business in the State of Texas, and defendant HID conducts business in the State of Texas.

15. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). At least HDS is registered to do business in Texas, and upon information and belief, Hitachi has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas.

MOV INTELLIGENCE'S LANDMARK INVENTIONS

16. The groundbreaking inventions in DRM and digital watermarking taught in the patents-in-suit were pioneered by Rovi. Rovi, established in 1983 under the name Macrovision, was a trailblazing technology company focused on inventing and bringing to market fundamental technologies designed to allow producers and distributors of film and music to widely distribute their products while simultaneously protecting their art from unauthorized copying.[4] Macrovision's copy protection technology became so important to content creators that Congress specifically regulated the manufacture and sale of technology that was incompatible with Macrovision's copy protection technology. *See* 17 U.S.C. § 1201(k)(1) ("unless such recorder conforms to the automatic gain control copy control technology").[5] Rovi broadened its focus to include copy protection and DRM for other media,[6] including computer executables, firmware, operating system images, watermarking, and encryption.

[4] Aljean Harmetz, *Cotton Club Cassettes Coded to Foil Pirates*, N.Y. TIMES (April 24, 1985).

[5] *See also* David Nimmer, *Back from the Future: A Proleptic Review of the Digital Millennium Copyright Act*, 16 BERKELEY TECH. L.J. 855, 862 (2001) (The DMCA "contains a welter of corporation-specific features, relating to Macrovision Corp. The features in question relate to section 1201's controls on consumer analog devices.") (citations omitted).

[6] *See* Michael Arnold et al., TECHNIQUES AND APPLICATIONS OF DIGITAL WATERMARKING AND CONTENT PROTECTION 203 (2002) (Describing Rovi's Cactus Data Shield product which by 2002 had been used in over 100 million compact discs. "This scheme [Rovi Cactus Data Shield] operates by inserting illegal data values instead of error-correcting codes."); *see also Rovi*

17. MOV Intelligence's patent portfolio, which includes more than 233 issued patents worldwide, is a direct result of Rovi's substantial investment in research and development. The asserted MOV Intelligence patents are reflective of this history of innovation, embodying a number of firsts in the development of DRM and watermarking technologies.

18. MOV Intelligence long-term financial success depends in part on its ability to establish, maintain, and protect its proprietary technology through patents. Defendants' infringement presents significant and ongoing damage to MOV Intelligence's business. Hitachi, in an effort to expand its product base and profit from the sale of patented technology, has chosen to incorporate MOV Intelligence's fundamental technology without a license or payment.

THE ASSERTED PATENTS

U.S. PATENT NO. 6,802,006

19. U.S. Patent No. 6,802,006 (the "'006 patent"), entitled "System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images," was filed on July 22, 1999, and claims priority to January 15, 1999. MOV Intelligence is the owner of all right, title, and interest in the '006 patent. A true and correct copy of the '006 patent is attached hereto as Exhibit A. The '006 patent claims specific methods and systems for verifying the authenticity of executable images. The system includes a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable image, determines an authenticity digital signature to verify that the executable image has not been improperly modified.

SafeDisc Copy Protection Overview, MACROVISION CORPORATION DATASHEET at 2 (1999) ("SafeDisc incorporates a unique authentication technology that prevents the re-mastering of CD-ROM titles and deters attempts to make unauthorized copies. The SafeDisc authentication process ensures that consumers will only be able to play original discs. The user is forced to purchase a legitimate copy."); Kirby Kish, MACROSAFE SYSTEM: A SOLUTION FOR SECURE DIGITAL MEDIA DISTRIBUTION at 7 (January 2002) (showing the architecture of the MacroSafe system and use of a DRM Server and Key Escrow Server).

20. The ‘006 patent has been cited by over 85 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘006 patent as relevant prior art:

- Intertrust Technologies Corporation
- International Business Machines Corporation
- Intel Corporation
- Microsoft Corporation
- Check Point Software Technologies, Inc.
- Nokia Corporation
- Ipass, Inc.
- Nytell Software LLC
- Amazon Technologies, Inc.
- Panasonic Corporation
- Matsushita Electric Ind. Co. Ltd.
- NXP B.V. (now Cisco Systems, Inc.)
- Intel Corporation
- Hewlett-Packard Development Company, L.P.
- Apple, Inc.
- Lockheed Martin Corporation
- Symantec Corporation
- Zone Labs, Inc.

21. The ‘006 patent claims a technical solution to a problem unique to computer systems: verifying and authenticating executable images.

U.S. PATENT NO. 7,650,504

22. U.S. Patent No. 7,650,504 (the “‘504 patent”), entitled “System and Method of Verifying the Authenticity of Dynamically Connectable Executable Images,” was filed on August 23, 2004, and claims priority to July 22, 1999. MOV Intelligence is the owner of all right, title and interest in the ‘504 patent. A true and correct copy of the ‘504 patent is attached hereto as Exhibit B. The ‘504 patent claims specific methods and systems for verifying the authenticity of executable images. The systems and methods taught in the ‘504 patent incorporate a validator that determines a reference digital signature for an executable image using the contents of the executable image excluding those portions of the executable that are fixed-up by a program loader. The validator then, subsequent to the loading of the executable

image, determines an authenticity digital signature to verify that the executable image has not been improperly modified. In addition, the validator ensures that each of the pointers in the executable image have not been improperly redirected.

23. The '504 patent and its underlying application have been cited by over 30 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '504 patent as relevant prior art:

- Qualcomm Incorporated
- Intel Corporation
- Micro Beef Technologies, Ltd
- Microsoft Corporation
- Apple, Inc.
- Symantec Corporation
- Samsung Electronics Co., Ltd.
- Cybersoft Technologies, Inc.
- Electronics and Telecommunications Research Institute (ETRI)

24. The '504 patent claims a technical solution to a problem unique to the transmission of digital information over a network: verifying the identity of a software application in a dynamic loading environment. In particular, the system determines whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

U.S. PATENT NO. 7,124,114

25. U.S. Patent No. 7,124,114 (the "'114 patent"), entitled "Method and Apparatus for Determining Digital A/V Content Distribution Terms Based on Detected Piracy Levels," was filed on November 9, 2000. MOV Intelligence is the owner of all right, title and interest in the '114 patent. A true and correct copy of the '114 patent is attached hereto as Exhibit C. The '114 patent claims specific methods and systems for distributing copyrighted material over a computer network. Specifically, the '114 patent teaches the providing of protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient; and providing or withholding a copy of the protected material to the prospective recipient in accordance with the terms. The

‘114 patent also discloses the use of a first set of program code which serves to ascertain terms for providing a protected material to a prospective recipient according at least in part to information of unauthorized copying of other protected material previously provided to the prospective recipient. The first set of program code also serves to provide or withhold a copy of the protected material to or from the prospective recipient in accordance with the terms.

