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

ST. LUKE TECHNOLOGIES, LLC, ***Plaintiff,*** v. **HEWLETT-PACKARD COMPANY and HP ENTERPRISE SERVICES, LLC,** ***Defendants.***	**Civil Action No._____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff St. Luke Technologies, LLC ("St. Luke" or "Plaintiff"), by and through its attorneys, brings this action and makes the following allegations of patent infringement relating to U.S. Patent Nos. 8,316,237 ("the '237 patent"); 7,181,017 ("the '017 patent"); 7,869,591 ("the '591 patent"); 8,904,181 ("the '181 patent"); 7,587,368 ("the '368 patent"); 8,498,941 ("the '941 patent"); 8,380,630 ("the '630 patent") and 8,600,895 ("the '895 patent") (collectively, the "patents-in-suit"). Defendant Hewlett-Packard Company ("HPC") and HP Enterprise Services, LLC ("HPES") (collectively, "HP" or "Defendant") infringes the patents-in-suit in violation of the patent laws of the United States of America, 35 U.S.C. § 1 *et seq*.

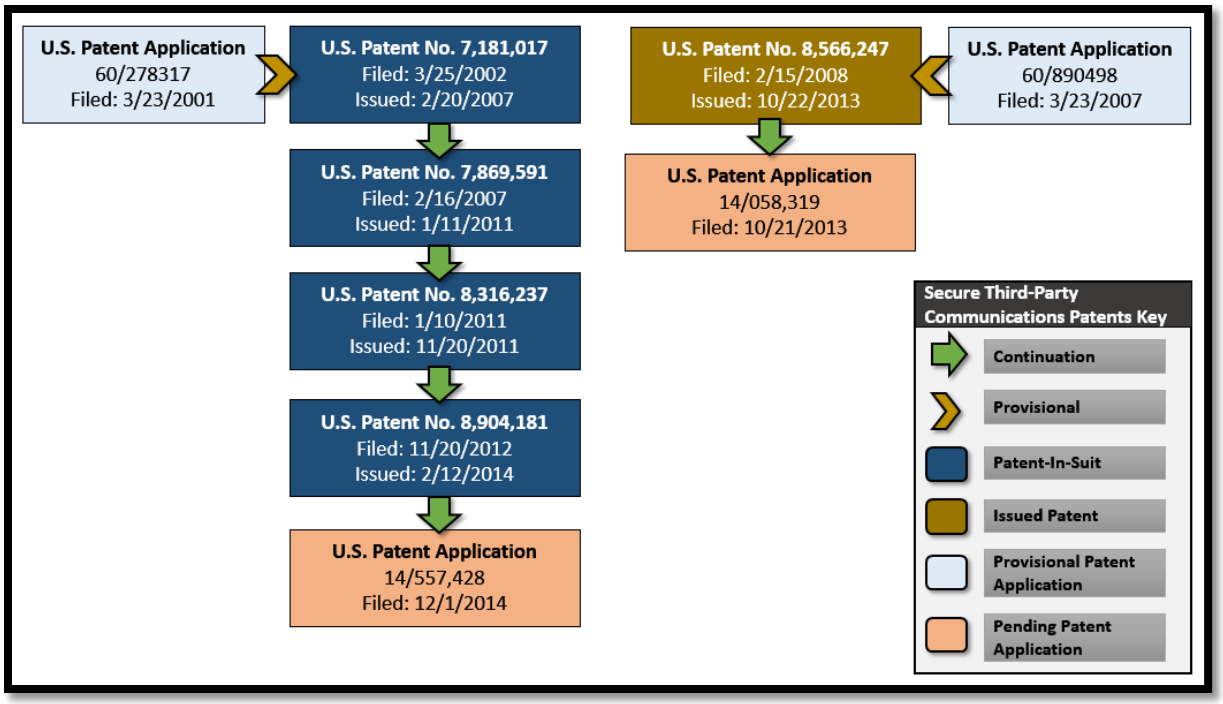
INTRODUCTION

1. In an effort to expand its product base and profit from the sale of infringing cloud computing encryption technologies and information record infrastructure technologies, HP has unlawfully and without permission copied the technologies and inventions of Dr. Robert H. Nagel, David P. Felsher, and Steven M. Hoffberg.

2. Dr. Nagel, Mr. Felsher, and Mr. Hoffberg are the co-inventors of the '237 patent, '017 patent, '591 patent, '181 patent, and U.S. Patent No. 8,566,247 ("the '247 patent")

(collectively, the "Secure Third-Party Communications Patents" or "STPC patents"). The STPC patents have been cited in over 550 United States patents and patent applications as prior art before the United States Patent and Trademark Office. The STPC patents disclose systems and methods for secure communications over a computer network where a third party (intermediary) performs a requisite function with respect to the transaction without requiring the intermediary to be trusted with respect to the private information or cryptographic keys for communicated information. The inventions taught in the STPC patents employ secure cryptographic schemes, which drastically reduce the risk of unauthorized disclosure of encrypted data.

3. The below diagram shows St. Luke's STPC patents, pending STPC patent applications, and the STPC patents HP infringes.[1]



4. Over a decade after Dr. Nagel and his co-inventors conceived of the inventions disclosed in the STPC patents, an HP white paper described systems such as Dr. Nagel, Mr.

[1] St. Luke's STPC patents are in two patent families claiming priority to U.S. Patent Applications 60/278,317 and 60/890,498.

Felsher, and Mr. Hoffberg's secure third party communications system as "breakthrough" and "important."

> ***Data encryption is one of the most important methods*** of protecting data-at-rest in the cloud . . . . HP Atalla Cloud Encryption is the only system available that offers the convenience of cloud-based hosted key management without sacrificing trust. ***Breakthrough split-key encryption technology*** protects keys and guarantees they remain under customer control and are never exposed in storage; and with homomorphic key encryption—even while they are in use.

Choosing an Architecture for Securing Data in The Cloud, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE 2-3 (2015) (emphasis added).

5. HP has cited the patents-in-suit in 15 issued United States patents and published patent applications.[2]

6. HP executives, have repeatedly stated that the use of encryption technologies is central to HP's business, particularly where data is stored in the "Cloud."

> Disruptive technologies that drive business opportunity, such as Cloud computing and consumerization, can strain established processes and potentially introduce undesirable security conditions if they're not approached in compelling ways.

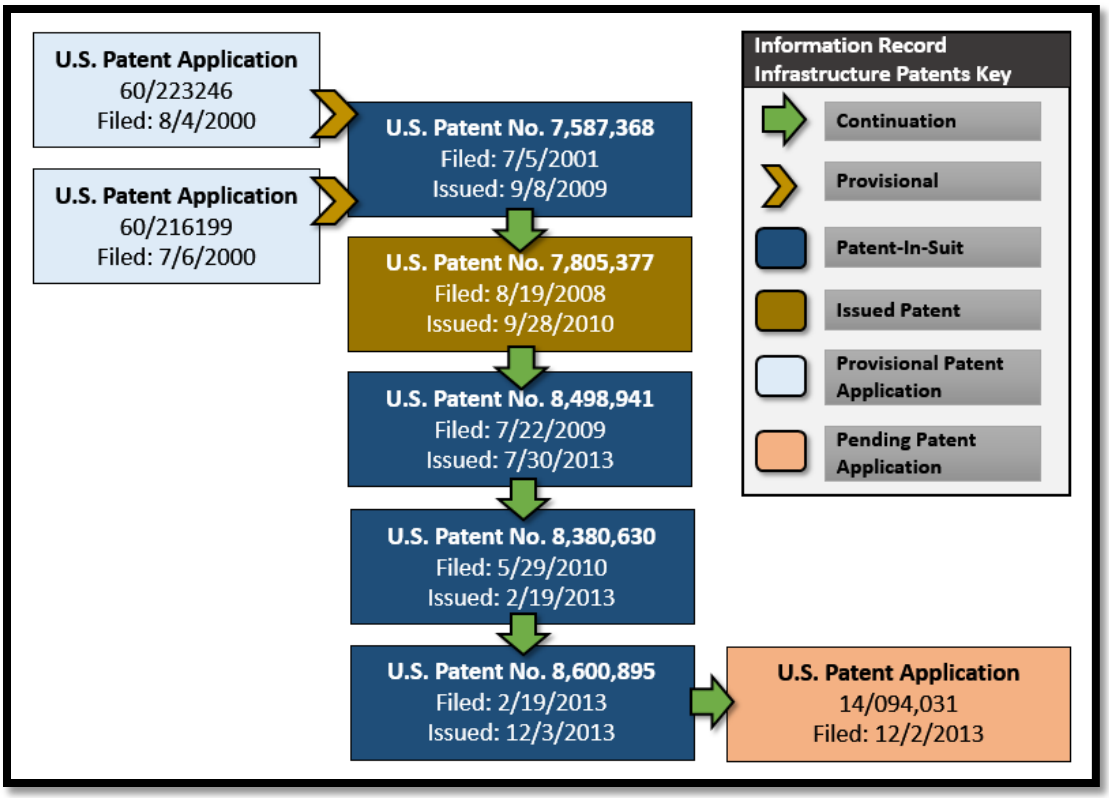
Demonstrating the Value of Security: An Interview with HP's Jim Tiller (Director of HP Security Consulting), HP ENTERPRISE SERVICES BLOG (August 29, 2014).

7. Mr. Felsher is the inventor of the '368 patent, '941 patent, '630 patent, '895 patent, and U.S. Patent No. 7,805,377 patent ("the '377 patent") (collectively, "Information Record Infrastructure Patents" or "IRI patents"). The IRI patents have been cited by over 970 United States patents and patent applications as prior art before the United States Patent and Trademark Office.

8. The IRI patents disclose systems and methods for distributing and granting access to data where data is stored in multiple external computer databases. The IRI patents address the difficult problem of authorizing access to protected information records where authorization will depend on the access privileges of the user.

[2] *See* U.S. Patent Nos. 7,289,993; 7,149,806; 7,992,002; 2014/010,1774; 8,364,729; 8,484,477; 8,601,276; 8,984,298; 8,509,225; 7,610,407; 8,509,225; 8,571,995; WO2008/005,640; 2005/0246,200; 2011/0267,986.

9. The below diagram shows the IRI patent family tree, a pending IRI patent application, and the IRI patents HP is accused of infringing.

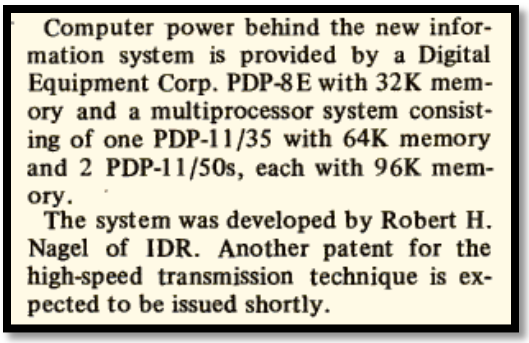


THE INVENTORS' LANDMARK SECURE COMMUNICATION SYSTEMS

10. Mathematician Dr. Robert Nagel, the named inventor of four patents-in-suit, pioneered development of large-scale computer-based data distribution systems. In the 1970s Dr. Nagel developed some of the first computer systems for distributing encrypted data over computer networks. Dr. Nagel is the named inventor of twenty-three United States Patents. Dr. Nagel's patents have been cited thousands of times by various companies, including HP. Later in life, Dr. Nagel founded two publicly traded companies, and served as a representative to the United Nations.

11. In 1975, Dr. Nagel developed a system harnessing burgeoning microprocessor power to broadcast stock prices and related data over coaxial cable and telephone networks. Dr.

Nagel's patented system was the foundation of Reuters's high-speed transmission technologies for distributing real-time market information.



Computer power behind the new information system is provided by a Digital Equipment Corp. PDP-8E with 32K memory and a multiprocessor system consisting of one PDP-11/35 with 64K memory and 2 PDP-11/50s, each with 96K memory.

The system was developed by Robert H. Nagel of IDR. Another patent for the high-speed transmission technique is expected to be issued shortly.

REUTERS GETS NEWS SYSTEM PATENT, COMPUTERWORLD at 36, April 23, 1975 (describing Dr. Nagel's development of one of the first terminals for displaying real-time stock market data).[3]

12. The data distribution system developed by Dr. Nagel in the mid-1970s was commercialized by Reuters and allowed the rapid transmission of market and news information over coaxial cable and telephone lines.[4]

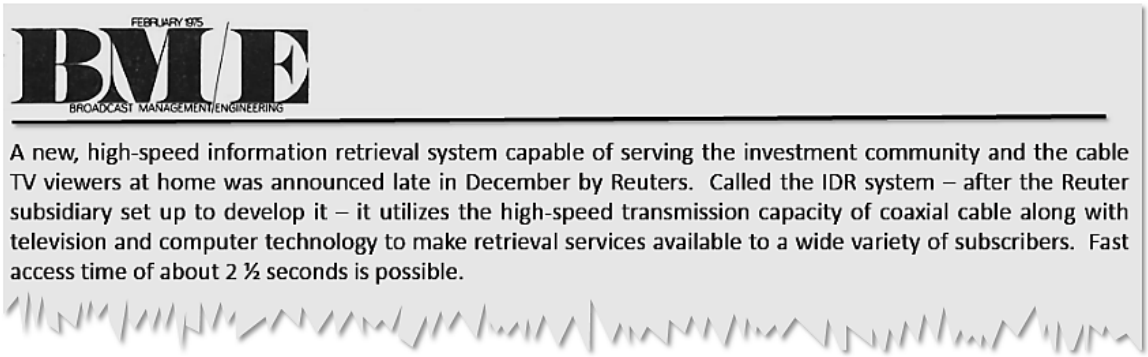
IMAGE OF THE DEC PDP-11/50 SYSTEM, COLUMBIA UNIVERSITY COMPUTING HISTORY ARCHIVE (circa 1976), http://www.columbia.edu/cu/computinghistory/ (showing an installed PDP-11/50 device that was a component in Dr. Nagel's data distribution system).

---

[3] *See* U.S. Patent Nos. 3,875,329, which issued on April 1, 1975. Dr. Nagel's work at IDR, Inc. (a subsidiary of then Reuters Group PLC) lead to the development of U.S. Patent Nos. 3,889,054; 4,042,958; 4,064,494; 4,120,003, 4,135,213; and 4,148,066. These patents have been cited in over 830 patent applications and issued patents of companies including Cisco Technology, Inc., Sony Corporation, Intel Corporation, etc.

[4] REUTERS TECHNICAL DEVELOPMENT CHRONOLOGY 1975-1979, THE BARON, July 13, 2015), http://thebaron.info/archives/technology/reuters-technical-development-chronology-1975-1979.

13. Reuters sold thousands of information systems modeled on Dr. Nagel's patented inventions.[5] Hundreds of companies including IBM, Intel, and Xerox cite Dr. Nagel's groundbreaking inventions described in his patents as relevant prior art in their own patents.[6]



FEBRUARY 1975

BM/E

BROADCAST MANAGEMENT/ENGINEERING

A new, high-speed information retrieval system capable of serving the investment community and the cable TV viewers at home was announced late in December by Reuters. Called the IDR system – after the Reuter subsidiary set up to develop it – it utilizes the high-speed transmission capacity of coaxial cable along with television and computer technology to make retrieval services available to a wide variety of subscribers. Fast access time of about 2 ½ seconds is possible.

REUTERS ANNOUNCES RETRIEVAL SYSTEM FOR CABLE TV SUBSCRIBERS, BROADCAST MANAGEMENT/ENGINEERING MAGAZINE at 9, February 1975.

14. In the 1990s, Dr. Nagel was the Chief Technology Officer of eSecure Docs, Inc., Founder of Digits Corporation, and Executive Vice President and Chief Technology Officer of InfoSafe Systems, Inc.[7] Publications including Fortune Magazine and ComputerWorld

[5] REUTERS TECHNICAL DEVELOPMENT CHRONOLOGY 1975-1979, THE BARON, July 13, 2015), http://thebaron.info/archives/technology/reuters-technical-development-chronology-1975-1979 (More than 10,000 units are eventually produced. It revolutionizes the Monitor product financials and field staffing and provides valuable cash flow for IDR.").

[6] PROCEEDINGS OF THE DIGITAL EQUIPMENT USERS SOCIETY, DIGITAL EQUIPMENT CORPORATION PROCEEDINGS Vol. 3 Issue 1 at 1 (1977) ("Reuters has developed a network to assist stock and commodity brokers and foreign exchange dealers by giving them the latest prices and rate of exchange via terminals in this book."); ANNUAL REVIEW OF INFORMATION SCIENCE AND TECHNOLOGY, AMERICAN SOCIETY OF INFORMATION SCIENCE, AMERICAN DOCUMENTATION INSTITUTE Vol. 12 at 223 (1977) ("Reuters provides the user with a 1.2 Kbps leased connection to the nearest network processor or multiplexor. The Monitor user configuration is a Digital Equipment Corporation PDP 8 with up to three display units."); REUTERS BLENDS CATV & COMPUTER SKILLS IN NEWS RETRIEVAL SYSTEM, DATA PROCESSING DIGEST at 12 (1975) ("Reuters has introduced in New York a high-speed information retrieval system for the investment community. The system was developed by Information Dissemination and Retrieval, Inc. (IDR), a Reuters subsidiary, and uses the high-speed transmission capacity of coaxial cable with television and computer technology.").

[7] In addition to his work in private industry, Dr. Nagel served as a consultant to the Defense Advanced Research Projects Agency ("DARPA"), responsible for the development of emerging technologies used by the U.S. Department of Defense. Dr. Nagel was a designer of the Navy's Tactical Air Navigation System ("TACAN") and assisted in the development of the nuclear reactor that powers the Navy's Seawolf class of nuclear submarines. Dr. Nagel was also the developer of the Hot Well Liquid Level Control system that is a part of the control system of the nuclear power plant aboard the Seawolf, Defender and other submarines.

described Dr. Nagel as a "noted computer scientist" for his groundbreaking work[8]—work that led to the inventions disclosed in the patents-in-suit.

> The technology Nagel designed at InfoSafe Systems, Inc., won the Seybold Award for Excellence as the "most innovative product of the year." His work in high technology received major press coverage in such publications as Fortune, Forbes, and Business Week. He testified before Congress on the capabilities of a system he designed for NASDAQ.

Aliye Pekin Celik, OUR COMMON HUMANITY IN THE INFORMATION AGE: PRINCIPLES AND VALUES FOR DEVELOPMENT at 191 (2007).

15. Following his development of groundbreaking electronic data distribution systems for Reuters, Dr. Nagel used his insights to develop the secure communications technologies that are used today by HP and many of the world's largest corporations without attribution or compensation.

16. Dr. Nagel foresaw the need for enabling secure communications between two parties wherein an intermediary performs a requisite function with respect to the transaction without requiring the intermediary to be trusted with respect to the private information or cryptographic keys for communicated information.

17. Dr. Nagel's interest in developing secure systems for the provision of highly secure data was driven in part by his experience being totally blind.[9] Dr. Nagel recognized that the growing adoption of the Internet and increased computational power presented unique challenges to the security of medical records. Dr. Nagel also had the insight that the challenges presented in controlling access to secure medical records could be applied outside the context of

---

[8] *See* Rick Tetzeli, et al., *Fortune Checks Out 25 Cool Companies For Products, Ideas, And Investments*, FORTUNE MAGAZINE, July 11, 1994.

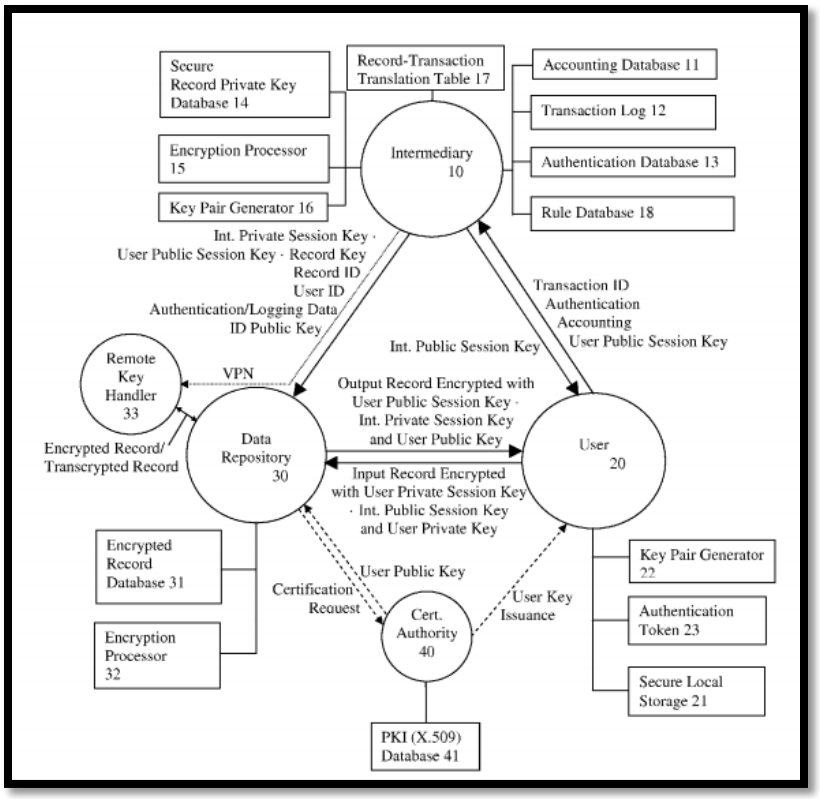
[9] Dr. Nagel served as a representative to the United Nations Committee that authored the International Convention on the Protection of the Rights of Dignity of Persons with Disabilities *See* Jan Jekielek, *Human Rights Panel Explores Implementation of Rights and Global Well-Being*, Epoch Times, December 3, 2010, http://www.cccun.net/cccun-12-2-10-eventepochtim.pdf ("Nagel, who is blind himself. He expounded on the remarkable accomplishment that is the Convention on the Rights of Persons with Disabilities, the 21st century's first U.N. human rights convention.").

medical records, with wide applicability to the security of data on networks where an intermediary could have access to secure information.

18. The rise of cloud computing (the delivery of on-demand computing resources over a distributed network), has made Dr. Nagel and his co-inventors' insights uniquely valuable. Medical records, financial information, email messages, and other forms of electronic data are now placed on remote servers and accessed via a network by a diverse variety of users, under a diverse variety of circumstances.

19. The inventions disclosed in the STPC patents address shortcomings in systems available at the time of the patents' conception—for example, the need for users in particular contexts, to access and/or modify data stored at or by an intermediary without allowing the intermediary to access an unencrypted version of the data.

20. Prior art systems such as the "Micali Fair Encryption scheme do[] not . . . allow communications of a secret in which only one party gains access to the content, and in which the third party or parties and one principal operate only on encrypted or secret information." '237 patent, col. 2:40-44.



‘237 Patent Fig. 1.

21. Dr. Nagel worked with Steven Hoffberg and David P. Felsher to develop the systems and methods disclosed in the STPC patents. The inventions taught in these patents relate to the secure transmission of data—for example, wherein an intermediary performs a requisite function with respect to a secure data transmission without requiring the intermediary to be trusted with the private, secure contents of the transmission and/or without requiring the intermediary to have access to the cryptographic keys required to access the protected information. The STPC patented systems and methods employ secure cryptographic schemes, which reduce the risks and liability of unauthorized disclosure of private information as it travels across a network.

22. Mr. Hoffberg holds a Master of Science degree from the Massachusetts Institute of Technology and an advanced degree in electrical engineering from Rensselaer Polytechnic Institute. Mr. Hoffberg is a named inventor on sixty-seven patents in the fields of telematics, wireless ad hoc networking, image and audio signal processing, and cryptography. Mr. Hoffberg

also spent three years in the University of Connecticut Medical School Medical Doctorate Program.