26. The ‘114 patent family has been cited by over 39 issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘114 patent as relevant prior art:

- Google, Inc.
- NBCUniversal Media, Inc.
- Digimarc Corporation
- Hewlett-Packard Development Company, L.P.
- Aigo Research Institute of Image Computing Co., Ltd.
- AT&T Intellectual Property I, L.P.
- General Electric Company
- The Nielsen Company (US), LLC
- Sca Ipla Holdings, Inc.
- Thomson Licensing, Inc.
- Fujitsu Limited

27. The ‘114 patent claims a technical solution to a problem unique to the transmission of digital information over a network: preventing the unauthorized copying of digital content. The patent teaches the use of a distribution server that distributes A/V content to a recipient according to terms determined from information stored in a database of prior unauthorized copying attributed to that recipient.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 6,802,006

28. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

29. At least Vantara and/or HL design, make, use, sell, and/or offer for sale in the United States products and/or services for determining the authenticity of an executable image.

30. On information and belief, Vantara and/or HL makes, sells, offers to sell, imports and/or uses the Hitachi Content Platform Versions 7.1.2, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.3, and 7.3.1, and Hitachi Content Platform Anywhere Versions 2.04, 2.1, 2.1.1, 2.1.2, 3.0 (collectively, the "Hitachi Content Platform").

31. On information and belief, Vantara sells the Hitachi Content Platform (collectively, the "Hitachi '006 Products") to customers in the Eastern District of Texas.

32. The Vantara website (www.hitachivantara.com) contains hundreds of technical documents, marketing materials, and white papers authored by Vantara that describe and market the Hitachi '006 Products.

33. In addition, or in the alternative, on information and belief, HL makes, sells, offers to sell, imports, and/or uses the Hitachi '006 Product(s). For example, Vantara documentation relating to the Hitachi Content Platform explain that "Hitachi, Ltd., reserves the right to make changes to this document at any time without notice . . . ."[7] HL further explains that Hitachi Data Systems is a registered trademark belonging to HL.[8] The same or similar statements appear in numerous other documents related to the Hitachi '006 Products.

THE HITACHI CONTENT PLATFORM

34. On information and belief, one or more Hitachi subsidiaries and/or affiliates use the Hitachi Content Platform in regular business operations.

35. On information and belief, one or more of the Hitachi Content Platform products include authentication technology.

36. On information and belief, the Hitachi Content Platform is a system wherein an executable image has one or more pointers needed for fixing up by a program loader. Specifically, the Hitachi Content Platform "includes many features specifically designed to

[7] HITACHI CONTENT PLATFORM DOCUMENTATION, *Hitachi Data Instance Director User's Guide*, available at: https://support.hds.com/download/epcra/hdid0010.pdf.
[8] *Id.*

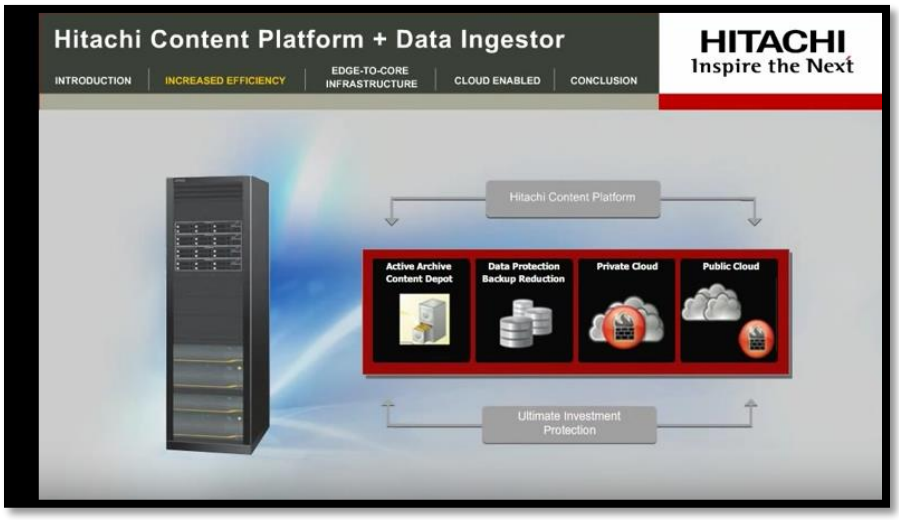
protect the integrity and ensure the security of stored data." HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM at 17-18 (April 2012).

37. On information and belief, the executable image in the Hitachi Content Platform is a stored object. "[E]ach object permanently associates data HCP receives (for example, a file, an image or a database) with information about that data, called metadata." HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM at 10 (April 2012).[9]

38. On information and belief, the Hitachi Content Platform enables the storage of "backup images" of systems. "Some actually store backup images to HCP where, compression, efficient data protection, and faster recall rates provide value beyond backup storage to tape or expensive block deduplication appliances." HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS at 6 (September 2016).

39. Hitachi Product demonstration videos for the Hitachi Content Platform state "this platform gives IT organization the ability to deploy a single intelligent object-based storage infrastructure to house and manage the massive amounts of unstructured data."

[9] *See also* HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS at 5 (September 2016) ("HCP serves as the single foundation for storing data from multiple applications, such as a variety of archiving applications (for example, file, email, recordings, database, Microsoft SharePoint and medical images.) It also serves as a repository for newer Web 2.0 S-3-enables cloud, big data, mobile sync and share, remote and branch office, file and open sources application data – all form a single point of management.").