23. Mr. Felsher is an appellate attorney, health care activist, and inventor. After graduating from MIT with a Bachelor of Science Degree in Chemistry, Mr. Felsher went on to earn an MBA from the Wharton School of Business of the University of Pennsylvania and a J.D. from Fordham Law School.[10] Mr. Felsher has served as counsel to the Association of American Physicians and Surgeons, Inc.

24. The STPC patents have been cited in over 550 United States patents and published patent applications as prior art before the United States Patent and Trademark Office.[11] Companies whose patents cite the Secure Third-Party Communication Patents include:

- Microsoft Corporation
- Nokia Corporation
- Apple, Inc.
- International Business Machines Corporation
- Massachusetts Institute Of Technology
- Ncr Corporation
- Netapp, Inc.
- Adobe Systems Incorporated
- American Express Travel Related Services Company, Inc.
- AT&T Intellectual Property LLP
- Canon Kabushiki Kaisha
- Hytrust, Inc.
- Cisco Technology, Inc.
- Intuit Inc.
- Cloudera, Inc.
- Novell, Inc.
- Google Inc.
- Teradata Us, Inc.
- Mitsubishi Electric Corporation
- Texas Instruments Inc.
- Unitedhealth Group Incorporated
- Fujitsu Limited
- Hewlett-Packard Development Company, L.P.
- Verizon Patent and Licensing Inc.
- Visa U.S.A. Inc.
- Western Digital Technologies, Inc.

[10] During his legal career, Mr. Felsher has been counsel of record on seventeen briefs to the United States Supreme Court.

[11] The 550 forward citations to the Secure Third-Party Communication Patents do not include patent applications that were abandoned prior to publication in the face of the Secure Third-Party Communication Patents.

- Xerox Corporation
- Yahoo! Inc.
- Koninklijke Philips Electronics, N.V.
- Zynga Inc.
- Square, Inc.
- Sprint Communications Company L.P.
- Sony Corporation
- Siemens Aktiengesellschaft
- Sharp Laboratories of America, Inc.
- Sap AG
- EMC Corporation
- Samsung Electronics Co., Ltd.
- Ricoh Co., Ltd.
- Red Hat, Inc.
- Panasonic Corporation
- Broadcom Corporation
- Oracle International Corporation

The inventions taught in the STPC patents relate to the encryption of data passed through an intermediary and have been recognized by HP as crucial. "We are rapidly moving toward a cloud majority world, but the problem of full trust remains unresolved. In applying encryption to protect sensitive data, the most crucial secret is the encryption key itself."[12]

25. The adoption of secure encryption technologies is critical to the success of HP's products and services.

> Our long-term strategy is focused on leveraging our portfolio of hardware, software and services as we adapt to a changing and hybrid model of IT delivery and consumption driven by ***the growing adoption of cloud computing*** and increased demand for integrated IT solutions. To successfully execute on this strategy, we need to continue evolving our focus towards the delivery of integrated IT solutions for our customers and to c***ontinue to invest and expand into cloud computing, security***, big data and mobility.

HEWLETT-PACKARD COMPANY FORM 10-K at 19-20 (2014) (emphasis added).

26. The IRI patents have been cited by over 970 United States patents and patent applications as prior art before the United States Patent and Trademark Office.[13] Companies whose patents cite the IRI patents include:

- Bank Of America Corporation
- Siemens Medical Solutions Health Services Corporation
- AthenaHealth, Inc.

[12] *HP Atalla Cloud Encryption: Securing Data in the Cloud* at 1, HP DATASHEET (2014).

[13] The 970 forward citations to the IRI Patents and their related patent applications do not include patent applications that were abandoned prior to publication in the face of the IRI Patents.

- Robert Bosch Gmbh
- Thompson Reuters (Healthcare) Inc.
- Northrop Grumman Information Technology, Inc.
- McKesson Corporation
- Lockheed Martin Corporation
- Sandisk Technologies Inc.
- Intel Corporation
- Greenway Medical Technologies, Inc.
- Medtronic, Inc.
- Sybase, Inc.
- General Electric Company
- Epic Systems Corporation
- Allscripts Software, Llc
- Ebay, Inc.
- 3Com Corporation
- Oracle International Corporation
- Intuit Inc.
- Gemalto Sa
- Adobe Systems Incorporated
- Koninklijke Philips Electronics N.V.
- Electronic Data Systems Corporation
- American Express Travel Related Services Company, Inc.
- Google Inc.
- Apple, Inc.
- Mcafee, Inc.
- Hewlett-Packard Development Company L.P.
- EMC Corporation
- Blackboard Inc.
- AT&T Intellectual Property LLP
- Cerner Innovation, Inc.
- Cisco Technology, Inc.
- Citrix System, Inc.
- International Business Machines Corporation

THE PARTIES

27. Tyler, Texas-based St. Luke is committed to advancing the current state of innovation in the field of data encryption technologies for secure communications over a distributed network. In addition to the ongoing efforts of Messrs. Felsher and Hoffberg, St. Luke employs a resident of Tyler, Texas as a Technology Analyst. St. Luke is a Texas limited liability company with its principal place of business at 719 West Front Street, Suite 247, Tyler, Texas 75710.

28. St. Luke is a small, Texas-based company. St. Luke depends on patent protection to effectively license its innovative technologies and build its business. Like Defendant HP, St. Luke relies on its intellectual property. HP's Chairperson and Chief Executive Officer, Meg Whitman, explained the importance of protecting HP's intellectual property:

> We will do the best job we can to protect that intellectual property. . . . But obviously, you've got to be careful of your I.P. assets and it's a challenge. And not only in China, it is a challenge in a lot of other countries, as well.

CNBC's David Faber Speaks with Hewlett-Packard Chairman & CEO Meg Whitman, CNBC: SQUAWK ON THE STREET (May, 22, 2015), http://video.cnbc.com/gallery/?video=3000382233

29. HP has also attributed its success to the patent laws of the United States and ensuring that entities do not infringe HP's patents.

> ***We rely upon patent, copyright, trademark and trade secret laws in the United States***, similar laws in other countries, and agreements with our employees, customers, suppliers and other parties, to establish and maintain intellectual property rights in the products and services we sell, provide or otherwise use in our operations.

HEWLETT-PACKARD COMPANY FORM 10-K at 19-20 (2014) (emphasis added).

30. On information and belief, HP has asserted its patents in federal courts, including the Eastern District of Texas.[14]

[14] *See e.g., Hewlett-Packard Co. v. Ninestar Image Tech Limited et al.*, Case No. 14-cv-04473 (N.D. Cal. Filed Oct. 6, 2014); *Hewlett-Packard Co. v. ServiceNow, Inc.*, Case No. 14-cv-00570 (N.D. Cal. Filed Feb. 6, 2014); *Hewlett-Packard Co. et al v. Microjet Tech. Co, Ltd. et al.*, Case No. 10-cv-02175 (N.D. Cal. Filed May 20, 2010); *Hewlett Packard Co. v. Zhuhai Gree Magneto-Electric Co. Ltd. et al.*, Case No. 09-cv-06929 (C.D. Cal. Filed Sept. 23, 2009); *Hewlett-Packard Co. v. Acer, Inc. et al.*, Case No. 07-cv-00150 (E.D. Tex. Filed April 19, 2007); *Hewlett-Packard Co. v. Acer, Inc. et al.*, Case No. 07-cv-00103 (E.D. Tex. Filed Mar. 27, 2007).

31. On information and belief, Defendant HPC is a Delaware corporation, with its North American headquarters at 11445 Compaq Center West Drive, Houston, Texas 77070, and a worldwide headquarters at 3000 Hanover Street, Palo Alto, California 94304. On information and belief, HPC can be served through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, Texas 75201.

32. On information and belief, HPES is a Delaware limited liability company having a principal place of business at 5400 Legacy Drive, Plano, Texas 75024. On information and belief, HPES can be served through its registered agent, CT Corporation System, 1999 Bryan St., Ste. 900, Dallas, Texas 75201.

33. According to HP's website, infringing products are offered for sale and sold throughout the United States and Canada, including in this District, through various channels. HP offers its infringing products through its distribution channel, which includes numerous distribution points in Texas. Further, HP advertises its infringing products throughout the Eastern District of Texas.

34. On information and belief, HP has offices in Texas where it sells, develops, and/or markets its products including:

- HP developers, which are integral to the accused products' infringing capabilities.
- HP employs thousands of employees in the Eastern District of Texas.[15]
- HPES is headquartered in Plano, Texas.

35. On information and belief, HP has acquired companies relevant to the accused products, including Electronic Data Systems ("EDS") which was based in Plano, Texas.[16]

[15] *See Abstrax, Inc. v. Hewlett-Packard Co.*, Case No. 14-cv-158 Dkt. No. 86 (E.D. Tex. Nov. 11, 2014) (finding significant ties to the district including 5000 HP employees located in the district at HP's Plano, Texas facility); *Mirror Worlds Techs., LLC v. Dell Inc., et al.*, Case No. 13-cv-00941 Dkt. No. 179 (E.D. Tex. Sept. 29, 2014) (denying HP's motion to transfer venue and concluding that HP [along with other defendants] collectively employ thousands of people in or near the Eastern District of Texas.).

[16] EDS is now the core of HPES. *See EDS, an HP Company, Becoming HP Enterprise Services*, HP PRESS RELEASE (September 23, 2009) ("The name change marks the next major step in a year-long integration of EDS into HP and emphasizes the growing global role of enterprise technology services in HP's portfolio.").

JURISDICTION AND VENUE

36. 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).

37. Upon information and belief, this Court has personal jurisdiction over Defendants HPC and HPES in this action because HPC and HPES have committed acts within the Eastern District of Texas giving rise to this action and have established minimum contacts with this forum such that the exercise of jurisdiction over HPC and HPES would not offend traditional notions of fair play and substantial justice. Defendants HPC and HPES, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), have committed and continue to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the asserted patents. Moreover, both HCP and HPES are registered to do business in the state of Texas, and each has appointed CT Corporation System, 1999 Bryan St., Suite 900, Dallas, TX, 75201-3136, as its agent for service of process. This Court also has personal jurisdiction over Defendants HPC and HPES because HPC and HPES each have a principal place of business in Texas.

38. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Each of Defendants HOPC and HPES is registered to do business in Texas, and upon information and belief, has transacted business in the Eastern District of Texas and has committed acts of direct and indirect infringement in the Eastern District of Texas. In addition, HPC and HPES has a principal place of business in Texas.

TECHNOLOGY BACKGROUND

39. Advances in computational power and the explosive growth of the Internet have led to the development of secure encryption systems and information record management systems that enable secure communications between two or more computers on a network where the data that is sent and/or processed by an intermediary without access to the plaintext data.

- ***The STPC patents*** teach specific computer based encryption systems, including systems that use composite key asymmetric cryptographic algorithms to avoid substantially revealing plaintext data during intermediate processing.
- ***The IRI patents*** teach specific computer based systems and methods, including systems for electronically structuring and controlling access to protected data in a plurality of external databases.

A. Secure Third Party Communications Patents

40. HP prizes systems that provide secure third party communications through an intermediary.

> As HP can attest, this market is becoming more sophisticated and our customers and partners must contend with this bad-guy ecosystem on a daily basis. Additionally, cloud and other mobility-driven technologies are creating countless new gateways and access points that must be evaluated to protect what lives inside the network

Rob Roy, *Public Sector Chief Technology Officer HP Enterprise Security Products*, *Encryption: Even the Playing Field By Protecting What Matters*, HP SECURITY PRODUCTS BLOG (August 12, 2015).

41. In a 2015 presentation to financial analysts, Meg Whitman (Chairperson and Chief Executive Officer of HP), tied the financial success of HP to following four principals: Transform, Protect, Enable and Empower. "Protect" refers to HP integrating strong data protection functionality into its products and services.[17]

[17] See also *Hewlett-Packard "Playing to Win" the Secret to HP's Turnaround* at 2, UBS "STRAT TALK" TRANSCRIPT, (July 14, 2014) (Mohamad Ali, Chief Strategy Officer of Hewlett Packard).

Meg Whitman, *Chief Executive Officer Overview Presentation* at 14, HEWLETT-PACKARD SECURITIES ANALYST MEETING (September 15, 2015).

42. Security for data stored on a computer network has been described to financial analysts as key to HP's success. Mohamad Ali, Chief Strategy Office of Hewlett Packard described 'security' as the underpinning for HP's turnaround.

> We're in the early stages of this newest wave compromised of four key things: cloud, mobile, Big Data, and social with security a crucial underpinning. As with most major shifts, these new dynamics really put significant pressure on existing IT systems for both HP and our customers. CIOs are under this continuous pressure to simplify the architecture, to innovate at rapid speeds, and to manage risk.

Hewlett-Packard "Playing to Win" the Secret to HP's Turnaround at 8, UBS STRAT TALK TRANSCRIPT (July 14, 2014).

43. HP's competitors such as Microsoft, Apple, and Oracle have confirmed the importance and value of encryption systems that protect data in the Cloud. Brendon Lynch, Chief Privacy Officer at Microsoft described the importance that Microsoft places on secure encryption in the cloud:

> We share the same concerns as our customers do around government surveillance. We know that customers will not use technology that they do not trust that is what people should know about our [Microsoft's] approach to this . . . we're implementing strong encryption right throughout our services to ensure that governments can only access data by lawful means."

Brendon Lynch, *Microsoft Privacy and Compliance in the Cloud*, TRUSTWORTHY COMPUTING - VIDEO TRANSCRIPT, January 9, 2015, https://www.youtube.com/watch?v=q5rwwQBTJxo.

44. Tim Cook, Apple's Chief Executive Officer, has repeatedly stated that the use of encryption technologies is central to Apple's business.

> Tim Cook: We've also communicated and demonstrated our commitment to respecting and protecting users' privacy with strong encryption and strict policies that govern how our data is handled.

APPLE Q4 2014 EARNING CALL TRANSCRIPT, October 20, 2014, http://seekingalpha.com/article/2576865-apples-aapl-ceo-tim-cook-on-q4-2014-results-earnings-call-transcript.

45. Vipin Samar, Vice President of database security product development at Oracle states in a 2014 press release that, "As regulations worldwide increasingly call for more data to be encrypted, organizations need a centralized solution to securely manage all the encryption keys and credential files in their data centers." The press release continued by pointing out the importance of secure encryption in the cloud.

> and backup mechanisms. As organizations increasingly encrypt data at rest and on the network, securely managing all the encryption keys and credential files in the data center has become a major challenge.
>
> At the same time, organizations also need to comply with stringent regulatory requirements for managing keys and certificates. Many global regulations and industry standards call for audits demonstrating that keys are routinely rotated, properly destroyed, and accessed solely by authorized entities.

ORACLE CUSTOMERS SECURE CRITICAL ENCRYPTION KEYS WITH ORACLE KEY VAULT, ORACLE PRESS RELEASE, August 7, 2014.

46. Although secure third party encryption systems that protect access to data at an intermediary are offered by major corporations today, at the time the inventions disclosed in the STPC patents were conceived, no such systems existed.

47. The claims in the STPC patents describe a solution that is unquestionably rooted in computer technology to overcome a problem specific to and characteristic of complex computer networks. Professor of Computer Science at Columbia University, Steven M. Bellovin[18] described in a 1996 academic article, contemporaneous to the development of the

[18] At the time Professor Bellovin authored the above referenced article he was a Fellow at AT&T Labs Research.

patents-in-suit (and cited on the face of the STPC patents) that the development of modern cryptography was a reaction to the rise of the Internet as a mass medium and concerns unique to the exchange of information over the Internet.

> In early 1994, CERT announced[1] that widespread password monitoring was occuring on the Internet. In 1995, Joncheray published a paper explaining how an eavesdropper could hijack a TCP connection [Jon95]. In mid-1998, there is still very little use of cryptography. Finally, though, there is some reason for optimism.
>
> A number of factors have combined to change people's behavior. First, of course, there is the rise of the Internet as a mass medium, and along with it the rise of Internet commerce. Consider the following quote from a popular Web site:

Steven M. Bellovin, *Cryptography and the Internet*, AT&T LABS-RESEARCH, Aug. 1998, Florham Park, New Jersey.

48. Although encryption, in some form, has been an objective of individuals (and governments) for many years, the STPC patents are directed at solving problems that are unique to the realm of computers and specifically network cloud computing.

49. The specific technologies disclosed and claimed in the STPC patents are discussed in detail below. However, the history of cryptography provides context for the inventions disclosed in the STPC patents and confirms that the patented inventions are limited to specific computer systems and methods addressing issues specific to modern computer networks.

50. ***Pre-Mechanical Encryption***. The origin of cryptography has been around since the reign of Pharos; however, the problems that "pre-silicon" societies faced were markedly different than those the patent-in-suit was directed at solving and the requirements of cryptography reflect that difference. In 1900 BC, Egyptian scribes developed a rudimentary form of cryptography that allowed the passing of messages written on papyrus. The key to unlocking the meaning of non-standard hieroglyphs (the encrypted message or cipher) was located in an inscription on the same document. Thus, a recipient of a message could decipher the meaning of the encoded message using the key transmitted with the message. This early

form of encryption was susceptible to frequency analysis, a method utilizing the frequency that certain letters or symbols would be used.[19]

Alexander Stanoyevitch, INTRODUCTION TO CRYPTOGRAPHY WITH MATHEMATICAL FOUNDATIONS AND COMPUTER IMPLEMENTATIONS PRESS (2002).

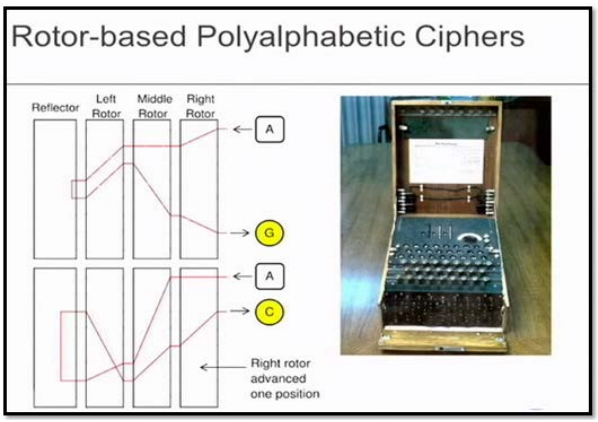
51. Over the following four millennia, the advance of cryptography was limited. In the mid-1400s, Leon Battista Alberti invented an encryption system using a mechanical device with sliding disks that allowed for various methods of substitution.[20] This is the base concept of a polyalphabetic cipher, which is an encryption method that switches through several substitution ciphers throughout encryption. Polyalphabetic substitution by rotating the discs to change the encryption logic limited the use of frequency analysis to crack the cipher. However, polyalphabetic substitution was susceptible to plain text attack that would try various permutations of the code.

52. ***Encryption in the Mechanical Age***. In the 1920s, electro-mechanical devices were developed that used electrical signals to perform rudimentary calculations that would encrypt messages. The Enigma machine developed by the German government at the end of

[19] NIGEL SMART, CRYPTOGRAPHY: AN INTRODUCTION 3RD EDITION 40 (2004) ([U]nderlying statistics of the language could be used to break the cipher. For example it was easy to determine which ciphertext letter corresponded to the plaintext letter *E*.").

[20] DAVID KAHN, THE CODE BREAKERS: THE STORY OF SECRET WRITING 125 (1967) (David Kahn calls Alberti "the father of western cryptography" based on his development of a device that had two copper disks that fit together. "Each one of them had the alphabet inscribed on it. After every few words, the disks were rotated to change the encryption logic, thereby limiting the use of frequency analysis to crack the cipher.")

World War I used mechanical devices to encrypt and decrypt messages. Germany's Enigma device used a set of codes that, when programed into a device, would generate an encrypted message. Ciphers generated by the Enigma could thus be decrypted if one had both possession of an Enigma device and the "crib" or the symmetric key that was used to program the device.[21] Alan Turing (among others) wanted a technique to break Enigma that did not rely on the key, which could (and frequently did) change.[22] Turing developed several ways of using Bayesian inference coupled with "the Bombe," an electromechanical device that could detect the setting for the Enigma.



Steve Weis, THEORY AND PRACTICE OF CRYPTOGRAPHY 9:23 (November 2007) (image of the Enigma machine).

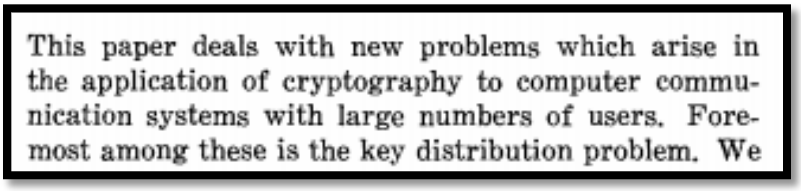
53. ***The Development of Public Key Encryption***. Prior to 1976 (roughly three decades before the patents-in-suit issued), the only method of encryption was use of a symmetric key. Egyptian Ciphers, Polyalphabetic Encryption, and the Enigma Machine relied on the sender

[21] DAVID KAHN, , SEIZING THE ENIGMA: THE RACE TO BREAK THE GERMAN U-BOAT CODES, 1939-1943 (1991) (In 1941 the British were able to decrypt ciphers generated by the enigma machine by discovering that portions of weather reports (Short Weather Codes) transmitted by German Warships were the symmetric key. However, in the fall of 1941 the German cryptographers stopped using short Weather Codes as symmetric keys. Subsequently, Germany out of abundance of caution changed the configuration of the enigma machines.).

[22] DAVID LEAVITT, THE MAN WHO KNEW TOO MUCH: ALAN TURING AND THE INVENTION OF THE COMPUTER (2006) (Turing settled on a known plaintext attack, using what was known at the time as a "crib." A crib was a piece of plaintext that was suspected to lie in the given piece of cipher text. The methodology of this technique was to form a given piece of cipher text and a suspected piece of corresponding plaintext to first deduce a so-called "menu." A menu is simply a graph, which represents the various relationships between cipher text and plaintext letters. Then the menu was used to program an electrical device called a Bombe.).

and receiver sharing the same key (a symmetric key). The advent of computer networks and the increasing computational power of computers spurred the invention of a cryptographic system specifically tailored toward encrypting and decrypting electronic messages communicated using a computer.

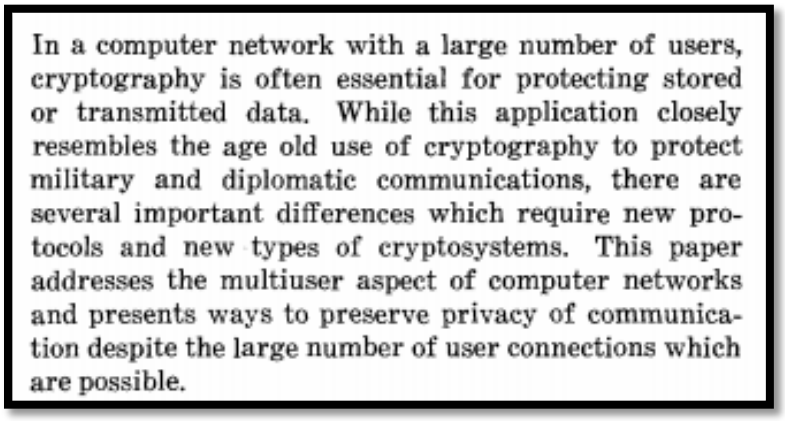
54. In a 1976 paper, cited on the face of the STPC patents, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* (frequently, and more generally, called *asymmetric key*) cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key. Systems that utilize *public key* encryption were developed specifically to address problems unique to computer networking. Public key encryption at the time of the invention of the STPC patent technologies was not a long-held view, nor a technology that simply amounted to taking something and "doing it on a computer." The introduction to Diffie and Hellman's paper makes clear that public key systems were specific to computer networking.