Hitachi Content Platform and Hitachi Data Ingestor Product Demo, HITACHI DATA SYSTEMS VIDEO at 3:02 (March 2011), available at: https://www.youtube.com/watch?v=5WfIVW4rvAc

40. On information and belief, the Hitachi Product enables functionality where the executable image contains both the "fixed-content data, "system metadata," "custom metadata," "access control lists," and "appendable objects." HITACHI CONTENT PLATFORM: ADMINISTERING HCP at 2-3 (2015).

41. On information and belief, Hitachi's documentation states that the cryptographic hash algorithm used by the Hitachi Content Platform is "namespace dependent."

> One of the hash values that's generated only from the object data is also stored with the secondary metadata for the object. The cryptographic hash algorithm HCP uses to calculate this hash value is namespace dependent. It is set when the namespace is created. Once set, it cannot be changed.

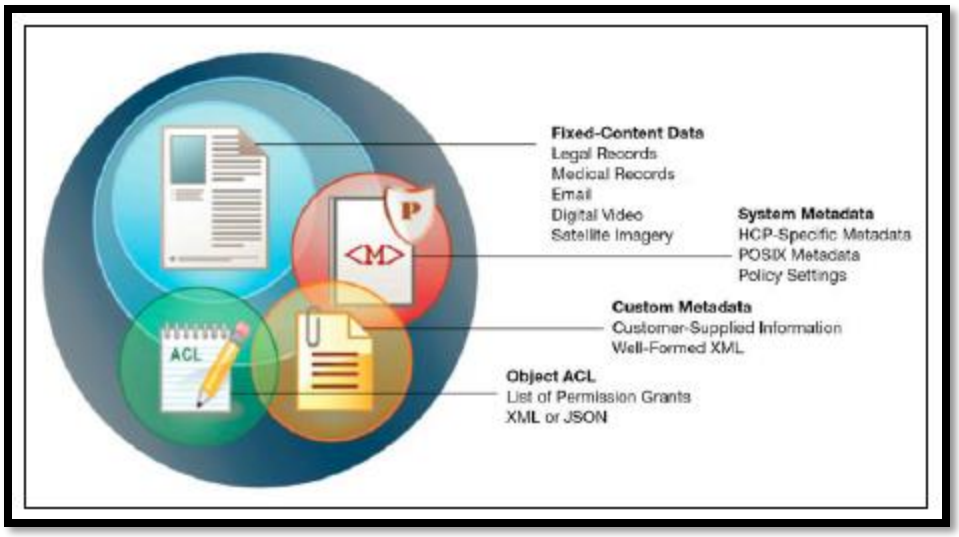
HCP-Specific HTTP Response Headers, HITACHI CONTENT PLATFORM (HCP) System Management Help (2016).

42. On information and belief, the Hitachi Content Platform includes the ability to store "appendable objects," "access control lists," and "metadata" with fixed-content data.

43. On information and belief, Hitachi documentation for the Hitachi Content Platform states, "if the primary metadata is missing a pointer to a copy of the object data, the service reconstructs the pointer." HITACHI CONTENT PLATFORM: ADMINISTERING HCP at 350

(2015). Moreover, an access control list which is a "set of grants of permissions to preform various operations on the object" are configured to function as a pointer that references either a point in the executable image or reference a location in the memory of the system for managing access control to the executable image. HITACHI CONTENT PLATFORM: ADMINISTERING HCP at 3 (2015).

44. On information and belief, the below image from Hitachi's documentation of the Hitachi Content Platform shows the executable image (e.g., Object Container Structure) that is stored in the system and is comprised of the "fixed content data" and metadata and access control list.



HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS at 16 (September 2016) (showing the storage of Object ACL, Custom Metadata, System Metadata in the executable image ("object container structure").

45. On information and belief, the Hitachi Content Platform contains a validator that determines whether the reference digital signature matches the authenticity digital signature. Specifically, the Hitachi Content Platform implements a content verification system that "[g]uarantees data integrity of repository objects by ensuring that a file matches its digital hash signature. HCP repairs the object if the hash does not match." HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS at 18 (September 2016).

46. On information and belief, white papers from Hitachi discussing the Hitachi Content Platform state that the validator includes functionality where the "digital signature for each object is periodically computed and compared by [the Hitachi] Content Platform against the original value that was stored when the file was first archive."

> *Authenticity*
>
> A request to guarantee of data's authenticity usually emerges during legal investigations or compulsory procedures. The organization must be able to prove that documents have not been altered. HCP addresses this security requisite with a digital signature for each incoming file. One of the following hashing algorithms creates the unique identifier: MD5, SHA-1, SHA-256, SHA-384 or SHA-512. The digital signature for each object is periodically computed and compared by Content Platform against the original value that was stored when the file was first archived.

Solve Data Protection and Security Issues Amid Big Data Cloud and Unbridled Enterprise Growth, HITACHI DATA SYSTEMS WHITE PAPER at 10 (January 2015).

47. On information and belief, the Hitachi Content Platform comprises a system that contains a validator capable of generating at a first point in time a reference digital signature based upon a selected content of the executable image excluding each of the pointers. Specifically, the Hitachi Content Platform generates a reference digital signature when an object is ingested into the system. The reference digital signature is based on the "fixed content data" and thus excludes the each of the pointers which would be contained in the Object ACL, Appended Object Data or Metadata that is part of the executable image ("HCP Object").

48. On information and belief, Hitachi documentation describing the Hitachi Content Platform states that a file is "fingerprinted upon ingest using a hash algorithm."

> **Fixed-content data** is an exact digital copy of a written file which is "fingerprinted" upon ingest using a hashing algorithm: MD5, SHA-1, **SHA-256 (default)**, SHA384, SHA-512 or RIPMD160. These files become immutable after being successfully stored in a virtual storage pool. If the object is under retention, it cannot be deleted before the expiration of its retention period (see compliance modes). If versioning is enabled, multiple versions of a file can be retained.

HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS at 16 (September 2016).