This paper deals with new problems which arise in the application of cryptography to computer communication systems with large numbers of users. Foremost among these is the key distribution problem. We

Diffie, et al, in *Multiuser Cryptographic Techniques,* AFIPS--CONFERENCE PROCEEDINGS, Vol. 45 at 109 (1976).

55. A public key system contains two keys (numbers) so that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair. Public key encryption offered a novel mechanism for allowing two parties to share data over a network.

56. The development of Diffie and Hellman's first public key system was directly motivated by the need to protect stored or transmitted data on a modern computer network.



In a computer network with a large number of users, cryptography is often essential for protecting stored or transmitted data. While this application closely resembles the age old use of cryptography to protect military and diplomatic communications, there are several important differences which require new protocols and new types of cryptosystems. This paper addresses the multiuser aspect of computer networks and presents ways to preserve privacy of communication despite the large number of user connections which are possible.

Id.

57. The Diffie-Hellman public key system illustrates the limitations present in systems for encrypting and decrypting information over a computer network contemporaneous to the STPC patents. The Diffie-Hellman system lacked the ability to enable the exchange of data between two parties through an intermediary where the intermediary would not have the ability to substantially decrypt the data. A 2005 paper (cited on the face of the STPC patents) described the limitations of the Diffie-Hellman system when conducting secure third party communications. The paper also described a problem that the STPC patents solve as one that had only recently been addressed:

> It was only recently that the problem has been formally addressed in the three-party model, where the server is considered to be a trusted third party (TTP). This is the same scenario used in the popular 3-party Kerberos authentication system. The main advantage of these systems is that users are only required to remember a single password, the one they share with a trusted server, while still being able to establish secure sessions with many users. ***The main drawback is the need of the trusted server during the establishment of these secure sessions.***

Michel Abdalla and David Pointcheval, *Interactive Diffie-Hellman Assumptions With Applications To Password-Based Authentication*, in PROCEEDINGS OF THE 9TH INTERNATIONAL CONFERENCE ON FINANCIAL CRYPTOGRAPHY AND DATA SECURITY (2005) (emphasis added).

58. Another early encryption system developed for communications over a computer network is a method of public-key encryption developed by Ron Rivest, Adi Shamir, and Leonard M. Adleman, now generally referred to as "RSA." RSA is based on the use of two extremely large prime numbers which fulfill the criteria for a "trap-door, one-way permutation." Such a permutation function enables the sender to encrypt the message using a non-secret

encryption key, but does not permit an eavesdropper to decrypt the message through crypto-analytic techniques within an acceptable period of time. This is because, for a composite number composed of the product of two very large prime numbers, the computational time necessary to factor this composite number is unacceptably long. A brute force attack requires a sequence of putative keys to be tested to determine which, if any, is appropriate. A brute force attack requires a very large number of iterations. The number of iterations increases exponentially with the key bit size, while the normal decryption generally suffers only an arithmetic-type increase in computational complexity.

59. Like the Diffie-Hellman system, RSA was developed specifically to address problems with sending and receiving encrypted information over a computer network. The original RSA patent (cited on the face of the STPC patents) describes the use of public key encryption as directed toward a computer network.

> With the development of computer technology, the transfer of information in digital form has rapidly increased. There are many applications, including electronic mail systems, bank systems and data processing systems, where the transferred information must pass over communications channels which may be monitored by electronic eavesdroppers.

U.S. Patent No. 4,405,829, col. 1:14-20.

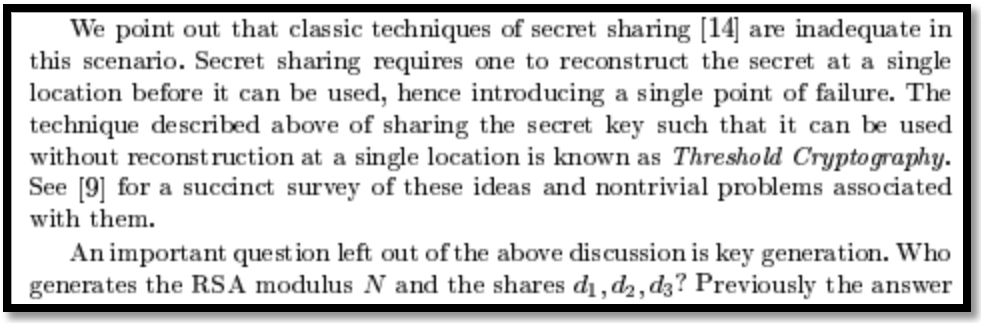
60. Academic articles from creators of the RSA system make clear that the use of public key encryption is specific to problems unique to computer networks.

> [W]e present a sketch of how a computer system might be modified to solve the problem of performing operations on encrypted data securely. . . All sensitive data in main memory, in the data bank files, in the ordinary register set, and on the communications channel will be encrypted. During operation, a load/store instruction between main memory and the secure register set will automatically cause the appropriate decryption/encryption operations to be performed.

Ronald L. Rivest, Leonard Adleman, and Michael L. Dertouzos, *On Data Banks and Privacy Homomorphisms*, IN ON DATA BANKS AND PRIVACY HOMOMORPHISMS 169 (1978).

61. The RSA system illustrates limitations in encryption technologies that preceded the STPC patents. RSA provided a mechanism for exchanging data between two parties but did not disclose the use of an untrusted intermediary when data was exchanged between two parties. A 1998 article contemporaneous to the development of the STPC patents (and cited on the face

of the STPC patents) describes this as a limitation in the RSA system and other systems known at the time.



We point out that classic techniques of secret sharing [14] are inadequate in this scenario. Secret sharing requires one to reconstruct the secret at a single location before it can be used, hence introducing a single point of failure. The technique described above of sharing the secret key such that it can be used without reconstruction at a single location is known as *Threshold Cryptography*. See [9] for a succinct survey of these ideas and nontrivial problems associated with them.

An important question left out of the above discussion is key generation. Who generates the RSA modulus N and the shares d_1, d_2, d_3? Previously the answer

D. Boneh, J. Horwitz, *Generating A Product Of Three Primes With An Unknown Factorization*, in PROC. OF THE THIRD ALGORITHMIC NUMBER THEORY SYMPOSIUM (ANTS), 237 (1998).

62. Silvio Micali's patents (U.S. Pat. Nos. 6,026,163 and 5,315,658; cited on the face of the STPC patents) describe a split key, or so-called "fair" cryptosystem, designed to allow a secret key to be distributed to a plurality of trusted entities, such that the encrypted message is protected unless the key portions are divulged by all of the trusted entities. Thus, a secret key may be recovered through cooperation of a plurality of parties. The Micali system provides that the decryption key is split between a number (n) of trusted entities, meeting the following functional criteria: (1) The private key can be reconstructed given knowledge of all n of the pieces held by the plurality of trusted entities; (2) The private key cannot be guessed at all if one only knows less than all (<n−1) of the special pieces; and (3) For i−1, . . . n, the i^{th} special piece can be individually verified to be correct.

63. The Micali system does not allow communication of a secret in which only one party gains access to the content, and in which the third party or parties and one principal operate only on encrypted or secret information.

B. The Value Of The Inventions Disclosed In The STPC Patents

64. Executives at leading technology companies have described the value of specific encryption techniques as critical, lasting, and prominent. Chris Cicotte, a Cloud Architect at EMC, stated strong encryption technologies specific for networked computers "are a vital component of a strong security posture for any size organization, and it should be a standard

offering within the cloud . . . . The threat landscape has already begun to evolve, and from an overall security perspective, we need to take a proactive approach by layering in technologies like encryption at every layer."[23]

65. Companies such as Oracle Corporation, International Business Machines Corporation, Hewlett-Packard Company, and Google, Inc., confirm the importance of providing strong encryption systems that address the unique threats posed by moving data to the cloud.

> Once data is moved to the cloud, ***it becomes vulnerable to a number of new threats*** ranging from stolen administrator credentials to new hacking techniques. In addition, new legislation, such as the USA PATRIOT Act, is making it possible for competitors and governments to access data from cloud providers without the consent of the data owner. Many cloud providers thought they could achieve data sovereignty through locating cloud services in different jurisdictions, but this theory has been shaken by the subpoena classification ruling handed down recently in the U.S. federal court.

HP Atalla Cloud Encryption: Securing Data in the Cloud, HP TECHNICAL WHITE PAPER 2 (2014) (emphasis added).

> The need to secure data is driven by an expanding privacy and regulatory environment coupled with an increasingly dangerous world of hackers, insider threats, organized crime, and other groups intent on stealing valuable data. ***The security picture is complicated even more by the rapid expansion of access to sensitive data via the Internet***, an unprecedented understanding of technology, increasing economic competition, and the push to achieve greater efficiencies through consolidation and cloud computing.

Oracle Database 12C Security And Compliance, ORACLE WHITE PAPER 2 (February 2015) (emphasis added).

> With rare exceptions, one of the most important assets for any company is its data. Your data may take the form of financial information, proprietary sales information, marketing information, healthcare information, intellectual property (IP), and more. Losing your data could negatively affect operations and potentially shut down your organization. . . . Cloud-aware applications create unique security challenges in that both Infrastructure as a Service (IaaS) providers and Platform as a Service (PaaS) providers make use of a shared-risk model.

Robi Sen, *Develop Secure Cloud-Aware Applications*, IBM DEVELOPER WORKS 2-3 (May 20, 2015).

> Business requirements, industry regulations, and government mandates increasingly dictate that your organization must secure electronic communications. Whether it is financial data, medical records, or proprietary

[23] Jude Chao, *Cloud Computing Demands Cloud Data Encryption*, ENTERPRISE NETWORKING PLANET WEBSITE, May 13, 2014, http://www.enterprisenetworkingplanet.com/netsecur/cloud-computing-demands-cloud-data-encryption.html

> corporate information, you simply must secure the delivery of sensitive content to its destination.

Google Message Encryption, GOOGLE APPLICATION SECURITY PAPER 1 (2008)

66. Numerous academics have concluded the advent of cloud computing has created challenges that are unique to cloud computing and these challenges require specific encryption technologies that were previously unnecessary.

> Security is the most important challenge for cloud technology, as CSP's [Cloud Service Providers] have to protect the consumer's data from theft and ensure the consumer is not exploited. Consumers may be exploited from denial of service (DoS) attacks . . . ***They must also protect the data through the use of advanced encryption algorithms*** and ensure that their data centers are physically secure using advanced biometrics and many other authentication methods.

Sean Carlin & Kevin Curran, *Cloud Computing Technologies*, in INTERNATIONAL JOURNAL OF CLOUD COMPUTING AND SERVICES SCIENCE (IJ-CLOSER) Vol.1, No.2 at 59 (June 2012) (emphasis added).

> The growth of computer networks and the opening that their interconnection brings, especially through Internet, mean that a great amount of information is traveling through network and ***crossing numerous intermediate systems. This results in the increase of the number of possible attacks and illegal operations***. . . . They should guarantee the identity of the communicating parties . . . the protection against unauthorized writing and, in some cases, unauthorized reading of transferred data. These services of authentication, nonrepudiation, integrity and confidentiality, respectively, can be provided using cryptosystems.

Natasha Prohic, *Public Key Infrastructures - PGP vs. X.509*, in INFOTECH SEMINAR ADVANCED COMMUNICATION SERVICES (ACS) 2005 1 (emphasis added).

1. <u>U.S. Patent No. 8,316,237</u>

67. U.S. Patent No. 8,316,237 (the "237 patent") entitled, System and Method for Secure Three-Party Communications, was filed on January 10, 2011 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '237 patent. A true and correct copy of the '237 patent is attached hereto as Exhibit A. The '237 patent claims specific methods and systems for securely transcrypting protected electronic information transmitted over at least one computer network from a first encrypted form to a second, different encrypted form substantially without intermediate decryption of the protected electronic information.

68. The '237 patent has been cited by over 100 issued United States patents as relevant prior art. Specifically, patents issued to the following companies have cited the '237 patent as relevant prior art.

- Electronics and Telecommunications Research Institute (ETRI)
- NEC Corporation
- Disney Enterprises, Inc.
- WMS Gaming, Inc.
- Verizon Patent and Licensing, Inc.
- Microsoft Corporation.
- Netapp. Inc.
- NCR Corporation
- EMC Corporation
- AT&T Intellectual Property, L.P.
- Sony Corporation
- SAP AG
- Blackberry Limited
- Adobe Systems Incorporated
- Nippon Telegraph and Telephone Corporation
- Novell, Inc.
- Spring Communications L.P.
- Hytrust, Inc.
- International Business Machines Corporation
- Google, Inc.
- Kabushiki Kaisha Toshiba
- Panasonic Intellectual Property Management Co., Ltd.
- Zynga Inc.
- Certicom Corp.
- Wincor Nixdorf International Gmbh
- Oracle International Corporation
- Futurewei Technologies, Inc.
- Dell Products, L.P.
- Intuit Inc.

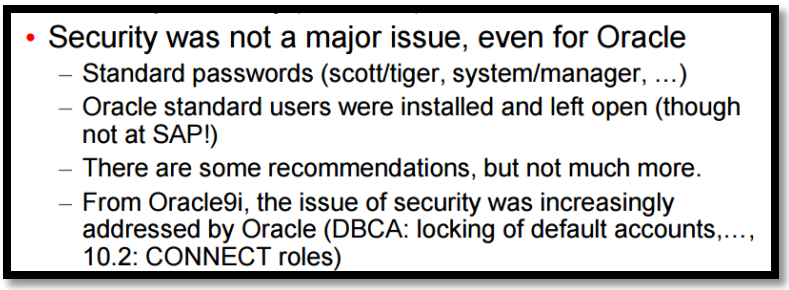
69. The ‘237 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

70. At the time of the inventions claimed in the ‘237 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the ‘237 patent: “Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy.” ‘237 patent, col. 2:13-17.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

71. Although the systems and methods taught in the '237 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '237 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '237 patent, col. 2:56-61. Indeed, companies such as Oracle have recognized that, until recently, security for distributed systems was not a primary concern.



Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

72. Further, the '237 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. "Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '237 patent, col. 2:61-64. Studies have confirmed that the inventions disclosed in the '237 patent improve the security of systems.

> Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

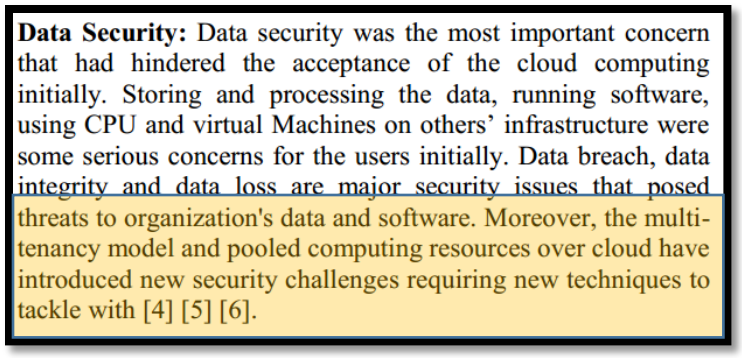
Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

73. The ‘237 patent claims are not directed to a “method of organizing human activity,” “fundamental economic practice long prevalent in our system of commerce,” or “a building block of the modern economy.” Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

74. The ’237 patent claims are not directed at the broad concept/idea of “encrypting” or “decrypting” information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

75. The inventive concepts claimed in the ’237 patent are technological, not “entrepreneurial.” For example, transcrypting protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

76. Researchers have identified the problems the ‘237 patent is directed at solving arise from new security challenges relating to cloud computing.



Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).

77. The '237 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '237 patent require transcrypting protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

78. The '237 patent claims are directed toward solving new threats that are related to moving data onto a computer network.

> Securing data—at rest and in use—is simpler when the data is located within the four walls of a data center. When data is moved to the cloud, it becomes vulnerable to a number of ***new threats ranging from stolen administrator credentials to new hacking techniques***. For many organizations, keeping data private and secure has also become a compliance requirement.

HP Atalla Cloud Encryption: Securing Data in the Cloud at 1, HP DATASHEET (2014) (emphasis added).

79. The '237 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '237 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '237 patent, col. 2:65–3:13. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential

cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. at col. 3:1–3:13. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the ’237 patent introduce several novel techniques to overcome these weaknesses and allow encrypted information to be securely transferred through an intermediary.

80. The preemptive effect of the claims of the ‘237 patent are concretely circumscribed by specific limitations. For example, claim 1 of the ‘237 patent requires:

> A transcryption device, comprising:
>
> > an automated communication port configured to receive a first message representing an encrypted communication associated with a first set of asymmetric keys, to receive a transcryption key, and to transmit a second message representing the encrypted communication associated with a second set of asymmetric keys, the first and second sets of encryption keys being distinct;
> >
> > a memory; and
> >
> > an automated processor, configured to communicate through the automated communication port and with the memory, to receive the first message, receive the transcryption key, automatically transcrypt the first message into the second message, and to transmit the second message, wherein the automated processor does not store as a part of the transcryption any decrypted representation of the encrypted communication, and the transcryption key is employed without revealing any secret cryptographic information usable for decrypting the first message or the second message.

81. The ‘237 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

82. The ‘237 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the ’237 patent includes inventive elements—embodied in specific claim limitations—that

concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

83. For example, the '237 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.
- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic

data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '237 lists 238 patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

84. Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[24] the '237 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

85. The '237 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

86. The claimed subject matter of the '237 patent is not a pre-existing but undiscovered algorithm.

87. The '237 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[25]

[24] *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[25] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible). *See also Paone v. Broadcom Corp.*, No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015).

88. The ’237 patent claims require the use of a computer system.

89. The claims in the ‘237 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the ‘237 patent improves the security of computer systems. Prior art systems that the ‘237 patent remedies enabled unauthorized “access to private communications or otherwise undermine[d] transactional security or privacy.” Companies have described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all ***require that organizations protect their data at rest and provide defenses against threats***.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

90. The ’237 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure. [26]

91. The claimed invention in the ’237 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

92. The systems and methods claimed in the ‘237 patent were not a longstanding or fundamental economic practice at the time of the patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one

[26] Limitations in the prior art that the ’237 patent was directed to solving included: computer systems where a “third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key” (*Id.*, col. 2:5-7); “[p]asswords may be written near access terminals (*Id.* col. 1:50-51);” “[s]ecurity tokens can be stolen or misplaced” (*Id.*, col. 1:51-52); “users may share supposedly secret information” (*Id.*, col. 1:52); and “unauthorized uses of the system” (*Id.*, col. 11:28). The '237 patent “allows the entity that transmits the information to be assured that the transmission will be secure, even with respect to a trusted third party, while ensuring that the intended recipient must cooperate with the intended third party.” ’237 patent, col. 8:48-52.

example, at the time the inventions disclosed in the '237 patent were conceived, the use of asymmetric encryption keys was described by Oracle as "relatively new."[27]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

93. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '237 patent is directed at overcoming were new and unique to distributed networks, as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[28]

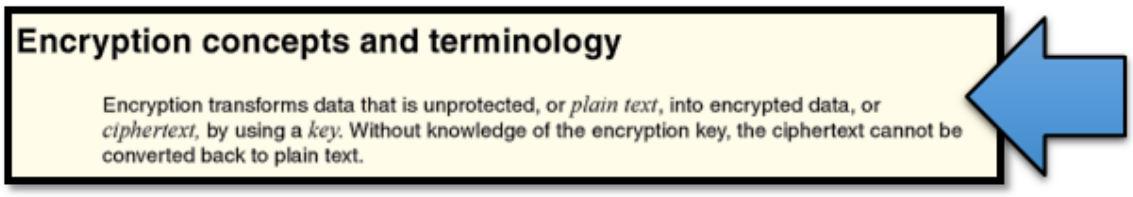
94. The '237 patent claims are not directed at a mathematical relationship or formula. The '237 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

95. '237 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected.

---

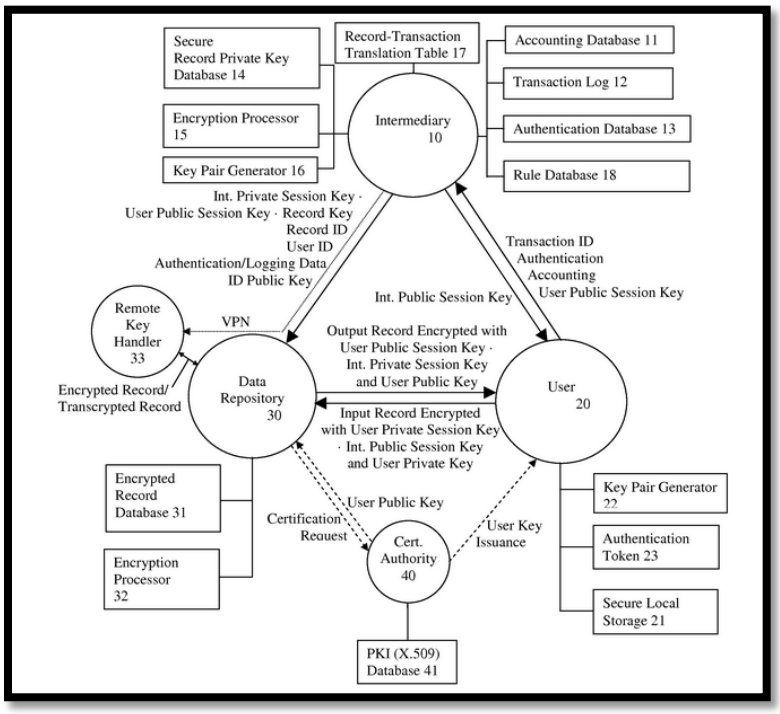
[27] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html ("Public key cryptography is relatively new and technically complex.").

[28] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).



Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

96. One or more claims of the '237 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '237 patent illustrates a specific configuration of hardware disclosed in the patent.



'237 patent, Fig. 1.

2. U.S. Patent No. 7,181,017

97. U.S. Patent No. 7,181,017 (the "'017 patent") entitled, System and Method for Secure Three-Party Communications, was filed on March 25, 2002, and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '017 patent. A true and correct copy of the

‘017 patent is attached hereto as Exhibit B. The ‘017 patent claims specific methods and systems for secure third-party communications—for example, a system and method for communicating information between a first party and a second party that includes identifying desired information; negotiating, through an intermediary, a cryptographic comprehension function for obscuring at least a portion of the information communicated between the first party and the second party; communicating the encrypted information to the second party, and decrypting the encrypted information using the negotiated cryptographic comprehension function. Moreover, in the patented systems and methods, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an “untrusted” intermediary.

98. The ‘017 patent has been cited by over 350 issued United States patents as relevant prior art. Specifically, patents issued to the following companies have cited the ‘017 patent.