49. On information and belief, the Hitachi Content Platform comprises a validator capable of generating a cryptographic hash value that is calculated from the object data. *See* HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM at 18 (April

2012) ("Each data object has a cryptographic hash value that is calculated from the object data. The content verification service ensures the integrity of each object by periodically checking that its data still matches its hash value.").

50. On information and belief, the Hitachi Content Platform comprises a validator that generates an authenticity digital signature at a second point in time based upon the selected content of the executable image excluding each of the pointers. Specifically, the Hitachi Product contains functionality where the "The content verification service regenerates cryptographic hash values to detect object corruption." HITACHI CONTENT PLATFORM: ADMINISTERING HCP at 348 (2015).

51. On information and belief, documentation for the Hitachi Content Platform identifies the authenticity digital signature as being a "cryptographic [] value." "A system-generated metadata value calculated by a cryptographic hash algorithm from object data or object data and metadata. This value is used to verify that the content of an object has not changed." *Id*. at 632.

52. On information and belief, Vantara and/or HL have directly infringed and continue to directly infringe the '006 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Hitachi '006 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation: Hitachi Content Platform Versions 7.1.2, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.3, and 7.3.1, and Hitachi Content Platform Anywhere Versions 2.04, 2.1, 2.1.1, 2.1.2, 3.0.

53. By making, using, testing, offering for sale, and/or selling verification and authentication products and services, including but not limited to the Hitachi '006 Products, Vantara and/or HL has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '006 patent, including at least claims 1-11 and 13-19, pursuant to 35 U.S.C. § 271(a).

54. On information and belief, Vantara and/or HL also indirectly infringe the '006 patent by actively inducing infringement under 35 USC § 271(b).

55. On information and belief, Vantara and/or HL had knowledge of the '006 patent since at least service of the first Complaint in this action or shortly thereafter, and on information and belief, Vantara and/or HL knew of the '006 patent and knew of its infringement, including by way of this lawsuit.

56. On information and belief, Vantara and/or HL intended to induce patent infringement by third-party customers and users of the Hitachi '006 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Vantara and/or HL specifically intended and were aware that the normal and customary use of the accused products would infringe the '006 patent. Vantara and/or HL performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '006 patent and with the knowledge that the induced acts would constitute infringement.

57. Vantara and/or HL provides the Hitachi '006 Products that have the capability of operating in a manner that infringe one or more of the claims of the '006 patent, including at least claims 1-11 and 13-19, and Vantara and/or HL further provides documentation and training materials that cause customers and end users of the Hitachi Content Platform[10] to utilize the products in a manner that directly infringe one or more claims of the '006 patent. By providing instruction and training to customers and end-users on how to use the Hitachi '006 Products in a manner that directly infringes one or more claims of the '006 patent, including at least claims 1-11 and 13-19, Vantara and/or HL specifically intended to induce infringement of the '006 patent.

[10] *See e.g.*, HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM (April 2012); HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS (September 2016); HITACHI CONTENT PLATFORM: ADMINISTERING HCP (2015); HITACHI CONTENT PLATFORM (HCP) SYSTEM MANAGEMENT HELP (2016); HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM (April 2012); *Solve Data Protection and Security Issues Amid Big Data Cloud and Unbridled Enterprise Growth*, HITACHI DATA SYSTEMS WHITE PAPER (January 2015).

On information and belief, Vantara and/or HL engaged in such inducement to promote the sales of the Hitachi '006 Products, *e.g.*, through user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '006 patent. Accordingly, Vantara and/or HL has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '006 patent, knowing that such use constitutes infringement of the '006 patent.

58. A detailed explanation of Vantara and/or HL's infringement of the '006 patent by the Hitachi '006 Products was provided to Defendants as Exhibit A of Plaintiff MOV Intelligence's Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to Local Patent Rules 3-1 and 3-2, served on July 12, 2017, and as Exhibit A to Plaintiff MOV Intelligence's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions, served on August 23, 2017.

59. The '006 patent is well-known within the industry as demonstrated by the over 85 citations to the '006 patent in issued patents and published patent applications assigned to technology companies and academic institutions. Several of Hitachi's competitors have paid considerable licensing fees for their use of the technology claimed by the '006 patent. In an effort to gain an advantage over Hitachi's competitors by utilizing the same licensed technology without paying reasonable royalties, Vantara and/or HL infringed the '006 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

60. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '006 patent.

61. As a result of Vantara and/or HL's infringement of the '006 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Hitachi's infringement, but in no event less than a reasonable royalty for the use made of the invention by Vantara and/or HL together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,650,504

62. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

63. At least Vantara and/or HL designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for verifying the authenticity of executable images.

64. On information and belief, Vantara and/or HL makes, sells, offers to sell, imports and/or uses the Hitachi Content Platform Versions 7.1.2, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.3, and 7.3.1, and Hitachi Content Platform Anywhere Versions 2.04, 2.1, 2.1.1, 2.1.2, 3.0 (collectively, the "Hitachi Content Platform").

65. On information and belief, Vantara sells the Hitachi Content Platform (collectively, the "Hitachi '504 Product(s)") to customers in the Eastern District of Texas.

66. The Vantara website (www.hitachivantara.com) contains hundreds of technical documents, marketing materials, and white papers authored by Vantara that describe and market the Hitachi '504 Products.

67. In addition, or in the alternative, on information and belief, HL makes, sells, offers to sell, imports, and/or uses the Hitachi '504 Product(s). For example, Vantara documentation relating to the Hitachi Content Platform explain that "Hitachi, Ltd., reserves the right to make changes to this document at any time without notice . . . ."[11] HL further explains that Hitachi Data Systems is a registered trademark belonging to HL.[12] The same or similar statements appear in numerous other documents related to the Hitachi '504 Products.

68. On information and belief, one or more Hitachi subsidiaries and/or affiliates use the Hitachi '504 Products in regular business operations.

69. On information and belief, one or more of the Hitachi '504 Products include authentication technology.

[11] HITACHI CONTENT PLATFORM DOCUMENTATION, *Hitachi Data Instance Director User's Guide*, available at: https://support.hds.com/download/epcra/hdid0010.pdf.
[12] *Id.*

70. On information and belief, one or more of the Hitachi '504 Products comprise systems and methods for determining the authenticity of an executable image.

71. On information and belief, one or more of the Hitachi '504 Products enable authenticating and verifying an executable image. In particular, the Hitachi '504 Products determine whether a software application that has been dynamically connected to another data object has been tampered with subsequent to the execution of the software application.

72. On information and belief, the Hitachi '504 Products are available to businesses and individuals throughout the United States.

73. On information and belief, the Hitachi '504 Products are provided to businesses and individuals located in the Eastern District of Texas.

74. On information and belief, the Hitachi '504 Products comprise a computer configured to execute an executable image having one or more pointers in need of fixing up by a program loader.

75. On information and belief, the Hitachi '504 Products enable the verification of the integrity of software images.

76. On information and belief, the Hitachi '504 Products encompass a validator configured to generate a reference digital signature prior to loading the executable image into memory and an authenticity digital signature after loading the executable image into memory.

77. On information and belief, the Hitachi '504 Product also supports generating a digital signature using a hash. As the comparison of a first hash and second hash (for the replicated data) is performed on an executable image that is unmounted the digital signature (hash) excludes one or more pointers in need of fixing-up.

78. On information and belief, the Hitachi '504 Product includes functionality whereby both the reference digital signature and the authenticity digital signature exclude the one or more pointers in need of fixing up.

79. On information and belief, the Hitachi '504 Product is configured to compare the reference digital signature and the authenticity digital signature for the performance of an authenticity check.

80. On information and belief, the Hitachi '504 Product contains functionality wherein the validator is configured to determine whether each of the pointers references a correct location that is within the executable image after each of the pointers has been bound.

81. On information and belief, the Hitachi '504 Products enable the detection of corrupted data in a computer image.

82. On information and belief, Vantara and/or HL have directly infringed and continue to directly infringe the '504 patent by, among other things, making, using, offering for sale, and/or selling content protection technology, including but not limited to the Hitachi '504 Products, which includes technology for verifying the authenticity of a software image. Such products and/or services include, by way of example and without limitation, the Hitachi Content Platform Versions 7.1.2, 7.2, 7.2.1, 7.2.2, 7.2.3, 7.3, and 7.3.1, and Hitachi Content Platform Anywhere Versions 2.04, 2.1, 2.1.1, 2.1.2, 3.0.

83. By making, using, testing, offering for sale, and/or selling authentication and verification technologies and services, including but not limited to the Hitachi '504 Products, Vantara and/or HL have has injured MOV Intelligence and are liable to MOV Intelligence for directly infringing one or more claims of the '504 patent, including at least claims 1-7 and 10-12, pursuant to 35 U.S.C. § 271(a).

84. On information and belief, Vantara and/or HL have also indirectly infringes the '504 patent by actively inducing infringement under 35 USC § 271(b).

85. On information and belief, Vantara and/or HL have had knowledge of the '504 patent since at least service of the first Complaint in this action or shortly thereafter, and on information and belief, Vantara and/or HL knew of the '504 patent and knew of its infringement, including by way of this lawsuit.

86. On information and belief, Vantara and/or HL intended to induce patent infringement by third-party customers and users of the Hitachi '504 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Vantara and/or HL specifically intended and were aware that the normal and customary use of the accused products would infringe the '504 patent. Vantara and/or HL performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '504 patent and with the knowledge that the induced acts would constitute infringement. For example, Vantara and/or HL provide the Hitachi '504 Products that have the capability of operating in a manner that infringe one or more of the claims of the '504 patent, including at least claims 1-7 and 10-12, and Vantara and/or HL further provides documentation and training materials that cause customers and end users of the Hitachi '504 Products to utilize the products in a manner that directly infringe one or more claims of the '504 patent.[13] By providing instruction and training to customers and end-users on how to use the Hitachi '504 Products in a manner that directly infringes one or more claims of the '504 patent, including at least claims 1-7 and 10-12, Vantara and/or HL specifically intended to induce infringement of the '504 patent. On information and belief, Vantara and/or HL engaged in such inducement to promote the sales of the Hitachi '504 Products, e.g., through user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '504 patent. Accordingly, Vantara and/or HL has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '504 patent, knowing that such use constitutes infringement of the '504 patent.

[13] *See e.g.*, HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM (April 2012); HITACHI CONTENT PLATFORM ARCHITECTURE FUNDAMENTALS (September 2016); HITACHI CONTENT PLATFORM: ADMINISTERING HCP (2015); HITACHI CONTENT PLATFORM (HCP) SYSTEM MANAGEMENT HELP (2016); HOW TO MANAGE UNSTRUCTURED DATA WITH THE HITACHI CONTENT PLATFORM (April 2012); *Solve Data Protection and Security Issues Amid Big Data Cloud and Unbridled Enterprise Growth*, HITACHI DATA SYSTEMS WHITE PAPER (January 2015).

87. A detailed explanation of Vantara and/or HL's infringement of the '504 patent by the Hitachi '504 Products was provided to Defendants as Exhibit C of Plaintiff MOV Intelligence's Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to Local Patent Rules 3-1 and 3-2, served on July 12, 2017, and as Exhibit B to Plaintiff MOV Intelligence's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions, served on August 23, 2017.

88. The '504 patent is well-known within the industry as demonstrated by the over 30 citations to the '504 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Apple, Inc. and Electronics and Telecommunications Research Institute (ETRI)). Several of Hitachi's competitors have paid considerable licensing fees for their use of the technology claimed by the '504 patent. In an effort to gain an advantage over Hitachi's competitors by utilizing the same licensed technology without paying reasonable royalties, Hitachi infringed the '504 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

89. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '504 patent.

90. As a result of Vantara and/or HL's infringement of the '504 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Vantara and/or HL's infringement, but in no event less than a reasonable royalty for the use made of the invention by Vantara and/or HL together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,124,114

91. MOV Intelligence references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

92. HID designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing the distribution of digital content and preventing unauthorized access to protected digital content.

93. On information and belief, HID designs, makes, sells, offers to sell, imports, and/or uses the Hitachi ID Identity and Access Management Suite Versions 10.0 and 10.1 (the "Hitachi '114 Product(s)").