- Electronics and Telecommunications Research Institute (ETRI)
- Sharp Laboratories of America, Inc.
- International Business Machines Corporation
- Microsoft Corporation
- Sony Corporation
- France telecom
- Siemens Medical Solutions USA, Inc.
- Canon Kabushiki Kaisha
- Nikon Corporation
- Apple, Inc.
- Fujitsu Limited
- Hewlett-Packard Development Company, L.P.
- SAP AG
- Guardian Data Storage, Llc
- Teradata US, Inc.
- AT&T Intellectual Property I, L.P.
- Panasonic Corporation
- Sharp Laboratories of America, Inc.
- Ricoh Company, Ltd.
- Nokia Corporation
- Boss Logic, Llc
- Juniper Networks, Inc.
- American Express Travel Related Services Company, Inc.
- Kyocera Mita Corporation
- Oracle International Corporation
- Medox Exchange Inc.
- Nortel Networks Limited

- Hitachi-Omron Terminal Solutions, Corporation
- Medapps, Inc.
- Samsung Electronics Co., Ltd.
- NEC Corporation
- Visa International Service Corporation
- Cisco Technology, Inc.
- Yahoo! Inc.
- Flexera Software Llc
- CompuGroup Medical AG
- Datcard Systems, Inc.
- Futurewei Technologies, Inc.
- Telecome Italia S.P.A.
- General Electric Company
- Fuji Xerox Co., Ltd.
- Massachusetts Institute Of Technology
- Netapp, inc.
- Koninkliike Philips N.V.
- Computer Associates Think, Inc.
- Huawei Technologies Co., Ltd.
- Texas Instruments, Inc.
- Nippon Telegraph And Telephone Corporation
- Research in Motion Limited.
- Net.Orange, Inc.
- Nokia Siemens Networks Oy
- Honeywell Int., Inc.

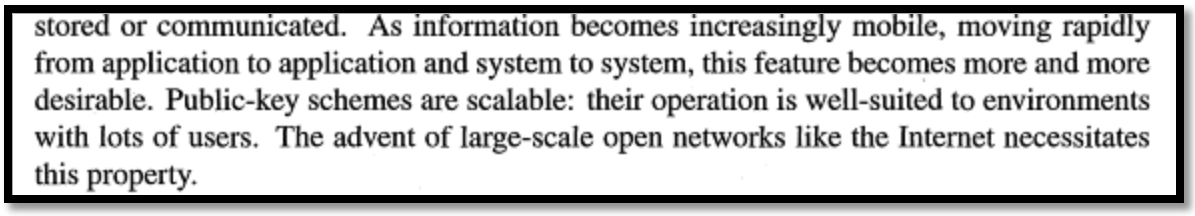
99. The claims in the '017 patent are directed at a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

100. At the time of the inventions claimed in the '017 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '017 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '017 patent, col. 1:54-61.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

101. Although the systems and methods taught in the '017 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '017 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '017 patent, col. 4:40-45. As described in an article contemporaneous to the '017 patent, the rise of cloud computing and distributed networks gave rise to a need to use key encryption to resolve security issues.


stored or communicated. As information becomes increasingly mobile, moving rapidly from application to application and system to system, this feature becomes more and more desirable. Public-key schemes are scalable: their operation is well-suited to environments with lots of users. The advent of large-scale open networks like the Internet necessitates this property.

Simon Blake-Wilson, *Information Security, Mathematics and Public-Key Cryptography*, in Designs, Codes and Cryptography, 19, 81 (2000).

102. Further, the '017 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. "Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '017 patent, col. 4:45-48. Studies have confirmed that the inventions disclosed in the '017 patent improve the security of systems.

> Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is

> stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

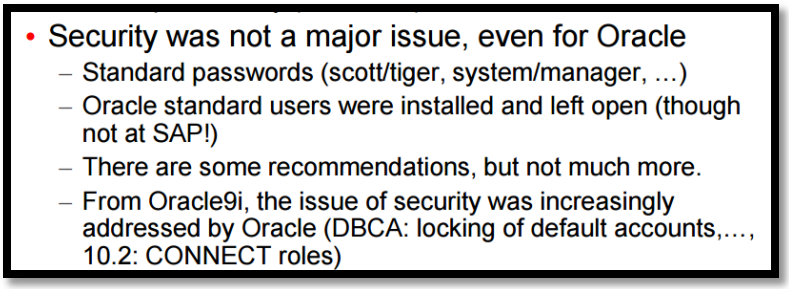
Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

103. The '017 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

104. The '017 patent claims are not directed at the broad concept/idea of "encrypting" or "decrypting" information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. This type of method and system is unique to the Internet age.

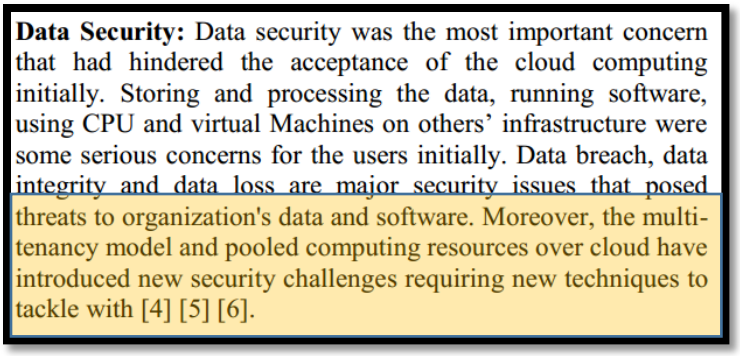
105. The inventive concepts claimed in the '017 patent are technological, not "entrepreneurial." For example, transcrypting protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

106. Companies such as Oracle have recognized that until recently security for distributed systems was not a primary concern.



Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

107. Researchers have identified the problems the ‘017 patent is directed at solving arise from new security challenges relating to cloud computing.



Data Security: Data security was the most important concern that had hindered the acceptance of the cloud computing initially. Storing and processing the data, running software, using CPU and virtual Machines on others' infrastructure were some serious concerns for the users initially. Data breach, data integrity and data loss are major security issues that posed threats to organization's data and software. Moreover, the multi-tenancy model and pooled computing resources over cloud have introduced new security challenges requiring new techniques to tackle with [4] [5] [6].

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).

108. The ‘017 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the ’017 patent require cryptographically manipulating protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

109. The ‘017 patent is directed to specific problems in the field of cryptography. In the “Background” section of the patent, the ’017 patent explains that encryption systems use “keys,” similar to passwords, to control how plaintext is encrypted and decrypted. ‘017 patent, col. 4:39–4:64. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work

with. The inventions of the ’017 patent introduce several novel techniques to overcome these weaknesses, particularly where encrypted information is held by an intermediary.

110. The preemptive effect of the ‘017 patent is concretely circumscribed by specific limitations. For example, claim 1 of the ‘017 patent requires:

> A method for processing information, comprising the steps of:
>
> receiving information to be processed:
>
> defining a cryptographic comprehension function for the information, adapted for making at least a portion of the information incomprehensible;
>
> receiving asymmetric cryptographic key information, comprising at least asymmetric encryption key information and asymmetric decryption key information;
>
> negotiating a new cryptographic comprehension function between two parties to a communication using an intermediary;
>
> processing the information to invert the cryptographic comprehension function and impose the new cryptographic comprehension function in an integral process, in dependence on at least the asymmetric cryptographic key information, without providing the intermediary with sufficient asymmetric cryptographic key information to decrypt the processed information; and
>
> outputting processed information,
>
> wherein the ability of the asymmetric decryption key information to decrypt the processed information changes dynamically.

111. The ‘017 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

112. The ‘017 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the ’017 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and limit its breadth. These inventive elements

are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

113. For example, the '017 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.
- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and

present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '017 lists numerous patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

114. Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[29] the claims in the '017 patent do not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

115. The '017 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer

116. The claimed subject matter of the '017 patent is not a pre-existing but undiscovered algorithm.

117. The '017 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[30]

[29] *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[30] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) ((finding claims directed to encryption to be patent eligible). *See also Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015).

118. The claims in the ‘017 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the ‘017 patent improves the security of computer systems. Prior art systems that the ‘017 patent remedies enabled unauthorized “access to private communications or otherwise undermine[d] transactional security or privacy.” HP has described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all ***require that organizations protect their data at rest and provide defenses against threats***.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

119. The ’017 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

120. The claimed invention in the ‘017 claims is rooted in computer technology and overcame problems specifically arising in the realm of computer networks.

121. The systems and methods claimed in the ‘017 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the ‘017 patent were conceived, the use of asymmetric encryption keys was described by Oracle as “relatively new.”[31]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

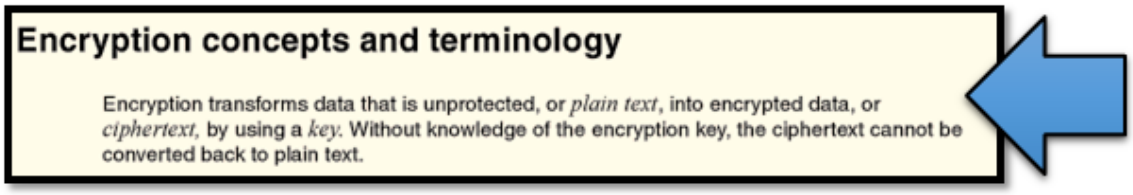
INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

[31] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as “new”); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html (“Public key cryptography is relatively new and technically complex.”).

122. The asserted claims do not involve a method of doing business implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '017 patent is directed at were new and unique to distributed networks as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[32]

123. The '017 patent claims are not directed to a mathematical relationship or formula. The '017 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

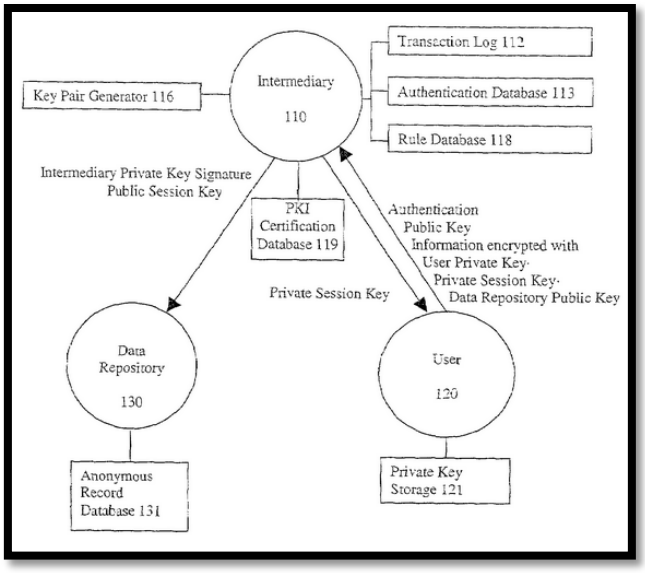
124. The '017 patent claims cover a systems and methods that transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected."



Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

125. One or more claims of the '017 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '017 patent illustrates a specific configuration of hardware disclosed in the patent.

[32] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).



'017 patent, Fig. 2.

3. U.S. Patent No. 7,869,591

126. U.S. Patent No. 7,869,591 (the "'591 patent") entitled, System and Method for Secure Three-Party Communications, was filed on February 16, 2007, and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '591 patent. A true and correct copy of the '591 patent is attached hereto as Exhibit C.

127. The '591 patent has been cited by over twenty issued United States patents as relevant prior art. Specifically, patents issued to the following companies have cited the '591 patent.

- Square, Inc.
- Konnklike Philips Electronics, N.V
- Red Hat, Inc.
- Microsoft Corporation
- Industrial Technology Research Institute ("ITRI")
- Electronics and Telecommunications Research Institute (ETRI)
- Saas Document Solutions Limited
- Good Technology Corporation
- Avanade Inc.
- Medical Management International, Inc.

128. The '591 patent claims specific methods and systems for secure third-party communications—for example, a system and method for communicating information between a first party and a second party that includes identifying desired information; negotiating, through

an intermediary, a cryptographic comprehension function for obscuring at least a portion of the information communicated between the first party and the second party; communicating the encrypted information to the second party; and decrypting the encrypted information using the negotiated cryptographic comprehension function. Moreover, in the patented systems and methods, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an "untrusted" intermediary.

129. The claims in the '591 patent are directed at a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

130. At the time of the inventions claimed in the '591 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '591 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '591 patent, col. 2:10-15.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

131. Although the systems and methods taught in the '591 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '591 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed

specifically to exclude third party monitoring." '591 patent, col. 2:54-69. As described in an article contemporaneous to the '591 patent, the rise of cloud computing and distributed networks gave rise to a need to use key encryption to resolve security issues.

> stored or communicated. As information becomes increasingly mobile, moving rapidly from application to application and system to system, this feature becomes more and more desirable. Public-key schemes are scalable: their operation is well-suited to environments with lots of users. The advent of large-scale open networks like the Internet necessitates this property.

Simon Blake-Wilson, *Information Security, Mathematics and Public-Key Cryptography*, in Designs, Codes and Cryptography, 19, 81 (2000).

132. Further, the '591 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. "Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '591 patent, col. 2:59-62. Studies have confirmed that the inventions disclosed in the '591 patent improve the security of systems.

> Key management is a big concern with encryption, because ***the effectiveness of the solution ultimately depends on protecting the key***. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

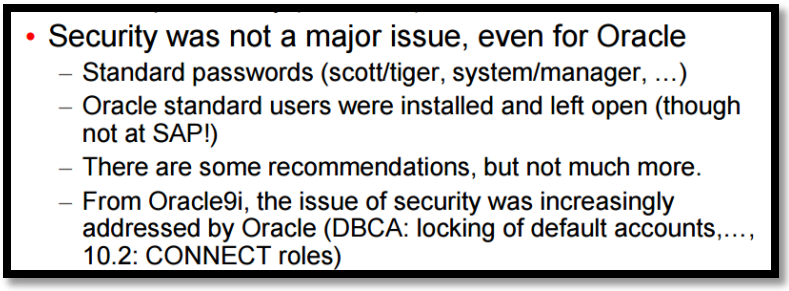
Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

133. The '591 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

134. The ‘591 patent claims are not directed at the broad concept/idea of “encrypting” or “decrypting” information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. This type of method and system is unique to the Internet age.

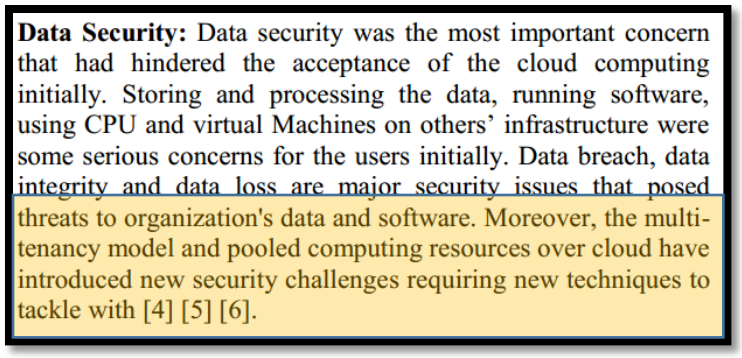
135. The inventive concepts claimed in the ’591 patent are technological, not “entrepreneurial.” For example, transcrypting protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

136. Companies such as Oracle have recognized that until recently security for distributed systems was not a primary concern.



Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

137. Researchers have identified the problems the ‘591 patent is directed at solving arise from new security challenges relating to cloud computing.



Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).

138. The '591 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, the claims of the '591 patent require cryptographically manipulating protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

139. The '591 patent is directed to specific problems in the field of cryptography. In the "Background" section of the patent, the '591 patent explains that encryption systems use "keys," similar to passwords, to control how plaintext is encrypted and decrypted. '591 patent, col. 2:16-37. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more information to work with. The inventions of the '591 patent introduce several novel techniques to overcome these weaknesses, particularly where encrypted information is held by an intermediary.

140. The preemptive effect of the ‘591 patent is concretely circumscribed by specific limitations. For example, claim 13 of the ‘591 patent requires:

> A method for transcrypting information, comprising:
>
> (a) receiving and storing in a first memory information encrypted based on a first set of cryptographic keys, a first portion of the first set of cryptographic keys having been employed to produce the encrypted information and a second portion of the first set of cryptographic keys being required to decrypt the information encrypted with the first portion of the first set of cryptographic information;
>
> (b) receiving and storing in a second memory a first portion of a second set of cryptographic keys, having a corresponding second portion of the second set of cryptographic keys being required for decryption of a message encrypted using the first portion of the second set of cryptographic keys;
>
> (c) negotiating a set of session keys through a communication port,
>
> (d) generating a transcryption key for transforming the received encrypted information to transcrypted information, in dependence on at least:
>
> (i) information representing the second portion of the first set of cryptographic keys,
>
> (ii) information representing the first portion of the second set of cryptographic keys; and
>
> (iii) a first portion of the set of session keys, and
>
> (e) transcrypting the stored encrypted information into transcrypted information using the transcryption key, wherein the generating a transcryption key step and the transcrypting the encrypted information step are performed without either requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcrypted information.

141. The ‘591 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

142. The ‘591 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the ’591 patent includes inventive elements—embodied in specific claim limitations—that

concretely circumscribe the patented invention and limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

143. For example, the '591 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.
- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic

data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '591 lists numerous patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

144. Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[33] the claims in the '591 patent do not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

145. The '591 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

146. The claimed subject matter of the '591 patent is not a pre-existing but undiscovered algorithm.

147. The '591 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[34]

[33] *Paone v. Broadcom Corp.*, No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[34] *TQP Dev., LLC v. Intuit Inc.*, No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) ((finding claims directed to encryption to be patent eligible). *See also Paone v.*

148. The claims in the ‘591 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the ‘591 patent improves the security of computer systems. Prior art systems that the ‘591 patent remedies enabled unauthorized “access to private communications or otherwise undermine[d] transactional security or privacy.” HP has described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all ***require that organizations protect their data at rest and provide defenses against threats***.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

149. The ’591 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

150. The claimed invention in the ‘591 claims is rooted in computer technology and overcame problems specifically arising in the realm of computer networks.

151. The systems and methods claimed in the ‘591 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the ‘591 patent were conceived, the use of asymmetric encryption keys was described by Oracle as “relatively new.”[35]

> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

Broadcom Corp., No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015).

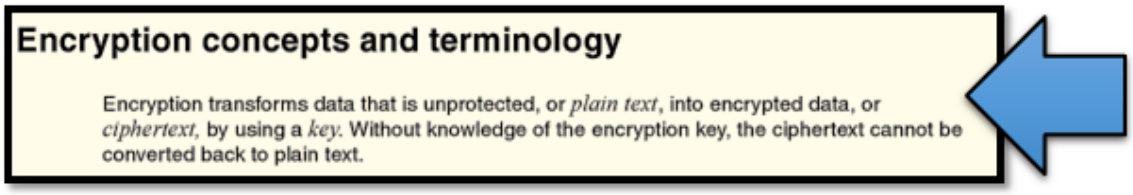
[35] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as “new”); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html (“Public key cryptography is relatively new and technically complex.”).

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

152. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '591 patent is directed at were new and unique to distributed networks as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[36]

153. The '591 patent claims are not directed at a mathematical relationship or formula. The '591 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

154. '591 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected.

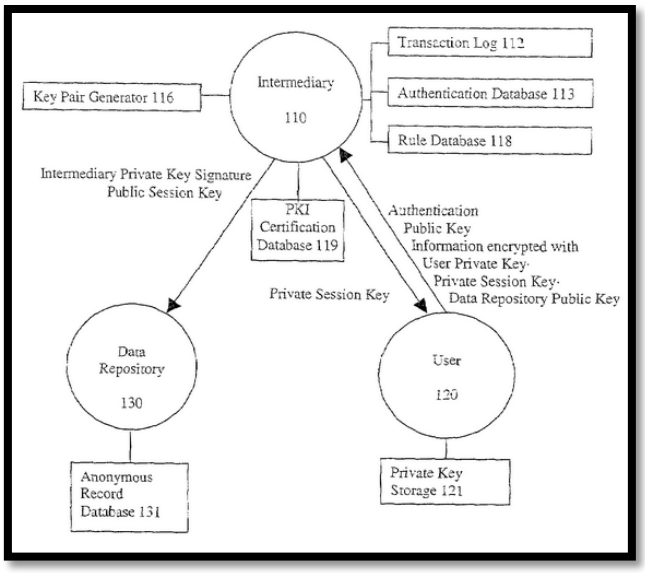


Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

155. One or more claims of the '591 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the

[36] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

claimed methods and systems to specific machines. For example, the below diagram from the '591 patent illustrates a specific configuration of hardware disclosed in the patent.



'591 patent, Fig. 2.

4. U.S. Patent No. 8,904,181

156. U.S. Patent No. 8,904,181 (the "'181 patent") entitled, System and Method for Secure Three-Party Communications, was filed on November 20, 2012 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the '181 patent. A true and correct copy of the '181 patent is attached hereto as Exhibit D. The '181 patent claims specific methods and systems for securely transcrypting protected electronic information transmitted over at least one computer network from a first encrypted form to a second, different encrypted form substantially without intermediate decryption of the protected electronic information.

157. The '181 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted electronic information via an intermediary device, wherein the electronic information is cryptographically secure not only from outside attackers, but also from the intermediary.

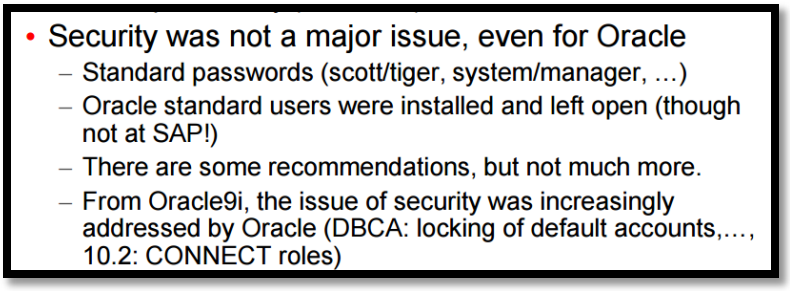
158. At the time of the inventions claimed in the '181 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing

environment presented new and unique issues over the state of the art. As explained in the '181 patent: "Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy." '181 patent, col. 2:14-20.

> Generating and protecting encryption keys while maintaining data availability has traditionally been a major barrier to implementing encryption, especially on an enterprise scale. Key management is complex and challenging, and often fails because issuance, storage, and renewing are difficult. ***Worse yet, lost keys can make important data permanently unrecoverable***.

Sustainable Compliance for the Payment Card Industry Data Security Standard, ORACLE WHITE PAPER 23 (July 2015) (emphasis added).

159. Although the systems and methods taught in the '181 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '181 patent claims were innovative and novel. "Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring." '181 patent, col. 2:59-64. Indeed, companies such as Oracle have recognized that, until recently, security for distributed systems was not a primary concern.



Andreas Becker, *High Security for SAP Data with Oracle Database Vault and Transparent Data Encryption*, ORACLE PRESENTATION 6 (2010).

160. Further, the '181 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary

without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient. "Third parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure." '181 patent, col. 2:64-67. Studies have confirmed that the inventions disclosed in the '181 patent improve the security of systems.

> Key management is a big concern with encryption, because the effectiveness of the solution ultimately depends on protecting the key. If the key is exposed, the data being protected with the key is, essentially, exposed. Wherever the key is stored, it must be protected, and it should be changed on occasion. For example, if an administrator with access to a key leaves an organization, the key should be changed.

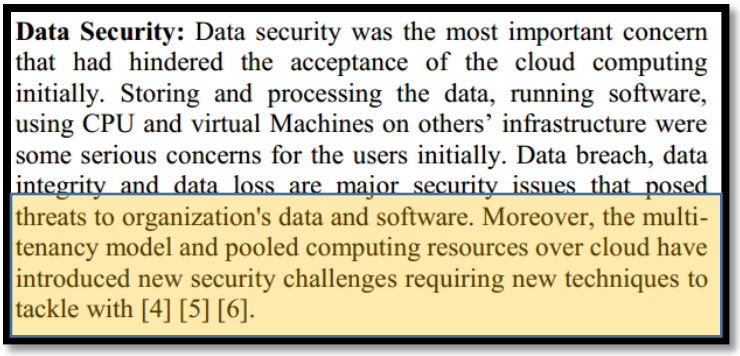
Tanya Baccam, *Transparent Data Encryption: New Technologies and Best Practices for Database Encryption*, SANS WHITE PAPER 3 (April 2010) (emphasis added).

161. The '181 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary.

162. The '181 patent claims are not directed at the broad concept/idea of "encrypting" or "decrypting" information. Instead, they are limited to a concretely circumscribed set of methods and systems for transcrypting electronic information that is transmitted over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

163. The inventive concepts claimed in the '181 patent are technological, not "entrepreneurial." For example, transcrypting protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

164. Researchers have identified the problems the ‘181 patent is directed at solving arise from new security challenges relating to cloud computing.



Data Security: Data security was the most important concern that had hindered the acceptance of the cloud computing initially. Storing and processing the data, running software, using CPU and virtual Machines on others' infrastructure were some serious concerns for the users initially. Data breach, data integrity and data loss are major security issues that posed threats to organization's data and software. Moreover, the multi-tenancy model and pooled computing resources over cloud have introduced new security challenges requiring new techniques to tackle with [4] [5] [6].

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).

165. The ‘181 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the ’181 patent require transcrypting protected electronic information using one or more intermediary computing devices specially configured to yield a desired result—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

166. The ‘181 patent is directed to specific problems in the field of cryptography. In the “Background” section of the patent, the ’181 patent explains that encryption systems use “keys,” similar to passwords, to control how plaintext is encrypted and decrypted. ‘181 patent, col. 2:11–5:8. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id*. Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of ciphertext (encrypted information) and different possible keys in order to eventually converge on the correct key and break the encryption. *Id*. at col. 4:10–4:27.

167. Both attacks exploit the fact that some encryption systems use static keys to create the ciphertext. *Id*. In other words, using the same key over and over gives an attacker more

information to work with. The inventions of the ’181 patent introduce several novel techniques to overcome these weaknesses and allow encrypted information to be securely transferred through an intermediary.

168. The preemptive effect of the claims of the ‘181 patent are concretely circumscribed by specific limitations. For example, claim 1 of the ‘181 patent requires:

> A key handler, comprising:
>
> > an interface to a memory which stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair;
> >
> > at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to transcrypt the encrypted message to a transcrypted message in an integral process substantially without intermediate decryption, using a transcryption key derived at least in part from the at least one asymmetric session key; and
> >
> > a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcrypted record.

169. The ‘181 patent does not attempt to preempt every application of the idea of encrypting electronic information transmitted over a computer network, or even the idea of encrypting electronic information transmitted over a computer network via an intermediary.

170. The ‘181 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the ’181 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

171. For example, the '181 patent describes numerous techniques for secure third-party communications that inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.
- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls And Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150

to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '181 patent lists hundreds of patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

172. Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[37] the '181 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

173. The '181 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

174. The claimed subject matter of the '181 patent is not a pre-existing but undiscovered algorithm.

175. The '181 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[38]

176. The '181 patent claims require the use of a computer system.

[37] *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing* Fid. Nat'l Info. Servs., Inc., Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[38] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible). *See also Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015).

177. The claims in the ‘181 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the ‘181 patent improves the security of computer systems. Prior art systems that the ‘181 patent remedies enabled unauthorized “access to private communications or otherwise undermine[d] transactional security or privacy.” HP has described the use of encryption in the cloud as important to improve the security and functioning of systems.

> For many organizations, keeping data private and secure has also become a compliance requirement. Standards including Health Insurance Portability and Accountability Act of 1996 (HIPAA), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standard (PCI DSS), the Gramm-Leach-Bliley Act, and EU Data Protection Directives all ***require that organizations protect their data at rest and provide defenses against threats***.

HP ATALLA CLOUD ENCRYPTION: SECURING DATA IN THE CLOUD, HP TECHNICAL WHITE PAPER 2 (2014).

178. The ’181 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure. [39]

179. The claimed invention in the ’181 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

180. The systems and methods claimed in the ‘181 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the ‘181 patent were conceived, the use of asymmetric encryption keys was described by Oracle as “relatively new.”[40]

---

[39] Limitations in the prior art that the ’181 patent was directed to solving included: computer systems where a “third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key” (*Id.*, col. 2:6-9); “[p]asswords may be written near access terminals (*Id.* col. 1:52-54);” “[s]ecurity tokens can be stolen or misplaced” (*Id.*, col. 1:54-55); and “users may share supposedly secret information” (*Id.*, col. 1:55).

[40] *See also* BACKUPEDGE ENCRYPTION WHITEPAPER, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as “new”); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), http://www.rogerclarke.com/II/CryptoSecy.html (“Public key cryptography is relatively new and technically complex.”).

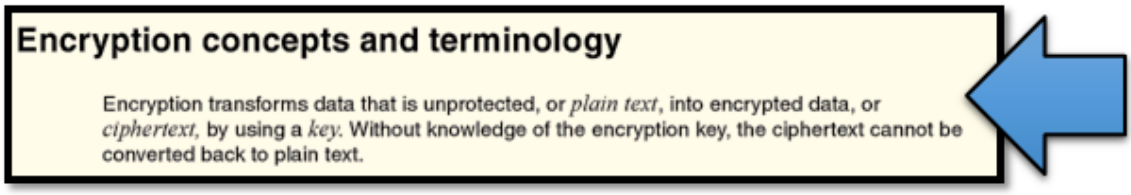
> A Public Key Infrastructure (PKI) consists of protocols, services, and standards supporting applications of public key cryptography. ***Because the technology is still relatively new***, the term PKI is somewhat loosely defined.

INTRODUCTION TO THE SSL TECHNOLOGY, ORACLE DOCUMENTATION (February 1, 2001), http://docs.oracle.com/cd/E53645_01/tuxedo/docs12cr2/security/publickey.html

181. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '181 patent is directed at overcoming were new and unique to distributed networks, as confirmed in a recent paper from Accenture Services Pvt. Ltd.: "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."[41]

182. The '181 patent claims are not directed at a mathematical relationship or formula. The '181 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

183. '181 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected.

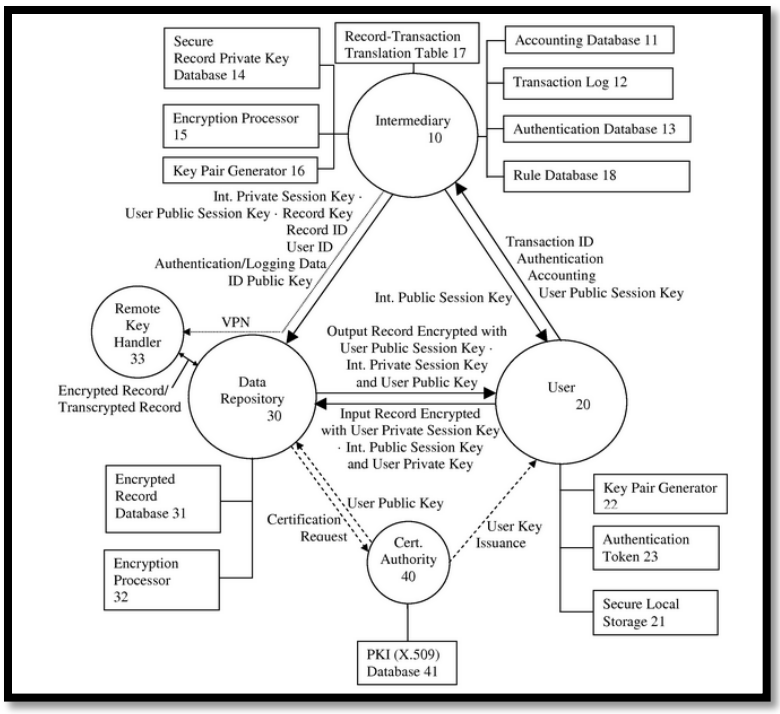


Bertrand Dufrasne and Robert Tondini, IBM DS8870 DISK ENCRYPTION 6th Edition at 4 (2015) (From a reference guide published by IBM.)

184. One or more claims of the '181 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the

[41] Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014).

claimed methods and systems to specific machines. For example, the below diagram from the '181 patent illustrates a specific configuration of hardware disclosed in the patent.



'181 patent, Fig. 1.

C. Information Record Infrastructure Patents

185. The IRI patents disclose specific computer based systems and methods for electronically structuring and controlling access to protected data in a plurality of external databases.

186. Over fifteen years ago, Mr. Felsher conceived of the inventions disclosed in the IRI patents, based on his experiences with the limitations in existing systems for controlling access to electronic medical records and protected electronic data.

187. During Mr. Felsher's work in the field of electronic medical records, he witnessed first-hand the drawbacks to existing computer systems and methods for controlling access to protected data. Existing systems failed to efficiently transmit unstructured protected information. '368 patent, col. 3:5-10. Other problems included the inability to secure the protection of data, integrate content management functions, and create a trust infrastructure

wherein an independent third party represents and serves as an agent for the content owner. *Id.* at col. 3:4-54:16. The result was an inability to effectively manage access to protective data. The IRI patents disclosed systems and methods that overcome these drawbacks. The inventions disclosed in the IRI patents improved upon the then-available technology, enabled efficient access control of unstructured data, reduced costs, and ultimately resulted in a more secure system.

188. HP values systems that provide secure systems and methods for controlling access to protected data such as the system disclosed in the IRI patents.

> ***What our customers need is a data-centric solution that protects sensitive information*** from the moment it's created throughout its entire lifecycle. That means protecting data *wherever* it moves – from emails to databases and attachments, in applications, in big data and analytic tools, through payment systems, mobile devices, on premise and in the cloud, in use, at rest, and in motion – for practically any data, anywhere.

Albert Biketi VP and General Manager, *HP Atalla*, *HP Gets Serious About End-To-End Data Protection*, HP SECURITY BLOG, February 19, 2015.

189. HP and its competitors, such as Microsoft Corporation, have confirmed the importance and value of systems and methods that manage access to protected data.

> Today, the need for data protection and security goes well beyond the realm of access privileges and firewalls. Organizations of all sizes, in public and private sectors, must not only protect information from unauthorized access and intrusion but also manage how documents, presentations, spreadsheets, and e-mails are handled in the normal course of daily business

HP INFORMATION RIGHTS MANAGEMENT SOLUTIONS ENSURING LIFE CYCLE PROTECTION OF DIGITAL INFORMATION IN MICROSOFT ENVIRONMENTS, HP WHITE PAPER (2005).

> Such cloud adoption within the healthcare industry is gaining momentum because the economic, clinician productivity and care team collaboration advantages of the cloud are undeniable. However, as was the case for UCHealth, there's ***one fundamental concern that continues to weigh heavily on the minds of providers: Is patient data safe, secure and private in the cloud***.

UNIVERSITY OF COLORADO HEALTH ADOPTS MICROSOFT OFFICE 365 FOR ITS DATA PRIVACY AND SECURITY COMMITMENT, MICROSOFT ON THE ISSUES BLOG (December 18, 2013), http://blogs.microsoft.com/on-the-issues/2013/12/18/university-of-colorado-health-adopts-microsoft-office-365-for-its-data-privacy-and-security-commitment/ (emphasis added).

190. Academics have confirmed the value of secure information access management systems such as the inventions disclosed in the IRI patents.

> With the proliferation of the Internet, the speed and ease of digital data exchange has increased, together with the number of potential parties that can exchange data. This has also meant that digital data security is no longer confined to the computer that holds the original data, or even behind corporate firewalls. Furthermore, data security no longer applies only to the access to data, but also to what the user can do with the data

Alapan Arnab and Andrew Hutchinson, *Digital Rights Management - An Overview of Current Challenges and Solutions*, in PROCEEDINGS OF INFORMATION SECURITY SOUTH AFRICA CONFERENCE (2004) (emphasis added).

191. Although major corporations offer systems for providing secure access to protected data today, at the time the inventions disclosed in the IRI patents were conceived, systems had significant limitations that were addressed by the inventions disclosed in the IRI patents.

> While "awareness of risks and of possible technical solutions is increasing," the authors would appear to be describing a rather precarious environment, at least in the short run. The picture does not improve when one focuses on the details of some of the technical fixes. Barrows and Clayton deem "tight" prospective access restrictions—a "need to know," mandatory access control model—as largely incompatible with the dynamic health care environment.

Reid Cushman, *Serious Technology Assessment for Health Care Information Technology*, JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION 4(4) (1997).[42]

192. The claims in the IRI patents describe solutions that are rooted in computer technology to overcome problems specific to and characteristic of complex computer networks where protected data is stored. For example, academics identified distributed information systems as leading to new problems regarding information rights management that the IRI patents solve.

> The development and wider use of wireless networks and mobile devices has led to novel pervasive computing environments ***which pose new problems for software rights management*** and enforcement on resource-constrained and occasionally connected devices. . . . The latter opens new channels for super-distribution and sharing of software applications that do not impose a cost on the user.

[42] This reference is cited on the face of the IRI patents as an exemplar illustrating limitations in systems existing at the time the inventions disclosed in the IRI patents were conceived; *see also* Alapan Arnab and Andrew Hutchinson, *Digital Rights Management - An Overview of Current Challenges and Solutions*, in PROCEEDINGS OF INFORMATION SECURITY SOUTH AFRICA CONFERENCE (2004) (emphasis added) ("none of these products provide for all the needs of an enterprise, and furthermore these products do not offer all the benefits that DRM potentially offers to an enterprise).

Ivana Dusparic, Dominik Dahlem, and Jim Dowling, *Flexible Application Rights Management in a Pervasive Environment*, in IEEE INTERNATIONAL CONFERENCE ON E-TECHNOLOGY, E-COMMERCE AND E-SERVICE, pages 680–685 (2005) (emphasis added).[43]

> Then there is the cloud. Cloud, cloud, cloud, it's on every webcast, in every article. The cloud has many advantages. Why wouldn't you want to outsource all your costs of network management, storage, system administration? The cloud makes perfect sense but has one massive concern... security.

Simon Thorpe, *Security in the Enterprise 2.0 World: Conflicts of Collaboration*, ORACLE OFFICIAL BLOG, September 27, 2010, https://blogs.oracle.com/irm/.

193. Although secure and effective information rights management, in some form, has been an objective of corporations and researchers for many years (‘368 patent, col. 6:61-7:3), the IRI patents are directed at solving problems that are unique to the realm of computers and specifically network cloud computing.

194. The systems and methods disclosed in the IRI patents have particular application to two primary fields: electronic medical records and electronic rights management. Shortcomings in available technology at the time the inventions disclosed in the IRI patents were conceived, led to the development of the IRI patents.

195. A brief overview of the state of the prior art in these two areas provides context to understanding the truly inventive nature of the IRI patents. The specific systems and methods disclosed and claimed in the IRI patents are discussed in detail later in this Complaint.

196. Background on the state of the art at the time of the inventions disclosed in the IRI patents confirms that the patented inventions are limited to specific computer systems and

---

[43] *See also* Aaron Franks, Stephen LaRoy, Miek Wood, and Mike Worth. *Idrm: An Analysis Of Digital Rights Management For The Itunes Music Store*, TECHNICAL REPORT, UNIVERSITY OF BRITISH COLUMBIA (2005) (“The need for secure digital rights management (DRM) is more urgent today than ever before. With the rapid increase in broadband availability, Internet file sharing has become a threat to content providers’ bottom line.”); Mike Godwin, *What Every Citizen Should Know About DRM, A.K.A. ‘Digital Rights Management,’* PUBLIC KNOWLEDGE (2004) (“As circumvention tools evolve, and as new technologies pose new infringement problems, the locking of industrial sectors into a particular “standard” scheme, mediated and supervised by government, actually slows the ability of the content sector to respond to new problems.); HP DIGITAL RIGHTS MANAGEMENT (DRM) FOR NETWORK AND SERVICE PROVIDERS (NSPS), HP SOLUTION BRIEF (2003) (“DRM [Digital Rights Management] is an emerging technology with fragmented addressable markets, solution capabilities and standards”).

methods and address issues specific to accessing protected data using modern computer networks.

197. ***Information Rights Management***. The inventions disclosed in the IRI patents have particular application to the management of rights in digital works, to allow a content owner to exploit the value of the works while assuring control over the use and dissemination. The IRI patents address problems specific to and arising from distribution and protected works on the internet.

198. At the time the inventions disclosed in the IRI patents were conceived, the growth of the internet created unique problems relating to managing rights to protected works.

> There's too much data being collected in so many ways, and a lot of it in ways that you don't feel you had a role in the specific transaction," he [Craig Mundie] said. "Now that you're just being observed, whether it's for commercial purposes or other activities, ***we have to move to a new model.***" . . . Under the model imagined by Mundie [a] central authority would distribute encryption keys to applications, allowing them to access protected data in the ways approved by the data's owners.

Tom Simonite, *Microsoft Thinks DRM Can Solve the Privacy Problem*, MIT TECHNOLOGY REVIEW, October 10, 2013 (emphasis added) (Craig Mundie is Senior Advisor to the CEO at Microsoft and its former Chief Research and Strategy Officer).[44]

199. In the late 1990s and early 2000s, information rights management systems had significant limitations. Prior art systems did not create a trust infrastructure, wherein an independent third party represents and serves as agent for the content owner, implementing a set of restrictive rules for use of the content, and interacting and servicing customers.

200. Rudimentary information rights management systems such as Microsoft's PlayForSure and RealNetwork's Rhapsody were still years from being released. Even when these systems were released in 2004 they had significant limitations. Both systems lacked the ability of a third party to act as an intermediary between a content creator and a user. The state

[44] *See also* Martin Abrahams, *Document Theft - IRM as a Last Line of Defense*, ORACLE IRM, THE OFFICIAL BLOG, August 1, 2011, https://blogs.oracle.com/irm/ ("The relevance of IRM is clear. . . . In a cloudy world, where perimeters are of diminishing relevance, you need to apply controls to the assets themselves.").

of the art at the time the inventions disclosed in the IRI patents were conceived underscores the inventive nature of the IRI patents.

201. ***Electronic Medical Records***. The IRI patents disclose systems and methods for controlling access to protected health information where the information is stored in one or more external databases. Systems for controlling access to medical records, contemporaneous to the IRI patents had significant limitations that the IRI patents address.[45] These systems include: (1) Anonymizing the record. A method used in contemporaneous systems to the IRI patents is the maintenance of anonymous medical records. However, such techniques did not provide patients and medical professionals the ability to access patient specific records. (2) Indexing. Contemporaneous systems sought to index records with anonymous identification codes. While this system preserves privacy, it made locating a database record other than by patient identifier, or its accession identifier, difficult. (3) Proxy Systems. Other contemporaneous systems used a proxy server to protect user privacy. However, systems using an Internet proxy resulted in a loss of rights and did not act in a representative capacity for the content owner, and did not integrate content management functions.

202. In addition, access to these early medical records systems was limited to authorized individuals who were on-site, as these systems provided little-to-no connectivity to anyone outside of the organization or to the Internet generally. Because access was restricted to on-site users on a local network using stationary terminals in designated areas, there was very little emphasis placed on data security.

203. In sharp contrast to the flexible, modular, and tightly integrated multi-layer security and access control framework disclosed and claimed in the IRI patents, systems such as

[45] *See* Reid Cushman, *Serious Technology Assessment for Health Care Information Technology*, J. AM. MED. INFORM. ASSOC. 4: 259-265 (1997) (This article is cited on the face of the IRI patents and finds "Data protection practices in the typical late twentieth-century organization are not very good, even in putatively "secure" institutions. . . The forthcoming study of health care security by the National Academy of Sciences, to be released in February 1997, is expected to reach a similar conclusion. The widespread deficits in security are hardly a secret; they are common fodder among information systems professionals.").

Epic System Corporation's CareWeb[46] had significant limitations, including: inability to effectively control access on a record-by-record basis within respective external databases, as claimed in several IRI patents; inability to distinguish between records within an external or backend database, the databases accessed through CareWeb were basically opaque to the "CareWeb" system; CareWeb's implementation because of its fixed structure was expressly limited to a particular, monolithic front-end architecture for secure implementation.

204. At the time the inventions disclosed in the IRI patents were conceived, the medical community showed little sign of implementing a system for controlling access to medical records that were stored in extern databases. However, computer networks presented new challenges and unique problems that the IRI patents addressed.

> As health care moves from paper to electronic data collection, providing easier access and dissemination of health information, the development of guiding privacy, confidentiality, and security principles is necessary to help balance the protection of patients' privacy interests against appropriate information access. . . . It is imperative that all participants in our health care system work actively toward a viable resolution of this information privacy debate.

Suzy Buckovich, Helga Rippen, and Michael Rozen, *Driving Toward Guiding Principles: A Goal for Privacy, Confidentiality, and Security of Health Information*, J. AM. MED. INFORM. ASSOC. 6 (1999).

205. The need for a secure system for providing access to medical records was specifically required to address cloud computing where medical records were stored in one or more external databases.

> The healthcare industry is in a major period of transformation and IT modernization. More than ever, healthcare providers and professionals are faced with the need to be more efficient, reduce costs and collaborate seamlessly as virtual teams to deliver higher quality care for more people at a lower cost point. Healthcare organizations are increasingly looking to cloud technologies to help them meet these goals. However, a natural concern with using cloud technology is keeping sensitive health information private and secure.

Hemant Pathak, DATA PRIVACY AND COMPLIANCE IN THE CLOUD IS ESSENTIAL FOR THE HEALTHCARE INDUSTRY (December 2013), http://www.microsoft.com/en-us/health/blogs/data-privacy-and-compliance-in-the-cloud-is-essential-for-the-healthcare-industry/default.aspx.

---

[46] John D. Halamka, Peter Szolovits, David Rind, and Charles Safran, *A WWW Implementation of National Recommendations for Protecting Electronic Health Information*, J. AM. MED. INFORM. ASSOC. 4: 458-464 (1997) (The limitations of the CareWeb system are discussed in depth in the specification of the IRI patents.).

1. U.S. Patent No. 7,587,368

206. U.S. Patent No. 7,587,368 (the "'368 patent") entitled, Information Record Infrastructure, System and Method, was filed on July 5, 2001, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '368 patent. A true and correct copy of the '368 patent is attached hereto as Exhibit E. The '368 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer.

207. The '368 patent has been cited by over 100 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '368 patent as relevant prior art.

- Microsoft Corporation
- LG Electronics, Inc.
- Canon Kabushiki Kaisha
- Hewlett-Packard Development Company, L.P.
- Voltage Security, Inc.
- Northrop Grumman Systems Corporation
- International Business Machines Corporation
- Mcafee, Inc.
- J.D. Power And Associates
- NEC Corporation
- Electronics And Telecommunications Research Institute (ETRI)
- Koninklijke Philps Electronics N.V.
- Huawei Technologies Co., Ltd.
- Ricoh Co., Ltd.
- Massachusetts Institute Of Technology

208. The '368 patent claims a technical solution to a problem unique to computer networks – securely transmitting encrypted digital records and controlling access to digital records requested by a remote computer.

209. At the time of the inventions claimed in the '368 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the '368 patent: "The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality." '368 patent, col. 54:27-33.

210. Although the systems and methods taught in the ‘368 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the ’368 patent claims were innovative and novel. “Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions.” ‘368 patent, col. 5:4-16.

211. Further, the ’368 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. “[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result.” ‘368 patent, col. 67:65-67.