94. For example, HID's website describes the features and architecture of the Hitachi '114 Product(s) and also markets the Hitachi '114 Product(s). HID documents related to the Hitachi '114 Product(s) available on HID's website include a "sales@Hitachi-ID.com" email address. HID is described by documents on its website as delivering "access governance and identity administration solutions to organizations globally. Hitachi ID solutions are used by Fortune 500 companies to secure access to systems in the enterprise and in the cloud."

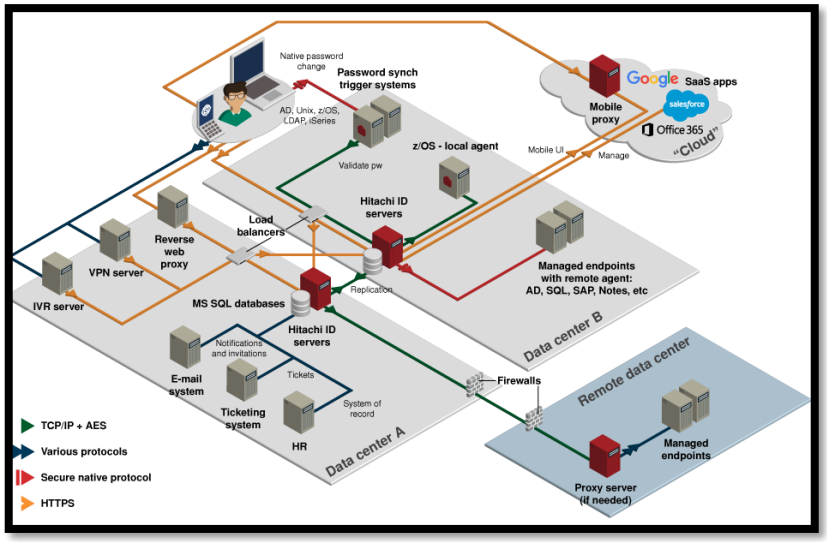
95. On information and belief, HID designs, makes, sells, offers to sell, imports, and/or uses the Hitachi '114 Product(s).

96. For example, a January 14, 2015 press release describes HID forming a "strategic partnership" with Vantara to "bundle its IAM suite, which consists of Identity Manager, Password Manager and Privileged Access Manager, with select Hitachi Content Platform and Hitachi Unified Compute Platform offerings from Hitachi Data Systems." Howard Trottenberg, HID's Senior Vice President, Channels, described the partnership as follows: "This strategic move opens new avenues for HIDS to expand the sales of its IAM solutions through the vast global reach of the HDS channel and direct sales force."

97. On information and belief, one or more Hitachi subsidiaries and/or affiliates use the Hitachi '114 Products in regular business operations.

98. On information and belief, one or more of the Hitachi '114 Products include content protection and content access technology.

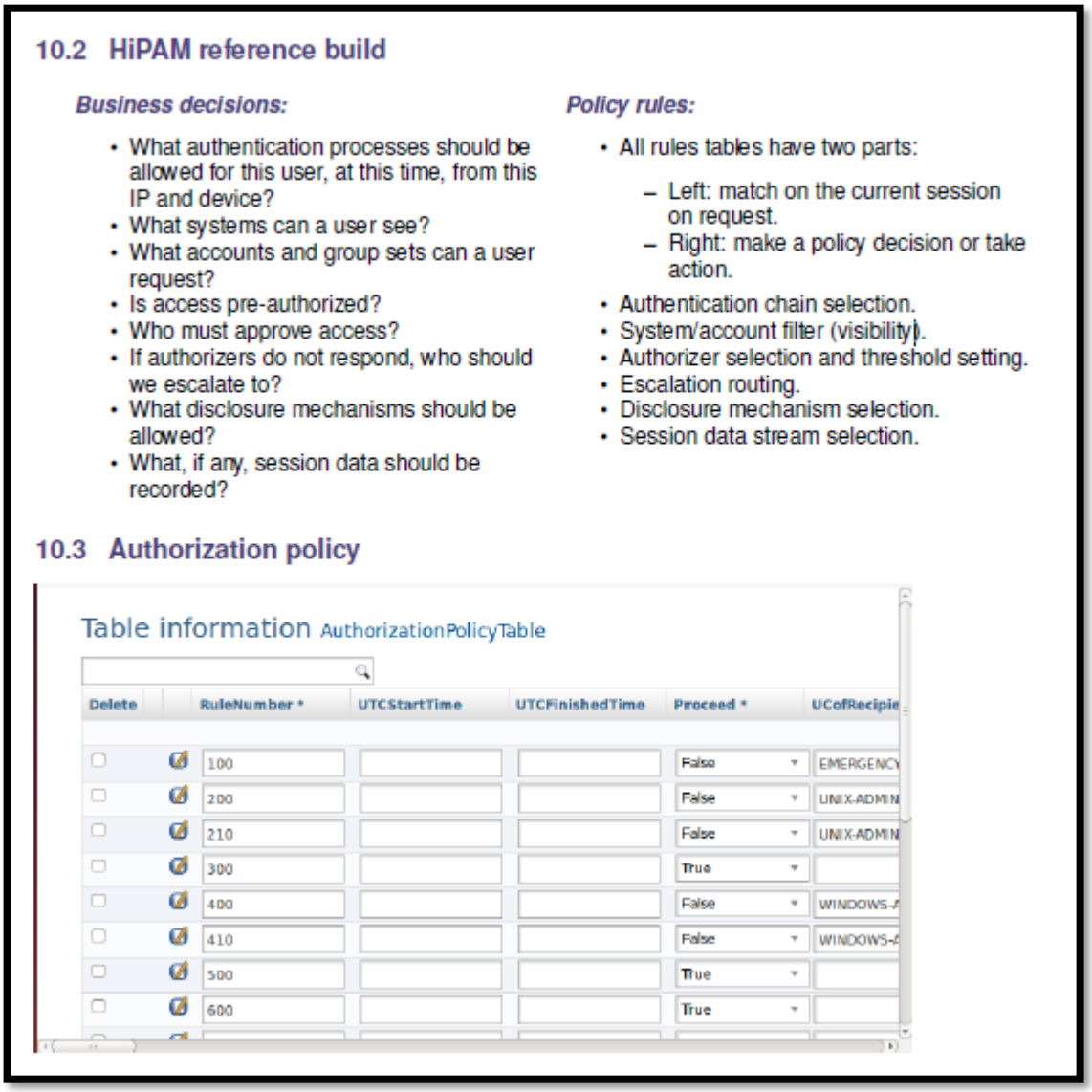
99. On information and belief, one or more of the Hitachi '114 Products enable providing or withholding access to digital content is accordance with digital rights management protection terms. The below image from the Hitachi ID website shows the system architecture.