212. The ‘368 patent claims are not directed to a “method of organizing human activity,” “fundamental economic practice long prevalent in our system of commerce,” or “a building block of the modern economy.” Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

213. The ’368 patent claims are not directed at the broad concept/idea of “managing digital records.” Instead, the ‘368 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

214. The ‘368 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the ’368 patent require encrypting and sending, by the server system, the requested digital record which has been validated, using the public key and the session key to

encrypt the digital record - a procedure that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

215. The ‘368 patent is directed to specific problems in the field of digital record access and transmission.

216. The preemptive effect of the claims of the ‘368 patent are concretely circumscribed by specific limitations. For example, claim 1 of the ‘368 patent requires:

> A method, comprising the steps of:
>
> > storing a plurality of digital records and respective access rules for each digital record in a computer memory associated with a server system;
> >
> > receiving a request for access, from a remote computer, to access a digital record stored in the computer memory;
> >
> > validating, by the server system, the received request to access the digital record by applying a respective set of access rules for the digital record stored in the computer memory;
> >
> > retrieving, by the server system, a public key having an associated private key, and associating a logging wrapper having a respective session key with the digital record, after validating the received request, wherein the session key is distinct from the public key and the private key;
> >
> > encrypting and sending, by the server system, the requested digital record which has been validated, using the public key and the session key to encrypt the digital record;
> >
> > receiving and decrypting the encrypted digital record, by the remote computer, using the private key, and the session key in conjunction with the logging wrapper;
> >
> > generating by the logging wrapper, at the remote computer, a logging event; and
> >
> > recording the logging event in an access log.

217. The ‘368 patent does not attempt to preempt every application of the idea of controlling access to an encrypted digital record over a computer network.

218. The ‘368 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the ’368 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are

not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

219. For example, the ‘368 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The techniques inform the invention’s development but do not, standing alone, fall within the scope of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained
- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.
- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.
- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.
- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.
- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.

- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.
- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).

220. Although "[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,"[47] the '368 patent does not claim, or attempt to preempt, "some process that involves the encryption of data for some purpose" (or similar abstraction).

221. The '368 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

222. The claimed subject matter of the '368 patent is not a pre-existing but undiscovered algorithm.

223. The '368 patent claims systems and methods that "could not conceivably be performed in the human mind or pencil and paper."[48]

224. The '368 patent claims require the use of a computer system.

---

[47] *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (*citing Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

[48] *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible). *See also Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015).

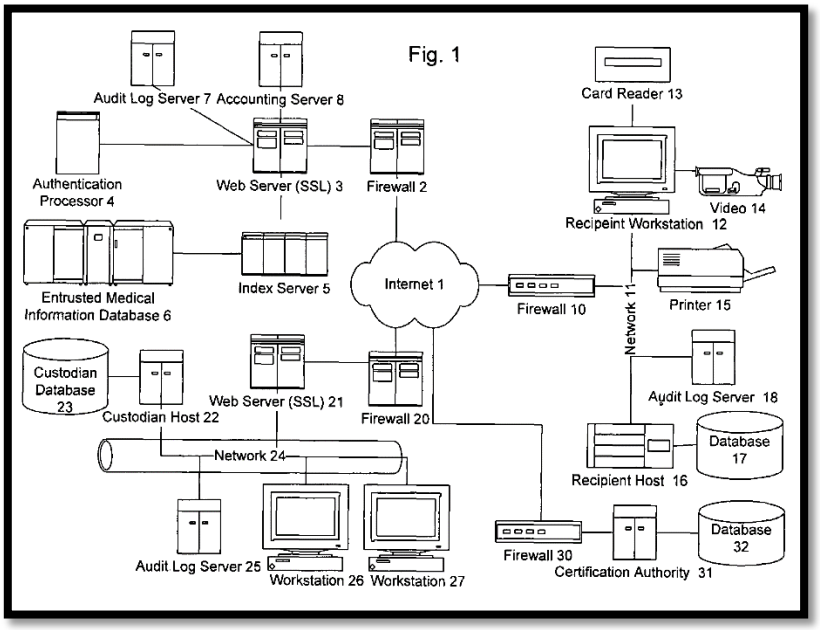
225. The ’368 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

226. The claimed invention in the ’368 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

227. The systems and methods claimed in the ‘368 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

228. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

229. One or more claims of the ’368 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the ‘368 patent illustrates a specific configuration of hardware disclosed in the patent.



‘368 patent, Fig. 1.

2. U.S. Patent No. 8,498,941

230. U.S. Patent No. 8,498,941 (the "'941 patent") entitled, Information Record Infrastructure, System and Method, was filed on July 22, 2009, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '941 patent. A true and correct copy of the '941 patent is attached hereto as Exhibit F. The '941 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer where each record has associated access rules.

231. The '941 patent has been cited by 10 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '941 patent as relevant prior art.

- Red Hat, Inc.
- Intuit, Inc.
- Microsoft Corporation
- Silver Spring Networks, Inc.
- Royal Canadian Mint
- Extendabrain Corporation

232. The '941 patent claims a technical solution to a problem unique to computer networks – controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

233. At the time of the inventions claimed in the '941 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the '941 patent: "The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality." '941 patent, col. 53:35-39.

234. Although the systems and methods taught in the '941 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '941 patent claims were innovative and novel. "Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing

a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions." '941 patent, col. 5:17-20.

235. Further, the '941 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. "[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result." '941 patent, col. 66:21-23.

236. The '941 patent claims are not directed to a "method of organizing human activity," "fundamental economic practice long prevalent in our system of commerce," or "a building block of the modern economy." Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

237. The '941 patent claims are not directed at the broad concept/idea of "managing digital records." Instead, the '941 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

238. The '941 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the '941 patent require the generation of an information polymer - a procedure that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

239. The '941 patent is directed to specific problems in the field of digital record access and transmission.

240. The preemptive effect of the claims of the ‘941 patent are concretely circumscribed by specific limitations. For example, claim 1 of the ‘941 patent requires:

> A method for controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules, comprising:
>
> receiving a request from a requestor, the requestor having at least one attribute;
>
> searching the plurality of automated electronic databases to find records in dependence on the request and on connections between respective records;
>
> applying a set of access rules associated with each found record by at least one automated processor, to produce a set of accessible records;
>
> linking the set of accessible records into an information polymer using a server device;
>
> applying at least one compensation rule by at least one automated processor, dependent on the at least one attribute of the requestor;
>
> logging at least the request for access by at least one automated processor; and
>
> communicating the information polymer to the requestor.

241. The ‘941 patent does not attempt to preempt every application of the idea of controlling access to a digital record over a computer network where the digital records are within a plurality of automated electronic databases.

242. The ‘941 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the ’941 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

243. For example, the ‘941 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The

techniques inform the invention's development but do not, standing alone, fall within the scope of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained
- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.
- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.
- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.
- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.
- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.
- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.
- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network.

This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.

- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).

244. The '941 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

245. The claimed subject matter of the '941 patent is not a pre-existing but undiscovered algorithm.

246. The '941 patent claims require the use of a computer system.

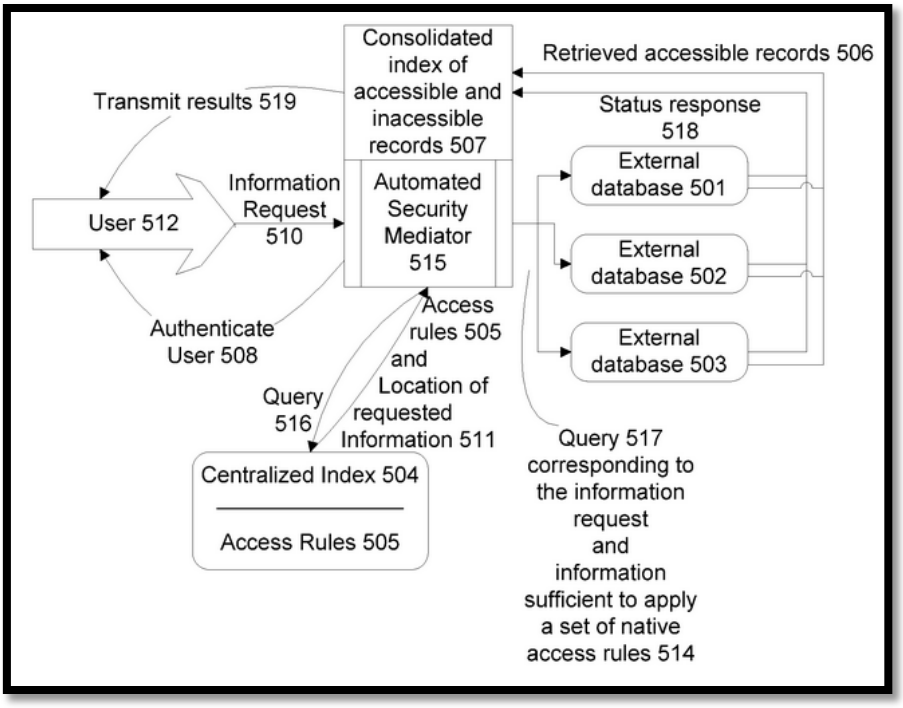
247. The '941 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

248. The claimed invention in the '941 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

249. The systems and methods claimed in the '941 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

250. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

251. One or more claims of the '941 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '941 patent illustrates a specific configuration of hardware disclosed in the patent.



'941 patent, Fig. 6.

3. U.S. Patent No. 8,380,630

252. U.S. Patent No. 8,380,630 (the "'630 patent") entitled, Information Record Infrastructure, System and Method, was filed on May 29, 2010, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '630 patent. A true and correct copy of the '630 patent is attached hereto as Exhibit G. The '630 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer, using a security mediator, where each record has associated access rules.

253. The '630 patent has been cited by ten United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '630 patent as relevant prior art.

- Informatica Corporation
- Electronics and Telecommunications Research Institute ("ETRI")
- J.D. Power and Associates
- CA, Inc.
- Microsoft Corporation

254. The ‘630 patent claims a technical solution to a problem unique to computer networks – controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

255. At the time of the inventions claimed in the ‘630 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the ‘630 patent: “The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality.” ‘630 patent, col. 53:45-49.

256. Although the systems and methods taught in the ‘630 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the ’630 patent claims were innovative and novel. “Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions.” ‘630 patent, col. 5:11-23.

257. Further, the ’630 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. “[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result.” ‘630 patent, col. 66:33-35.

258. The ‘630 patent claims require an automated security mediator (“ASM”).

259. The ‘630 patent claims require the ASM query the automated centralized index (“ACI”) to locate the record information within a plurality of external databases.

260. The ‘630 patent claims require that the ASM generate an index of accessible location record information that is available in a plurality of externally databases.

261. The ‘630 patent claims are not directed to a “method of organizing human activity,” “fundamental economic practice long prevalent in our system of commerce,” or “a building block of the modern economy.” Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

262. The ’630 patent claims are not directed at the broad concept/idea of “managing digital records.” Instead, the ‘630 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

263. The ‘630 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the ’630 patent require an ASM, require the generation of an Automated Centralized Index (“ACI”), require applying the access rules associated with the located requested information (“LRI”), require the ASM query the ACI to locate the record information within the plurality of external databases, and require that the ASM generate an index of LRI accessible in a plurality of external databases - a procedure that overrides the routine and conventional sequence of events in electronic communications.

264. The ‘630 patent is directed to specific problems in the field of digital record access and transmission.

265. The preemptive effect of the claims of the ‘630 patent are concretely circumscribed by specific limitations. For example, claim 1 of the ‘630 patent requires:

A method for security mediation, comprising:

> receiving an information request for information stored within a plurality of external databases (“POEDs”) from a user, wherein the information

request is received by an automated security mediator ("ASM") which is neither an owner nor custodian of the requested information;

authenticating the user;

querying an automated centralized index ("ACI"), maintained by the ASM to locate the requested information within the POEDs, wherein the ACI includes a location and a set of access rules for each entry;

applying the access rules associated with the located requested information ("LRI");

automatically communicating from the ASM to each of the POEDs storing the LRI: a query corresponding to the information request, and information sufficient to apply a set of native access rules of the respective POEDs storing the LRI to further control access to the LRI;

receiving at least a status response from at least one of the POEDs storing the LRI indicating whether the LRI is accessible or inaccessible;

automatically indexing the accessible and inaccessible LRI; and

at least one of:

retrieving, by the ASM, the accessible LRI from the POEDs storing the LRI and communicating, from the ASM to the user a consolidation of the retrieved accessible LRI; and

communicating, from the ASM to the user a consolidated index of the accessible LRI.

266. The '630 patent does not attempt to preempt every application of the idea of controlling access to a digital record over a computer network where the digital records are within a plurality of automated electronic databases.

267. The '630 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the '630 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

268. For example, the ‘630 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The techniques inform the invention’s development but do not, standing alone, fall within the scope of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained
- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.
- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.
- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.
- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.
- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.
- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.

- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).

269. The '630 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

270. The claimed subject matter of the '630 patent is not a pre-existing but undiscovered algorithm.

271. The '630 patent claims require the use of a computer system.

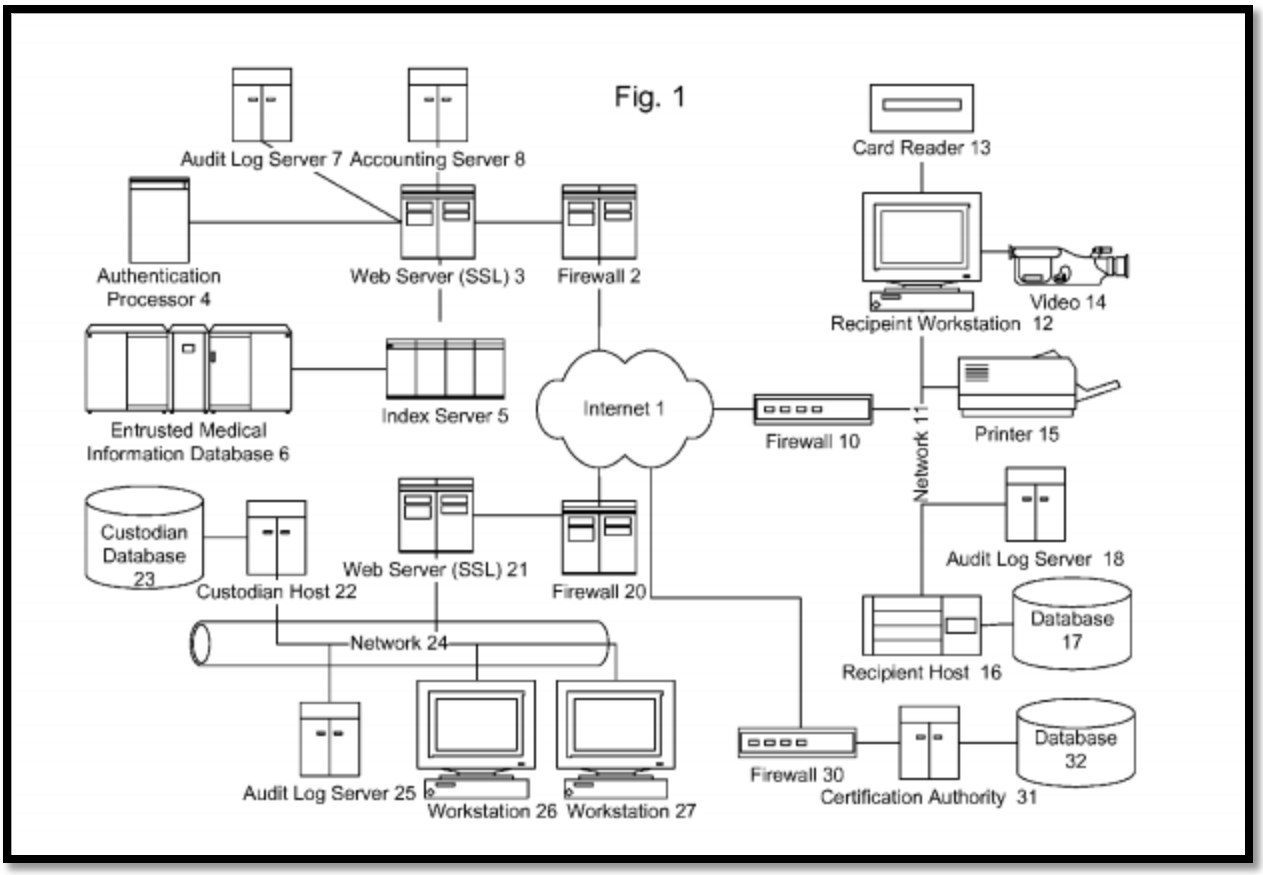
272. The '630 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

273. The claimed invention in the '630 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

274. The systems and methods claimed in the '630 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

275. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

276. One or more claims of the '630 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '630 patent illustrates a specific configuration of hardware disclosed in the patent.



'630 patent, Fig. 1.

4. U.S. Patent No. 8,600,895

277. U.S. Patent No. 8,600,895 (the "'895 patent") entitled, Information Record Infrastructure, System and Method, was filed on February 19, 2013, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the '895 patent. A true and correct copy of the '895 patent is attached hereto as Exhibit H. The '895 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer, using a security mediator, where each record has associated access rules.

278. The '895 patent has been cited by four United States patents and patent applications as relevant prior art.[49] Specifically, patents issued to the following companies have cited the '895 patent as relevant prior art.

[49] Although the '895 patent has only been cited 4 times, the patent applications to which the '895 patent claims priority have been cited by hundreds of companies. U.S. Patent Application 12/790,818 was cited in 45 issued patents and published patent applications, U.S. Patent

- J.D. Power and Associates
- Fujitsu Limited'
- Extendabrain Corporation

279. The '895 patent claims a technical solution to a problem unique to computer networks – controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

280. At the time of the inventions claimed in the '895 patent, electronically structuring and controlling access to protected data in a plurality of external databases presented new and unique issues over the state of the art. As explained in the '895 patent: "The present invention therefore seeks to provide a comprehensive set of technologies to address the full scope of issues presented in implementing a secure and versatile information content infrastructure that respects the rights of content owners and users to privileges, such as confidentiality." '895 patent, col. 53:53-57.

281. Although the systems and methods taught in the '895 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '895 patent claims were innovative and novel. "Existing systems do not create a trust infrastructure, wherein an independent third party represents and serves as an agent for the content owner, implementing a set of restrictive rules for use of content . . . Thus, existing intermediaries do not act in a representative capacity for the content owner, and do not integrate content management functions." '895 patent, col. 5:18-30.

282. Further, the '895 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary. This improves the security of the computer system and allows it to be more efficient. "[B]y consolidating a plurality of institutions [referring to digital records stored in external databases], uniformity, interoperability, cost reductions, and improved security result." '895 patent, col. 66:41-44.

Application was cited in 27 patents and published patent applications, and U.S. Patent Application 09/899,787 was cited in 751 patents and published patent applications.

283. The ‘895 patent claims require controlling access to a plurality of records stored within a plurality of automated external databases.

284. The ‘895 patent claims require an automated centralized index (“ACI”) that includes, for each record, a (1) location identifier (LI), (2) content identifier (CI), and (3) associated set of access rules (ASAR).

285. The ‘895 patent claims require logically associating the releasable accessible record (“AR”) into a linked set of releasable ARs (LAS) and communicating the LAS to the requestor.

286. The ‘895 patent claims are not directed to a “method of organizing human activity,” “fundamental economic practice long prevalent in our system of commerce,” or “a building block of the modern economy.” Instead, they are limited to a concretely circumscribed set of methods and systems that provide a conduit for the authorized transmission of digital records, while maintaining the security of the records against unauthorized access.

287. The ’895 patent claims are not directed at the broad concept/idea of “managing digital records.” Instead, the ‘895 patent claims are limited to a concretely circumscribed set of methods and systems for authorizing and transmitting secure digital records. These methods and systems are technologies unique to the Internet age.

288. The ‘895 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, one or more claims of the ’895 patent require an ACI, require a content identifier (“CI”), require querying ACI to find entries containing CI, require for each accessible record (AR) communicate to the plurality of external databases information sufficient for the external databases to apply native access rules to determine whether the AR is releasable.

289. The ‘895 patent is directed to specific problems in the field of digital record access and transmission.

290. The preemptive effect of the claims of the ‘895 patent are concretely circumscribed by specific limitations. For example, claim 16 of the ‘895 patent requires:

> An apparatus for controlling access to a plurality of records stored within a plurality of automated external databases (“AXES”), comprising:
>
> an automated centralized index (“ACI”), stored in a memory, configured to store an entry for each record consisting of a location identifier (“LI”), an associated set of access rules (“ASAR”), and a content identifier (“CI”);
>
> an input port configured to receive a request from a requestor for access to one or more records stored in the plurality of AXES, wherein the request specifies a CI with which to query the ACI;
>
> at least one processor configured to:
>
> generate a query based on the specified CI (“SCI”);
>
> find entries in the ACI containing the SCI;
>
> for each found entry, apply the ASAR corresponding to the LI to determine if the record stored in a respective one of the AXES corresponding to the LI is accessible;
>
> generate a communication, for communication to the respective one of the AXES storing an accessible record (“AR”), wherein the communication contains information sufficient for the respective one of the AXES storing the AR to apply a set of native access rules (“NAR”) it maintains to determine if the AR is releasable;
>
> form a linked set of releasable ARs by logically associating the releasable ARs; and
>
> generate a communication containing the linked set of releasable ARs; and
>
> at least one communications port configured to communicate:
>
> the generated communication to the respective one of the AXES storing the ARs; and
>
> the linked set of releasable ARs.

291. The ‘895 patent does not attempt to preempt every application of the idea of controlling access to a digital record over a computer network where the digital records are within a plurality of automated electronic databases.

292. The ‘895 patent does not preempt the field of electronically structuring and controlling access to protected data in a plurality of external databases. For example, the ‘895 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and greatly limit its breadth. These inventive elements are

not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

293. For example, the ‘895 patent describes numerous techniques for electronically structuring and controlling access to protected data in a plurality of external databases. The techniques inform the invention’s development but do not, standing alone, fall within the scope of its claims:

- Rights-Based Access to Database Records. U.S. Pat. No. 5,325,294 to Keene, relates to a system that receives and stores the individual's medical information, after the individual is tested to establish this information and the date on which such information was most recently obtained
- Role-Based Access. U.S. Pat. No. 6,023,765 to Kuhn, relates to a role-based access control in multi-level secure systems.
- Secure Networks. U.S. Pat. No. 5,579,393 to Conner, relates to a system and method for secure digital records, comprising a provider system and a payer system.
- Cryptographic Technology. U.S. Pat. No. 5,956,408 to Arnold, relates to an apparatus and method for secure distribution of data. Data, including program and software updates, is encrypted by a public key encryption system using the private key of the data sender.
- Watermarking. U.S. Pat. No. 5,699,427 to Chow, relates to a method to deter document and intellectual property piracy through individualization, and a system for identifying the authorized receiver of any particular copy of a document.
- Computer System Security. U.S. Pat. No. 5,881,225 to Worth, relates to a security monitor for controlling functional access to a computer system. A security monitor controls security functions for a computer system. A user desiring access to the system inputs a user identification and password combination, and a role the user to assume is selected from among one or more roles defined in the system.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, relates to a personal storage device for receipt, storage, and transfer of digital information to other electronic devices has a pocket sized crush resistant casing with a volume of less than about ten cubic centimeters.

- Computer Network Firewall. U.S. Pat. No. 5,944,823 to Jade, relates to a system and method for providing outside access to computer resources through a firewall. A firewall isolates computer and network resources inside the firewall from networks, computers and computer applications outside the firewall.
- Virtual Private Network. U.S. Pat. No. 6,079,020 to Liu, relates to a method and an apparatus for managing a virtual private network operating over a public data network. This public data network has been augmented to include a plurality of virtual private network gateways so that communications across the virtual private network are channeled through the virtual private network gateways.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos relates to a patient and healthcare provider identification system which includes a database of patient and healthcare provider information including the identity of each patient and provider and some identification criteria (such as fingerprint data).

294. The ‘895 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

295. The claimed subject matter of the ‘895 patent is not a pre-existing but undiscovered algorithm.

296. The ’895 patent claims require the use of a computer system.

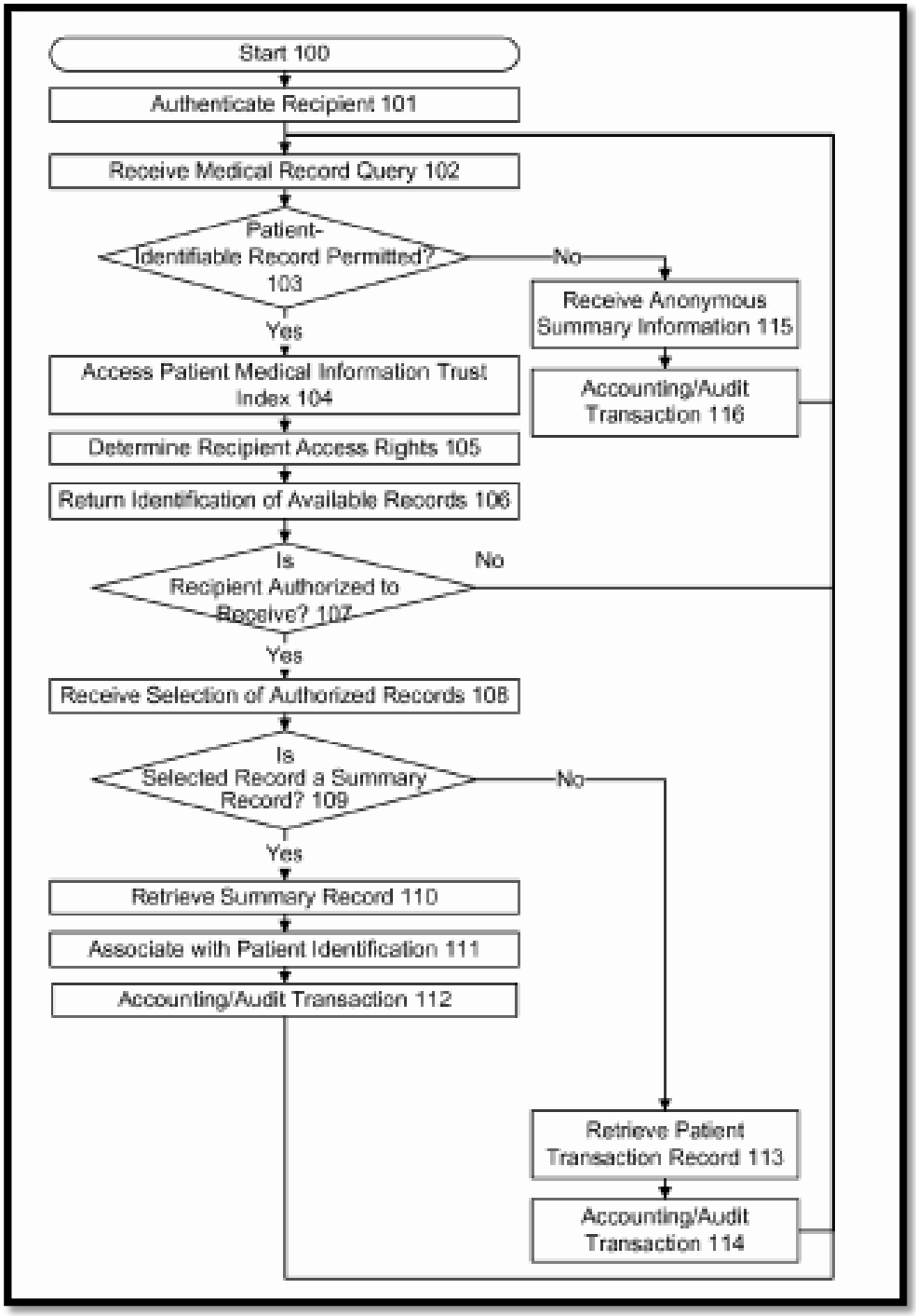
297. The ’895 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

298. The claimed invention in the ’895 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

299. The systems and methods claimed in the ‘895 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

300. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, it involves a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

301. One or more claims of the ’895 patent require a specific configuration of electronic devices, a network configuration, and the use of access rules to secure communications and manage access to secure digital records. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the ‘895 patent illustrates a specific configuration of hardware disclosed in the patent.



‘895 patent, Fig. 4.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 8,316,237

302. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

303. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

304. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security ("HP Voltage").

305. HP makes, sells, offers to sell, imports, and/or uses HP Atalla IPC Enterprise ("HP Atalla IPC").

306. HP makes, sells, offers to sell, imports, and/or uses HP Atalla Cloud Encryption ("HP Atalla Cloud Encrypt").

307. HP builds and offers to its customers the applications and services HP Voltage, HP Atalla IPC, and HP Atalla Cloud Encrypt (collectively, the "HP '237 Products").

308. On information and belief, one or more of the HP '237 Products include encryption technology.

309. On information and belief, one or more of the HP '237 Products enable sending encrypted information through an intermediary where the intermediary is not able to access the unencrypted message.

310. On information and belief, the HP '237 Products are available to businesses and individuals throughout the United States.

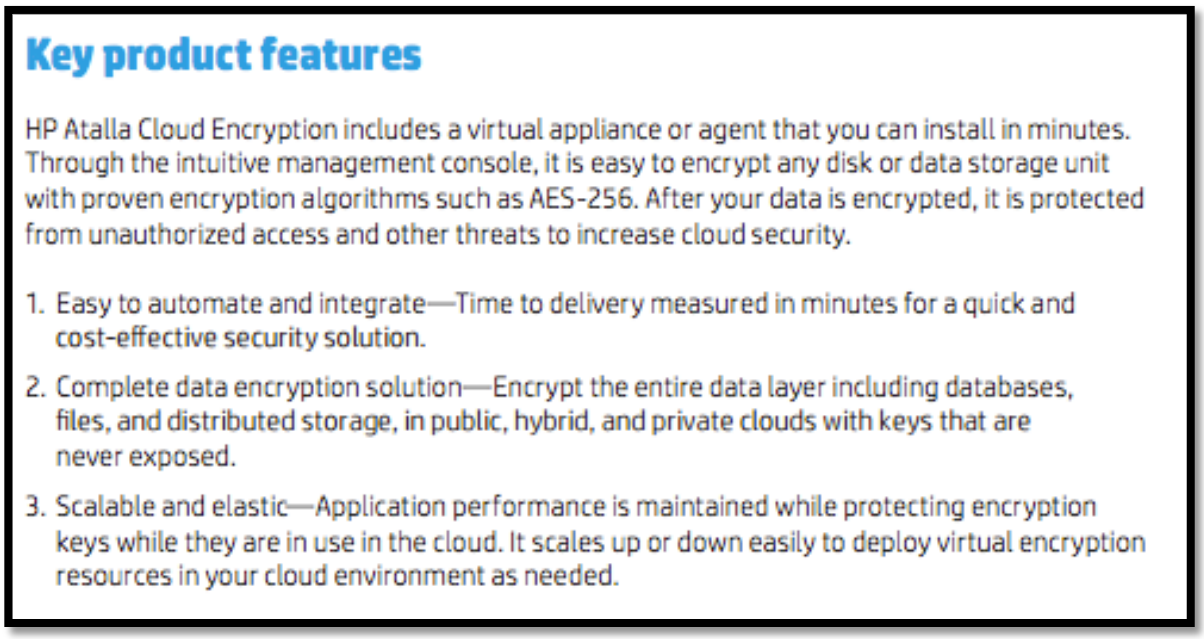
311. On information and belief, the HP '237 Products are provided to businesses and individuals located in the Eastern District of Texas.

312. On information and belief, the HP Atalla Cloud Encrypt system comprises a communication interface device configured to communicate with a plurality of independently operating servers, each communicating server encrypted information, wherein the server

encrypted information is in an encrypted form negotiated between a respective server and an intermediary.

313. On information and belief, HP Atalla Cloud Encrypt system comprises an HP Virtual Appliance. The HP Virtual Appliance comprises a communication interface to, and is configured to communicate with, a plurality of independently operating servers—e.g., a plurality of independently operating servers used for "cloud storage."

314. HP documentation establishes that the HP Atalla Cloud Encrypt system uses AES-256 algorithms to encrypt data.



Key product features

HP Atalla Cloud Encryption includes a virtual appliance or agent that you can install in minutes. Through the intuitive management console, it is easy to encrypt any disk or data storage unit with proven encryption algorithms such as AES-256. After your data is encrypted, it is protected from unauthorized access and other threats to increase cloud security.

1. Easy to automate and integrate—Time to delivery measured in minutes for a quick and cost-effective security solution.
2. Complete data encryption solution—Encrypt the entire data layer including databases, files, and distributed storage, in public, hybrid, and private clouds with keys that are never exposed.
3. Scalable and elastic—Application performance is maintained while protecting encryption keys while they are in use in the cloud. It scales up or down easily to deploy virtual encryption resources in your cloud environment as needed.

HP Atalla Cloud Encryption: Key Management and Security in the Cloud at 3, HP DATA SHEET (2014).

315. On information and belief, HP Cloud Encrypt independently operates servers and communicates server encrypted information, wherein the server encrypted information is in an encrypted form negotiated between a respective server and an intermediary. For example, in the cloud storage use case, each independently operating cloud storage server communicates server ("masked") encrypted storage objects to the HP Virtual Appliance.

316. On information and belief, HP Cloud Encrypt server encrypted storage objects are in an encrypted form negotiated between a respective storage server and an intermediary—the

HP Virtual Key Management (HPVKM) service, comprising the HPVKM server and a HPVKM module on the HP Virtual Appliance.

317. On information and belief, the intermediary in the HP Atalla Cloud Encrypt system has an automated processor configured to communicate with a network using network encrypted information, wherein the network encrypted information is in a form negotiated between a network endpoint and the intermediary, wherein for respective information, the automated processor transcrypts between the server encrypted information and the network encrypted information, substantially without an intermediate representation of the information in a decrypted form.

318. On information and belief, the HP Attala Cloud Encrypt HPVKM module on the HP Virtual Appliance includes an automated processor configured to communicate with a network using network (non-"masked") encrypted information, wherein the network encrypted information is in a form negotiated between a network endpoint (e.g., a user, represented by a distinct client platform) and the intermediary (the HPVKM service).

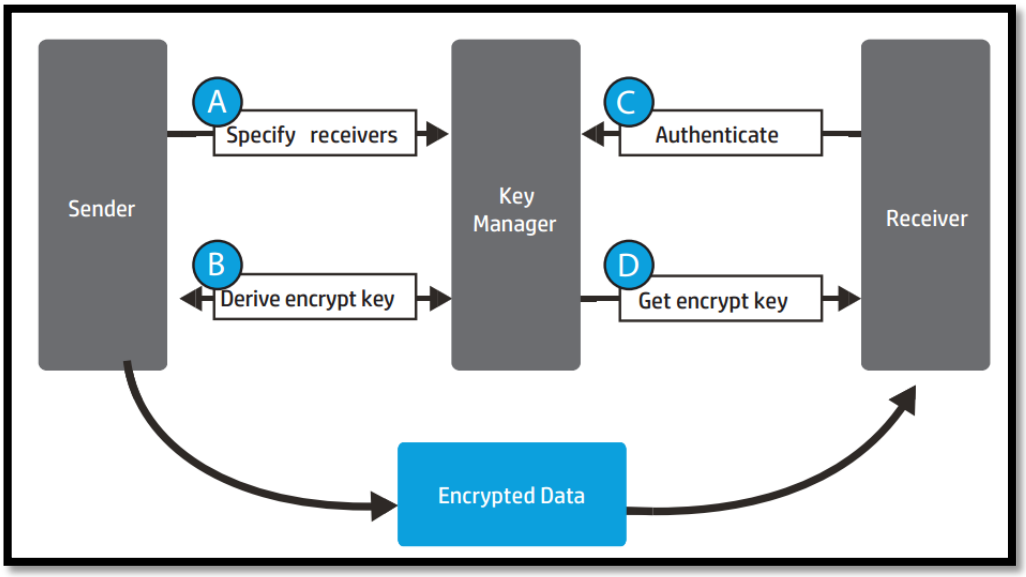
319. On information and belief, the HP Atalla Cloud Encrypt automated processor transcrypts between the server ("masked") encrypted information and the network (non-"masked") encrypted information, substantially without an intermediate representation of the information in a decrypted form.

320. On information and belief, the HP Atalla Cloud Encrypt system comprises an audit database configured to log usage of at least one of the plurality of independently operating servers and the activity of the intermediary.

321. On information and belief, HP Voltage system does not need to contact the key server to get an encryption key. Instead, the encryption key is mathematically derived from the receiver's identity.

322. On information and belief, the HP Voltage key server is able to construct the receiver's decryption key mathematically, eliminating the need for a database at the key server.

323. The below diagram shows how the HP Voltage system manages keys to enable secure communication of data through an intermediary.



The Identity-Based Encryption Advantage: HP Security Voltage at 6, HP TECHNICAL BRIEF (2015).

324. On information and belief, in an initial provisioning/registration process, HP Voltage creates an asymmetric key pair for an authenticated user. The public key is a piece of the user's authenticated identity information (e.g., an email address, verified against a trusted Active Directory server). The private key is a dynamically generated cryptographic counterpart to the email address, such that information encrypted using the email address can be decrypted using the private key. HP Voltage securely sends the private key to the authenticated user, and does not keep a copy of the private key.

325. On information and belief, when the user requests a protected record in the HP Voltage system (and the user and request have been properly authenticated and authorized), HP Voltage retrieves an asymmetric public key—the authenticated email address of the requestor—having an associated asymmetric private key (the previously generated cryptographic counterpart to the email address). HP Voltage associates with the record a wrapper (e.g., a Java crypto

applet) having a respective session key (e.g., a random AES key dynamically generated by HP Voltage). The session key is distinct from the public key and the private key.

326. On information and belief, HP Voltage encrypts and sends the requested digital record to the authenticated, authorized requestor, using the identity-based public key and the random AES session key to encrypt the digital record.

327. On information and belief, HP Voltage enables the requestor to receive the encrypted digital record, and decrypts the encrypted digital record using the requestor's stored private key (the previously-generated cryptographic counterpart to the email address) in conjunction with the wrapper (e.g., the Java crypto applet).

328. On information and belief, HP '237 Products comprise an automated processor, configured to communicate through the automated communication port of and with the memory, to receive the first message, receive the transcryption key, automatically transcrypt the first message into the second message, and to transmit the second message.

329. On information and belief, one or more of the HP '237 Products enable asymmetric encryption.

330. On information and belief, HP has directly infringed and continues to directly infringe the '237 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, the HP '237 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP Voltage Data Security, HP Atalla IPC Encryption, and HP Atalla Cloud Encryption.

331. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP '237 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '237 patent, including at least claims 1, 18 and 19, pursuant to 35 U.S.C. § 271(a).

332. On information and belief, HP also infringes indirectly the '237 patent by active inducement under 35 U.S.C. § 271(b).

333. HP has had knowledge of the ‘237 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the ‘237 patent and knew of its infringement, including by way of this lawsuit.

334. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP ‘237 Products and had knowledge that the inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘237 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ‘237 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP ‘237 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘237 patent, including at least claims 1, 18, and 19, and HP further provides documentation and training materials that cause customers and end users of the HP ‘237 Products to utilize the products in a manner that directly infringe one or more claims of the ‘237 patent. By providing instruction and training to customers and end-users on how to use the HP ‘237 Products in a manner that directly infringes one or more claims of the ‘237 patent, including at least claims 1, 18, and 19, HP specifically intended to induce infringement of the ‘237 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP Products, *e.g.,* through HP’s user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘237 patent.[50] Accordingly, HP 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 ‘237 patent, knowing that such use constitutes infringement of the ‘237 patent.

[50] *See Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

335. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘237 patent.

336. As a result of HP’s infringement of the '237 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP’s infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,181,017

337. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

338. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

339. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security (“HP Voltage”).

340. HP operates the website available at https://www.voltage.com.

341. HP publishes HP Voltage whitepaper, solution briefs, data sheets, and case studies available at https://www.voltage.com/resources/collateral/.

342. On information and belief, one or more of the HP Voltage products include encryption technology.

343. On information and belief, the HP Voltage products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

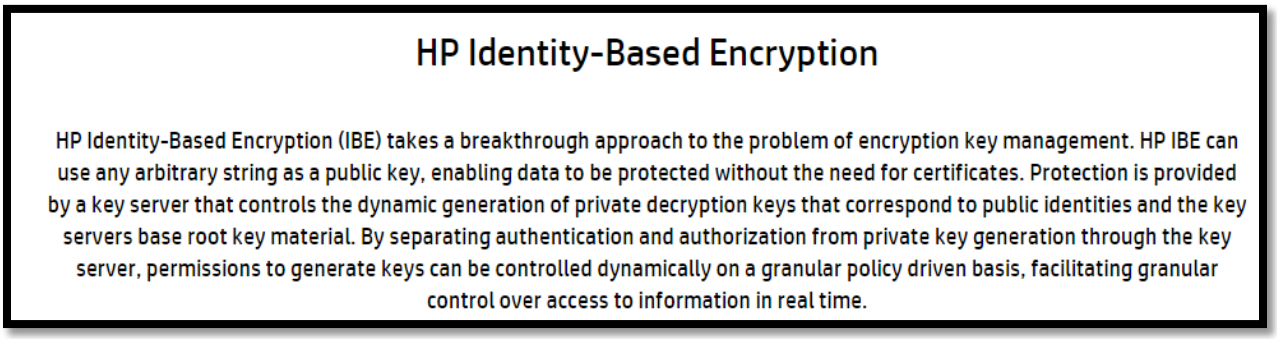
344. On information and belief, HP Voltage is available to businesses and individuals throughout the United States.

345. On information and belief, HP Voltage is available to businesses and individuals located in the Eastern District of Texas.

346. On information and belief, HP Voltage receives information to be processed from a mobile device.

347. On information and belief, HP Voltage utilizes public-private key pairs.

348. On information and belief, HP Voltage documentation represents that HP Voltage enables the synchronization of private data without exposing it to HP.



HP Identity-Based Encryption

HP Identity-Based Encryption (IBE) takes a breakthrough approach to the problem of encryption key management. HP IBE can use any arbitrary string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the dynamic generation of private decryption keys that correspond to public identities and the key servers base root key material. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control over access to information in real time.

HP Security Voltage: HP Identity-Based Encryption, HP VOLTAGE WEBSITE (2015).

349. On information and belief, the HP Voltage system receives information to be processed from a sending device.

350. On information and belief, HP Voltage defines a cryptographic comprehension function (e.g., session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) for information, adapted for making at least a portion of the information incomprehensible.

351. On information and belief, the HP Voltage uses "end-to-end" encryption.

352. On information and belief, in an initial provisioning/registration process, HP Voltage creates an asymmetric key pair for an authenticated user. The public key is a piece of the user's authenticated identity information (e.g., an email address, verified against a trusted Active Directory server). The private key is a dynamically generated cryptographic counterpart to the email address, such that information encrypted using the email address can be decrypted using the private key. HP Voltage securely sends the private key to the authenticated user, and does not keep a copy of the private key.

353. On information and belief, when the user requests a protected record in the HP Voltage system (and the user and request have been properly authenticated and authorized), HP Voltage retrieves an asymmetric public key—the authenticated email address of the requestor—having an associated asymmetric private key (the previously generated cryptographic counterpart to the email address). HP Voltage associates with the record a wrapper (e.g., a Java crypto applet) having a respective session key (e.g., a random AES key dynamically generated by HP Voltage). The session key is distinct from the public key and the private key.

354. On information and belief, HP Voltage encrypts and sends the requested digital record to the authenticated, authorized requestor, using the identity-based public key and the random AES session key to encrypt the digital record.

355. On information and belief, HP Voltage enables the requestor to receive the encrypted digital record, and decrypts the encrypted digital record using the requestor's stored private key (the previously-generated cryptographic counterpart to the email address) in conjunction with the wrapper (e.g., the Java crypto applet).

356. On information and belief, HP Voltage negotiates a new cryptographic comprehension function (e.g., new session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) between two parties using a server intermediary.

357. On information and belief, HP Voltage processes the information to invert the cryptographic comprehension function (e.g., the initial session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) and impose the new cryptographic comprehension function (e.g., the new session-specific cryptographic key, cipher suite, cryptographic mode of operation, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information, without providing the intermediary with sufficient asymmetric key information to decrypt the processed information.

358. On information and belief, HP has directly infringed and continues to directly infringe the ‘017 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, HP Voltage, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP Voltage Data Security.

359. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to HP Voltage, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the ‘017 patent, including at least claim 20, pursuant to 35 U.S.C. § 271(a).

360. On information and belief, HP also infringes indirectly the ‘017 patent by active inducement under 35 U.S.C. § 271(b).

361. On information and belief, HP had knowledge of the ‘017 patent since at least 2009. HP cited the ‘017 patent in U.S. Patent No. 7,610,407 issued on October 27, 2009 and assigned to Hewlett-Packard Development Company.

362. Alternatively, on information and belief, HP has had knowledge of the ‘017 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the ‘017 patent and knew of its infringement, including by way of this lawsuit.

363. On information and belief, HP intended to induce patent infringement by third-party customers and users of HP Voltage and had knowledge that the inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘017 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ‘017 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides HP Voltage, which has the capability of operating in a manner that infringe one or more of the claims of the ‘017 patent, including at least claim 20, and HP further provides documentation and training materials that cause customers and end users of HP Voltage to utilize the products in a manner that directly infringe one or more claims of the ‘017 patent, including at

least claim 20. By providing instruction and training to customers and end-users on how to use HP Voltage in a manner that directly infringes one or more claims of the '017 patent, including at least claim 20, HP specifically intended to induce infringement of the '017 patent. On information and belief, HP engaged in such inducement to promote the sales of HP Voltage through HP's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '017 patent.[51] Accordingly, HP 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 '017 patent, knowing that such use constitutes infringement of the '017 patent.

364. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '017 patent.

365. As a result of HP's infringement of the '017 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HPs infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT III
INFRINGEMENT OF U.S. PATENT NO. 7,869,591

366. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

367. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

368. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security ("HP Voltage").

369. HP makes, sells, offers to sell, imports, and/or uses HP Atalla IPC Enterprise ("HP Atalla IPC").

[51] *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

370. HP makes, sells, offers to sell, imports, and/or uses HP Atalla Cloud Encryption ("HP Atalla Cloud Encrypt").

371. HP builds and offers to its customers the applications and services HP Voltage, HP Atalla IPC, and HP Atalla Cloud Encrypt (collectively, the "HP '591 Products").

372. On information and belief, one or more of the HP '591 Products include encryption technology.

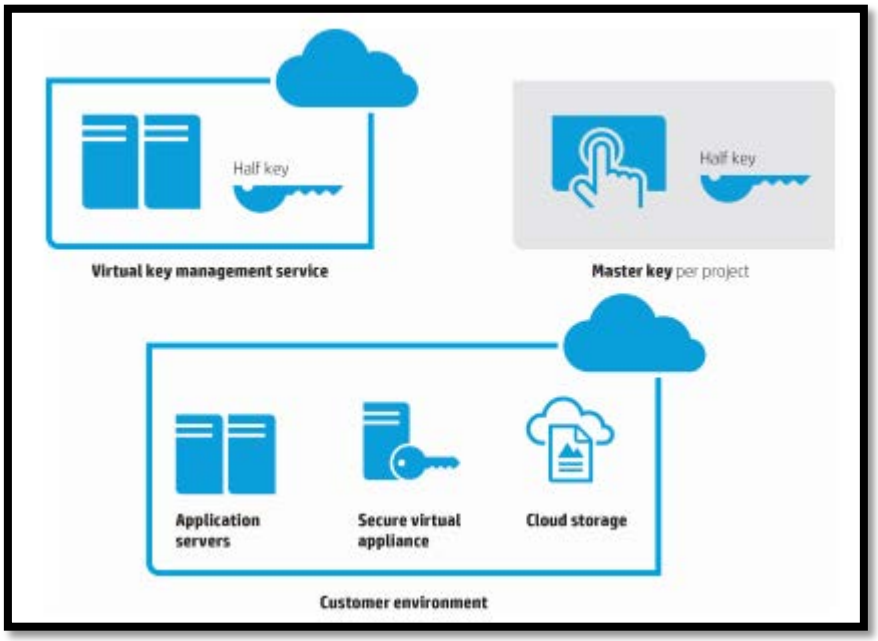
373. On information and belief, one or more of the HP '591 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

374. On information and belief, the HP '591 Products are available to businesses and individuals throughout the United States.