Hitachi ID Identity and Access Management Suite Architecture, HITACHI ID WEBSITE (last visited November 2016), *available at*: https://hitachi-id.com/technology/architecture.html

100. On information and belief, the Hitachi '114 Product performs the step of ascertaining terms for providing a protected material (e.g., digital file) to a prospective recipient (e.g., User A) according at least in part to information of unauthorized copying of other protected materials previously provided to the prospective recipient (e.g., User A). Specifically, HID determines whether to grant access or withhold access to a digital file based on the prior actions of a user on the network. For example, the Hitachi '114 Product will look at prior unauthorized requests to determine whether a user should be given access to a digital file that the user is requesting. "Expanded risk analytics, including ***pattern analysis to compare new requests to what peers of the recipient have recently accessed***." *Hitachi ID Suite 10.0 Features*, HITACHI ID WEBSITE (last visited November 2016), *available at:* https://hitachi-id.com/products/hitachi-id-identity-and-access-management-suite-10.0-whats-new.html (emphasis added).

101. On information and belief, the Hitachi '114 Product performs the step of providing or withholding a copy of the protected material to a user (e.g., User A) based on the ascertained terms. Specifically, the Hitachi '114 Product will deny access to content and not transmit a copy of the content to a user if the user has previously requested unauthorized content above a certain threshold.

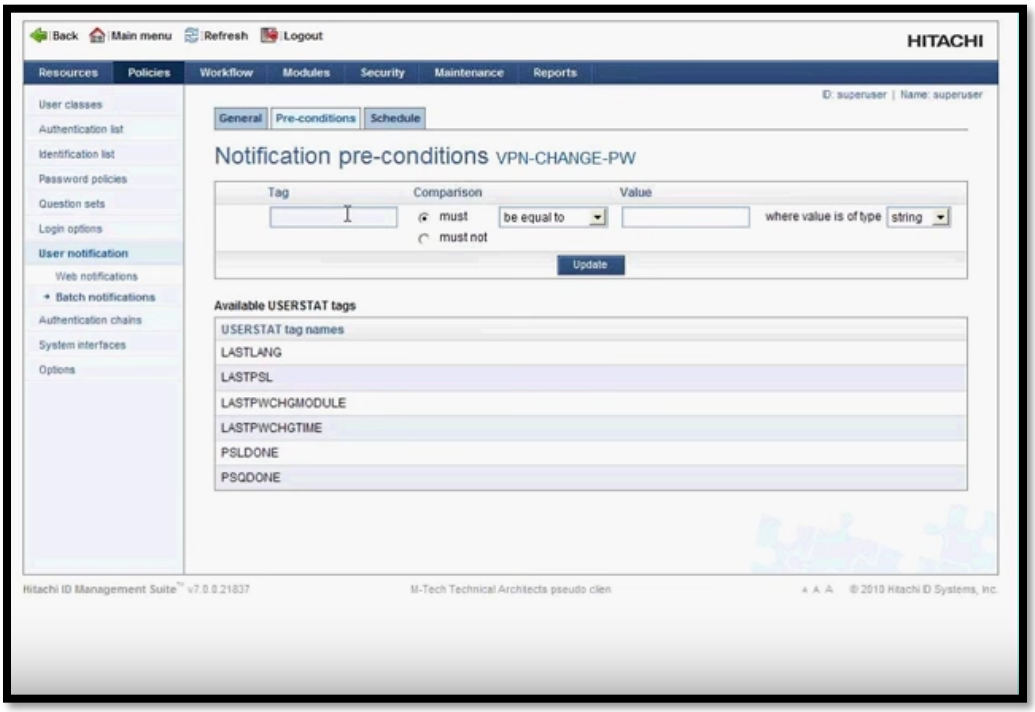


MANAGING THE USER LIFECYCLE ACROSS ON-PREMISES AND CLOUD-HOSTED APPLICATIONS at 11 (2016).

102. On information and belief, the Hitachi '114 Products are available to businesses and individuals throughout the United States.

103. On information and belief, the Hitachi '114 Products are provided to businesses and individuals located in the Eastern District of Texas.

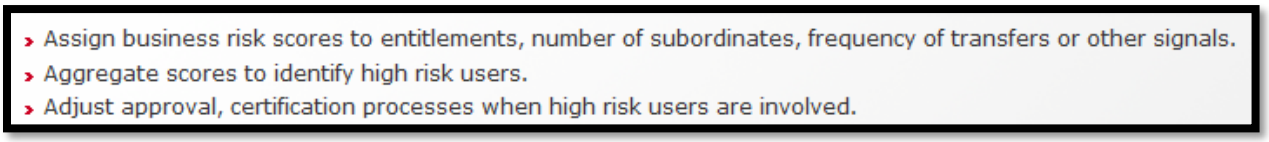
104. On information and belief, the Hitachi '114 Products enable the distribution of protected digital data. The below screenshot from the Hitachi ID Password Manager system shows various automated rules that can be employed to limit access.



HITACHI ID PASSWORD MANAGER 7.0 DEMO at 52:00 (2011), available at: https://www.youtube.com/watch?v=iJG-BszZOg8

105. On information and belief, the Hitachi '114 Products comprise systems and methods wherein the Hitachi '114 Products ascertain terms for providing protected data to a prospective requestor according at least in part to information of unauthorized copying of other protected material previously provided to said prospective requestor.

106. On information and belief, the Hitachi '114 Products comprise systems and methods that provide authorization to allow access or deny access to protected digital data based on ascertained terms. For example, Hitachi ID information describes the use of business risk scores to limit access.



Identity Management and Access Governance Solutions, HITACHI ID WEBSITE (last visited November 2016), available at: https://hitachi-id.com/security/.

107. On information and belief, HID has directly infringed and continues to directly infringe the '114 patent by, among other things, making, using, offering for sale, and/or selling digital content protection technology, including but not limited to the Hitachi '114 Products, which include infringing digital rights management technologies. Such products and/or services include, by way of example and without limitation, the Hitachi ID Identity and Access Management Suite Versions 10.0 and 10.1.

108. By making, using, testing, offering for sale, and/or selling digital rights management and access control products and services, including but not limited to the Hitachi '114 Products, HID has injured MOV Intelligence and is liable to MOV Intelligence for directly infringing one or more claims of the '114 patent, including at least claims 1-3 and 21-23, pursuant to 35 U.S.C. § 271(a).

109. On information and belief, HID also indirectly infringes the '114 patent by actively inducing infringement under 35 USC § 271(b).

110. On information and belief, Hitachi had knowledge of the '114 patent since at least service of the first Complaint in this action or shortly thereafter, and on information and belief, Hitachi knew of the '114 patent and knew of its infringement, including by way of this lawsuit.

111. On information and belief, HID intended to induce patent infringement by third-party customers and users of the Hitachi '114 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. HID specifically intended and was aware that the normal and customary use of the accused products would infringe the '114 patent. HID performed the acts that constitute induced infringement, and would induce actual infringement, with knowledge of the '114 patent and with the knowledge that the induced acts would constitute infringement. For example, HID

provides the Hitachi '114 Products that have the capability of operating in a manner that infringe one or more of the claims of the '114 patent, including at least claims 1-3 and 21-23, and HID further provides documentation and training materials that cause customers and end users of the Hitachi '114 Products to utilize the products in a manner that directly infringe one or more claims of the '114 patent.[14] By providing instruction and training to customers and end-users on how to use the Hitachi '114 Products in a manner that directly infringes one or more claims of the '114 patent, including at least claims 1-3 and 21-23, HID specifically intended to induce infringement of the '114 patent. On information and belief, HID engaged in such inducement to promote the sales of the Hitachi '114 Products, e.g., through user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '114 patent. Accordingly, HID has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '114 patent, knowing that such use constitutes infringement of the '114 patent.

112. A detailed explanation of HID's infringement of the '114 patent by the Hitachi '114 Products was provided to Defendants as Exhibit D of Plaintiff MOV Intelligence's Disclosure of Asserted Claims and Preliminary Infringement Contentions Pursuant to Local Patent Rules 3-1 and 3-2, served on July 12, 2017, and as Exhibit C to Plaintiff MOV Intelligence's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions, served on August 23, 2017.

113. The '114 patent is well-known within the industry as demonstrated by the over 39 citations to the '114 patent family in issued patents and published patent applications assigned to technology companies and academic institutions (*e.g.*, Aigo Research Institute of Image

[14] *See e.g., Hitachi ID Identity and Access Management Suite Architecture*, HITACHI ID WEBSITE (last visited November 2016), *available at*: https://hitachi-id.com/technology/architecture.html; *Hitachi ID Suite 10.0 Features*, HITACHI ID WEBSITE (last visited November 2016), available at: https://hitachi-id.com/products/hitachi-id-identity-and-access-management-suite-10.0-whats-new.html; *Identity Management and Access Governance Solutions*, HITACHI ID WEBSITE (last visited November 2016), available at: https://hitachi-id.com/security/; MANAGING THE USER LIFECYCLE ACROSS ON-PREMISES AND CLOUD-HOSTED APPLICATIONS at 11 (2016).

Computing Co., Ltd. and General Electric Company). Several of Hitachi's competitors have paid considerable licensing fees for their use of the technology claimed by the '114 patent. In an effort to gain an advantage over Hitachi's competitors by utilizing the same licensed technology without paying reasonable royalties, Hitachi infringed the '114 patent in a manner best described as willful, wanton, malicious, in bad faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate.

114. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '114 patent.

115. As a result of HID's infringement of the '114 patent, MOV Intelligence has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Hitachi's infringement, but in no event less than a reasonable royalty for the use made of the invention by Hitachi together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff MOV Intelligence respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff MOV Intelligence that Vantara, or in the alternative, HL has infringed, either literally and/or under the doctrine of equivalents, the '006 patent and the '504 patent;

B. A judgment in favor of Plaintiff MOV Intelligence that HID has infringed, either literally and/or under the doctrine of equivalents, the '114 patent;

C. An award of damages resulting from Defendants' acts of infringement in accordance with 35 U.S.C. § 284;

D. A judgment and order finding that Defendants' infringement was willful, wanton, malicious, bad-faith, deliberate, consciously wrongful, flagrant, or characteristic of a pirate within the meaning of 35 U.S.C. § 284 and awarding to Plaintiff enhanced damages.

E. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Defendant.

F. Any and all other relief to which MOV Intelligence may show itself to be entitled.

JURY TRIAL DEMANDED

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, MOV Intelligence requests a trial by jury of any issues so triable by right.

Dated: November 8, 2017

Respectfully submitted,

/s/ Dorian S. Berger _____
Elizabeth L. DeRieux (TX Bar No. 05770585)
D. Jeffrey Rambin (TX Bar No. 00791478)
CAPSHAW DERIEUX, LLP
114 E. Commerce Ave.
Gladewater, Texas 75647
Telephone: 903-845-5770
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
BERGER & HIPSKIND LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 95047
Telephone: 323-886-3430
Facsimile: 323-978-5508
E-mail: dsb@bergerhipskind.com
E-mail: dph@bergerhipskind.com

Attorneys for Marking Object Virtualization Intelligence, LLC

CERTIFICATE OF SERVICE

I hereby certify that counsel of record who are deemed to have consented to electronic service are being served this November 8, 2017 with a copy of this document via the Court's CM/ECF System per Local Rule CV-5(a)(3). Any other counsel of record will be served by electronic mail, facsimile transmission and/or first class mail on this same date.

/s/ Dorian S. Berger
Dorian S. Berger