375. On information and belief, the HP '591 Products are provided to businesses and individuals located in the Eastern District of Texas.

376. On information and belief, an HP 591 Product receive and store in a first memory information encrypted based on a first set of cryptographic keys (e.g., a first set of RSA-1280 asymmetric keys), a first portion (e.g., a private key portion) of the first set of cryptographic keys having been employed to produce the encrypted information and a second portion (e.g., a public key portion) of the first set of cryptographic keys being required to decrypt the information encrypted with the first portion of the first set of cryptographic information (e.g., the first set of RSA-1280 asymmetric keys).

377. The below schematic shows the exchange of keys in HP Atalla Cloud Encrypt.



HP Atalla Cloud Encryption: Securing Data In The Cloud at 5, HP TECHNICAL WHITE PAPER (2014).

378. On information and belief, one or more of the HP '591 Products receives and stores in a second memory (e.g., privileged memory dedicated to cryptographic key storage and/or manipulation) a first portion (e.g., a public key portion) of a second set of cryptographic keys (e.g., a second set of RSA-1280 asymmetric keys), having a corresponding second portion (e.g., a private key portion) being required for decryption of a message encrypted using the first portion of the second set of cryptographic keys (e.g., the public key portion of the second set of RSA-1280 asymmetric keys).

379. On information belief, one or more of the HP '591 Products negotiate a set of session keys (e.g., RSA and/or AES session keys) through a communications port.

380. On information and belief, the HP '591 Products, without requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcrypted information, generate a transcryption key for transforming the received encrypted information to transcrypted information.

381. On information and belief, one or more of the HP '591 Products generates a transcryption key for transforming the received encrypted information to transcrypted

information, in dependence on at least information representing the second portion of the first set of cryptographic keys (e.g., information representing the public key portion of the first set of RSA-1280 asymmetric cryptographic keys), information representing the first portion of the second set of cryptographic keys (e.g., information representing the public key portion of the second set of RSA-1280 asymmetric cryptographic keys), and a first portion of the set of session keys (e.g., a first portion of the set of RSA and/or AES session keys).

382. On information and belief, the HP '591 Products transcrypt information by authenticating a remote system and communicating the transcryption key to the authenticated remote system.

383. On information and belief, the HP '591 Products transcrypt information wherein the first set of cryptographic keys is associated with a first party, the second set of cryptographic keys is associated with a second party, and the method is conducted without exchanging cryptographic information between the first party and second party sufficient for decrypting the encrypted information or comprehending the transcrypted information.

384. On information and belief, the HP '591 Products transcrypt information where the set of session keys is dynamically generated for use in conjunction with a communication session, and the transcryption key and the second set of cryptographic keys together provide insufficient information to determine key components of the first set of cryptographic keys.

385. On information and belief, the HP '591 Products transcrypt information wherein the session keys are negotiated through the communication port with an intended recipient of the transcrypted information.

386. On information and belief, the HP '591 Products' session keys are negotiated through a communication port with an intended recipient of the transcrypted information.

387. On information and belief, HP has directly infringed and continues to directly infringe the '591 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, the HP '591 Products, which include infringing encryption technologies. Such products and/or services

include, by way of example and without limitation, HP Voltage Data Security, HP Atalla IPC Enterprise, HP Atalla Cloud Encryption.

388. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP '591 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '591 patent, including at least claim 13 pursuant to 35 U.S.C. § 271(a).

389. On information and belief, HP also infringes indirectly the '591 patent by active inducement under 35 U.S.C. § 271(b).

390. HP has had knowledge of the '591 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the '591 patent and knew of its infringement, including by way of this lawsuit.

391. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP '591 Products and had knowledge that the inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the HP '591 Products would infringe the '591 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '591 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP '591 Products that have the capability of operating in a manner that infringe one or more of the claims of the '591 patent, including at least claim 13, and HP further provides documentation and training materials that cause customers and end users of the HP '591 Products to utilize the products in a manner that directly infringe one or more claims of the '591 patent. By providing instruction and training to customers and end-users on how to use the HP '591 Products in a manner that directly infringes one or more claims of the '591 patent, including at least claim 13, HP specifically intended to induce infringement of the '591 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP Products, *e.g.*, through HP's user manuals, product support, marketing materials, and training

materials to actively induce the users of the accused products to infringe the '591 patent.[52] Accordingly, HP 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 '591 patent, knowing that such use constitutes infringement of the '591 patent.

392. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '591 patent.

393. As a result of HPs infringement of the '591 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP's infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT IV
INFRINGEMENT OF U.S. PATENT NO. 8,904,181

394. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

395. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

396. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security ("HP Voltage").

397. HP makes, sells, offers to sell, imports, and/or uses HP Atalla IPC Enterprise ("HP Atalla IPC").

398. HP makes, sells, offers to sell, imports, and/or uses HP Atalla Cloud Encryption ("HP Atalla Cloud Encrypt").

[52] *See Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

399. HP builds and offers to its customers the applications and services HP Voltage, HP Atalla IPC, and HP Atalla Cloud Encrypt (collectively, the "HP '181 Products").

400. On information and belief, one or more of the HP '181 Products include encryption technology.

401. On information and belief, one or more of the HP '181 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

402. On information and belief, the HP '181 Products are available to businesses and individuals throughout the United States.

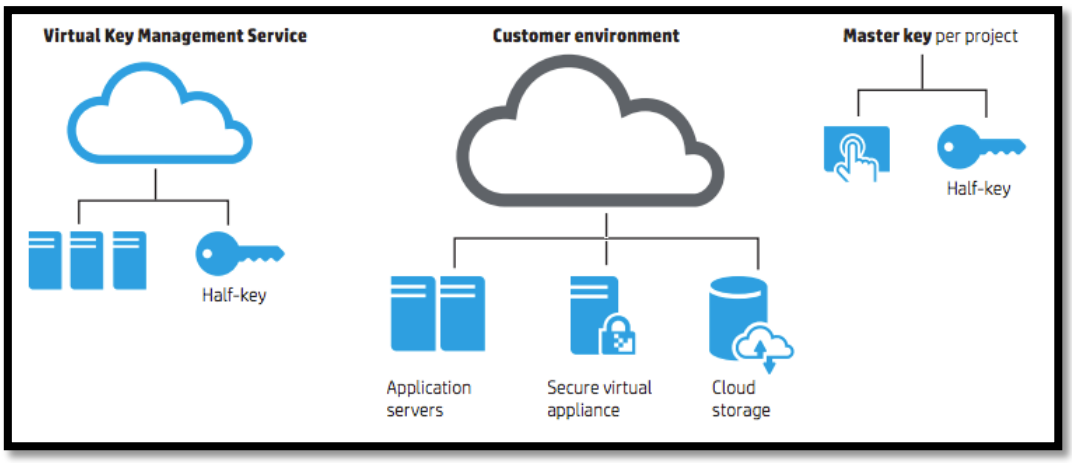
403. On information and belief, the HP '181 Products are provided to businesses and individuals located in the Eastern District of Texas.

404. On information and belief, the HP '181 Products use at least one key handler comprising an interface to a memory which stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair.

405. On information and belief, the HP '181 Products include a key handler that comprises an interface to a memory which stores a plurality of encrypted records (e.g., encrypted record), each encrypted record having an associated asymmetric encryption key pair (e.g., an associated RSA-1280 asymmetric key pair) and being encrypted with a first component (e.g., a private key component) of the associated asymmetric encryption key pair.

406. On information and belief, the HP Atalla Cloud Encrypt system comprises a key handler. For example, the HP Atalla Cloud Encrypt system includes logic and hardware for securely storing and managing customers' cryptographic keys in the cloud.

407. The below schematic shows the exchange of keys in HP Cloud Encrypt for communication between two devices.



HP Atalla Cloud Encryption: Key management and Security in the Cloud at 1, HP DATA SHEET (2014).

408. On information and belief, the HP '181 Products use at least one key handler comprising at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to transcrypt the encrypted message to a transcrypted message in an integral process substantially without intermediate decryption, using a transcryption key derived at least in part from the at least one asymmetric session key.

409. On information and belief, HP Atalla Cloud Encrypt comprises an interface to a memory that stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair.

410. On information and belief, each encrypted cryptographic key record in HP Atalla Cloud Encrypt has an associated asymmetric encryption key pair (e.g., an associated ElGamal public key-secret key pair pk_i, sk_i) and is encrypted with a first component of the associated asymmetric encryption key pair.

411. On information and belief, the HP Atalla Cloud Encrypt system comprises at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to transcrypt the encrypted message to a transcrypted message in an

integral process substantially without intermediate decryption, using a transcryption key derived at least in part from the at least one asymmetric session key.

412. On information and belief, the HP Atalla Cloud Encrypt system includes at least one automated processor operating in a privileged processing environment to securely perform the system's most security-sensitive operation: combining keyshares to access the encrypted data store.

413. On information and belief, the HP Atalla Cloud Encrypt system includes at least one privileged-mode automated processor in the HP Atalla Cloud Encrypt module of the security-hardened Porticor Virtual Appliance configured to homomorphically transform two separately-encrypted partial cryptographic key records—the Master Key, received from the user and wrapped with network (non-"masked") ElGamal encryption, and the project key, received through the interface and wrapped with server ("masked") ElGamal encryption—into a single, usable cryptographic.

414. On information and belief, the HP Atalla Cloud Encrypt system enables a homomorphic transcryption process that includes receiving, by the automated processor, a selected encrypted cryptographic key record from the HP Atalla Cloud Encrypt server memory through the interface.

415. On information and belief, the HP Atalla Cloud Encrypt homomorphic transcryption process also includes negotiating at least one asymmetric (ElGamal) session key, which simultaneously allows for homomorphic multiplication (among other operations) and reduces potential exposure from a security breach.

416. On information and belief, the HP Atalla Cloud Encrypt system enables a homomorphic transcryption process that further includes transcrypting the encrypted cryptographic key record to a transcrypted message (i.e., one usable as a cooperative input, together with the transcrypted Master key, to an encryption/decryption operation) in an integral process substantially without intermediate decryption.

417. On information and belief, the HP Atalla Cloud Encrypt system enables a homomorphic transcryption process, which leverages the homomorphic properties of ElGamal asymmetric encryption, and uses a transcryption key derived at least in part from the at least one ElGamal asymmetric session key.

418. On information and belief, the HP Atalla Cloud Encrypt system comprises at least one communication port configured to conduct the negotiation between the user and the HP Atalla Cloud Encrypt server for the at least one asymmetric session key, and to communicate the transcrypted record (e.g., by supplying the resulting cryptographic key to a stream processor for transparent encryption/decryption of cloud data).

419. On information and belief, the HP Atalla Cloud Encrypt virtual appliance is configured to communicate with the HP Atalla Cloud Encrypt server through at least two types of virtual private networks, SSL VPN and IPSec VPN. All connections within the HP Atalla Cloud Encrypt are authenticated and encrypted. At a minimum, SSL/TLS is always enabled, and cannot be turned off. Additionally, HP provides and enables IPSec communications through HP appliances.

420. On information and belief, the HP Atalla Cloud Encrypt system comprises a key handler, wherein the associated asymmetric key pair comprises at least one of an elliptic curve key pair and an ElGamal key pair.

421. On information and belief, HP '181 Products use at least one key handler comprising a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcrypted record.

422. On information and belief, the HP '181 Products' key handler is configured to communicate with the memory through a virtual private network.

423. On information and belief, the HP '181 Products' key handler is enabled to use an associated asymmetric key pair comprising a Diffie-Hellman type key.

424. On information and belief, the HP '181 Products' key handler is enabled to use an associated asymmetric key pair comprising a Rivest-Shamir-Adler type key.

425. On information and belief, the HP ‘181 Products’ key handler is enabled to use an associated asymmetric key pair comprising at least one of an elliptic curve key pair and an ElGamal key pair.

426. On information and belief, HP ‘181 Products use a transcryption key that has as components at least a second asymmetric component of the associated asymmetric key pair, and the at least one asymmetric session key, to result in a transcrypted message encrypted with at least one asymmetric session key.

427. On information and belief, the HP ‘181 Products’ key handler wherein at least one asymmetric session key comprises at least two asymmetric session keys negotiated with at least two respectively different parties, at least one of the two respectively different parties being a non-recipient of the transcrypted record.

428. On information and belief, the HP ‘181 Products’ key handler uses a transcryption key that has as components at least a second component of the associated asymmetric encryption key pair, the at least one asymmetric session key, and a received asymmetric key component, to result in a transcrypted message encrypted with at least one asymmetric session key and the received asymmetric key component.

429. On information and belief, the HP ‘181 Products store encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair, in a database.

430. On information and belief, HP has directly infringed and continues to directly infringe the ‘181 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, the HP ‘181 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP Voltage Data Security, HP Atalla IPC Enterprise, and HP Atalla Cloud Encryption.

431. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP ‘181 Products, HP has injured St. Luke and is

liable to St. Luke for directly infringing one or more claims of the '181 patent, including at least claims 1, 11, and 18, pursuant to 35 U.S.C. § 271(a).

432. On information and belief, HP also infringes indirectly the '181 patent by active inducement under 35 U.S.C. § 271(b).

433. HP has had knowledge of the '181 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the '181 patent and knew of its infringement, including by way of this lawsuit.

434. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP '181 Products and had knowledge that the inducing acts would cause infringement to the possibility that its inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the '181 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '181 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP '181 Products that have the capability of operating in a manner that infringe one or more of the claims of the '181 patent, including at least claims 1, 11, and 18, and HP further provides documentation and training materials that cause customers and end users of the HP '181 Products to utilize the products in a manner that directly infringe one or more claims of the '181 patent. By providing instruction and training to customers and end-users on how to use the HP '181 Products in a manner that directly infringes one or more claims of the '181 patent, including at least claims 1, 11, and 18, HP specifically intended to induce infringement of the '181 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP Products, *e.g.*, through HP's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '181 patent.[53]

[53] *See Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA

Accordingly, HP 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 ‘181 patent, knowing that such use constitutes infringement of the ‘181 patent.

435. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘181 patent.

436. As a result of HP’s infringement of the '181 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP’s infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 7,587,368

437. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

438. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

439. HP makes, sells, offers to sell, imports and/or uses HP Atalla Information Protection and Control (“HP Atalla IPC”).

440. HP makes, sells, offers to sell, imports, and/or uses HP Connected MX Mobile Information Managements (“HP MX”).

441. HP makes, sells, offers to sell, imports, and/or uses HP Autonomy Products for Compliance (HP Records Manager, HP Worksite Records Manager, HP Consolidated Archive, and HP DigitalSafe) (collectively, “HP Autonomy Compliance”).

442. HP makes, sells, offers to sell, imports, and/or uses HP LiveVault (“HP LiveVault”).

SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013)..

443. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security products (HP Voltage SecureData, HP Voltage SecureFile, HP Voltage SecureMail) (collectively, "HP Voltage DS").

444. HP makes, sells, offers to sell, imports, and/or uses HP Atalla IPC, HP MX, HP Autonomy Compliance, HP LiveVault, and HP Voltage DS (collectively, "HP '368 Products").

445. On information and belief, the HP MX stores data in the cloud data stores (e.g., NoSQL databases).

446. On information and belief, the HP MX system stores electronic information at rest using an AES session key.

447. On information and belief, the HP MX security intermediary negotiates a session key with a requesting user, and sets up a session- and user/client-specific encryption context for the data logically and mathematically related to at least a user/client-specific public key (the user/client has the private component) and the session key. The service securely logs all requests, responses, and end-user actions on protected information via an audit subsystem.

448. On information and belief, HP documentation states that HP Atalla IPC protects data by uniquely embedding protection within the data itself, at the moment of creation or initial access of the information in its unstructured form.[54]

449. On information and belief, HP documentation states that HP Atalla IPC is a full-service Information Rights Management process for the HP Atalla enterprise private cloud.

450. On information and belief, HP Voltage in an initial provisioning/registration process, creates an asymmetric key pair for an authenticated user. The public key is a piece of the user's authenticated identity information (e.g., an email address, verified against a trusted Active Directory server). The private key is a dynamically generated cryptographic counterpart to the email address, such that information encrypted using the email address can be decrypted

[54] *See HP Atalla Information Protection and Control Family Summary* at 2, HP DATA SHEET (2015).

using the private key. HP Voltage securely sends the private key to the authenticated user, and does not keep a copy of the private key.

451. On information and belief, in the HP Voltage system when the user requests a protected record from HP Voltage (and the user and request have been properly authenticated and authorized), HP Voltage retrieves an asymmetric public key—the authenticated email address of the requestor—having an associated asymmetric private key (the previously generated cryptographic counterpart to the email address). HP Voltage associates with the record a wrapper (e.g., a Java crypto applet) having a respective session key (e.g., a random AES key dynamically generated by HP Voltage). The session key is distinct from the public key and the private key.

452. On information and belief, HP Voltage encrypts and sends the requested digital record to the authenticated, authorized requestor, using the identity-based public key and the random AES session key to encrypt the digital record.

453. On information and belief, HP Voltage receives the encrypted digital record, and decrypts the encrypted digital record using the requestor's stored private key (the previously-generated cryptographic counterpart to the email address) in conjunction with the wrapper (e.g., the Java crypto applet).

454. On information and belief, in the HP Voltage system the Java crypto applet is tied into HP Voltage's secure audit subsystem, such that a successful decrypt method generates a logging event at the requesting client computer. The logging event triggers a notification to the HP Voltage server, which accounts for the decryption in a secure audit log.

455. On information and belief, HP has directly infringed and continues to directly infringe the '368 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the HP '368 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP Atalla IPC, HP MX, HP Autonomy Compliance, HP LiveVault, and HP Voltage DS.

456. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP '368 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '368 patent, including at least claims 1, 78, 133, and 140, pursuant to 35 U.S.C. § 271(a).

457. On information and belief, HP also infringes indirectly the '368 patent by active inducement under 35 U.S.C. § 271(b).

458. HP has had knowledge of the '368 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the '368 patent and knew of its infringement, including by way of this lawsuit.

459. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP '368 Products and had knowledge that the inducing acts would cause infringement to the possibility that its inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the '368 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '368 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP '368 Products that have the capability of operating in a manner that infringe one or more of the claims of the '368 patent, including at least claims 1, 78, 133, and 140, and HP further provides documentation and training materials that cause customers and end users of the HP '368 Products to utilize the products in a manner that directly infringe one or more claims of the '368 patent. By providing instruction and training to customers and end-users on how to use the HP '368 Products in a manner that directly infringes one or more claims of the '368 patent, including at least claims 1, 78, 133, and 140, HP specifically intended to induce infringement of the '368 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP '368 Products, *e.g.*, through HP's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '368

patent.[55] Accordingly, HP 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 '368 patent, knowing that such use constitutes infringement of the '368 patent.

460. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '368 patent.

461. As a result of HP's infringement of the '368 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP's infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 8,498,941

462. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

463. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

464. HP makes, sells, offers to sell, imports, and/or uses HP Connected MX Solution for Mobile Information Management ("HP MX").

465. HP makes, sells, offers to sell, imports, and/or uses HP Autonomy Products for Compliance (HP Records Manager, HP Worksite Records Manager, HP Consolidated Archive, and HP DigitalSafe) (collectively, "HP Autonomy Compliance").

466. HP makes, sells, offers to sell, imports, and/or uses HP LiveVault ("HP LiveVault").

[55] *See e.g.*, Jackie Su, *Data Protection: HP LiveVault 7.75 Cloud Backup and Recovery Service is Here!*, HP BIG DATA BLOG (April 30, 2014); *HP LiveVault: Turnkey, Secure Cloud and Hybrid-Cloud Data Protection*, HP BRIEF (2014); *Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

467. HP makes, sells, offers to sell, imports, and/or uses HP Atalla Information Protection and Control ("HP Atalla IPC").

468. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security products (HP Voltage SecureData, HP Voltage SecureFile, HP Voltage SecureMail) (collectively, "HP Voltage DS").

469. HP makes, sells, offers to sell, imports, and/or uses HP MX, HP Autonomy Compliance, HP LiveVault, HP Atalla IPC, and HP Voltage DS (collectively, "HP '941 Products").

470. On information and belief, HP Voltage DS implements at least per-user licensing and tiered per-request metering to determine compensation to HP and (where applicable) third party developers/vendors.

471. On information and belief, the HP '941 Products search a plurality of automated electronic databases to find records in dependence on the request and on connections between respective records;

472. On information and belief, the HP '941 Products apply a set of access rules associated with each record located within an automated electronic database.

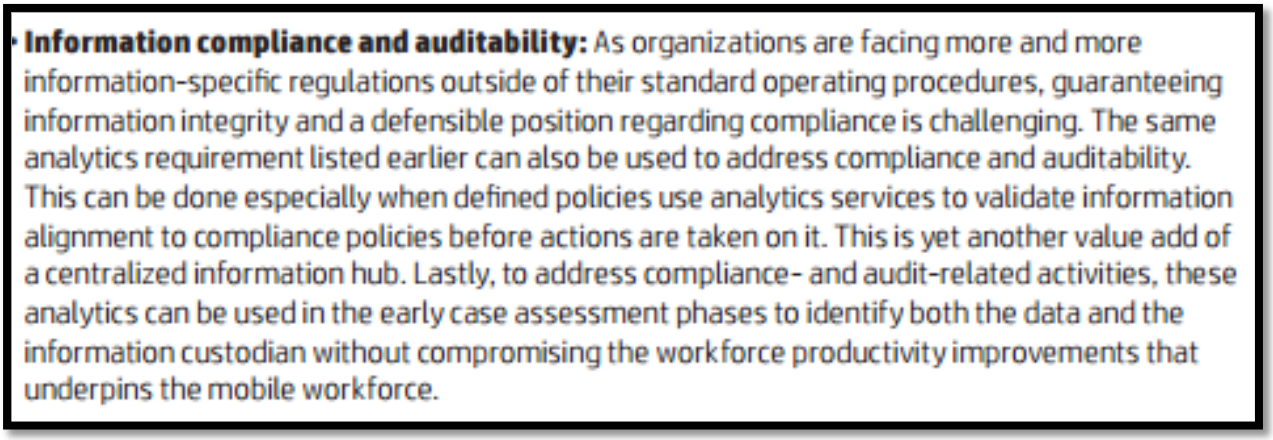
473. On information and belief, HP MX incorporates policy-based endpoint backup with rule-based file synchronization and sharing capabilities.'

474. On information and belief, HP MX is described in HP documentation as employing an information-based policy engine. "It controls more corporate data at a granular level than file types and folder paths. This enables organizations to deliver the appropriate information, which is protected and accessible by users and administrators."[56]

475. On information and belief, HP MX enables role based access control and granular audit trails that log and reports activity as well as information activity such as sharing and information flow.

[56] *HP Connected MX* at 1, HP DATA SHEET (2015).

476. HP MX documentation describes HP MX as enabling "address compliance" and "auditability."

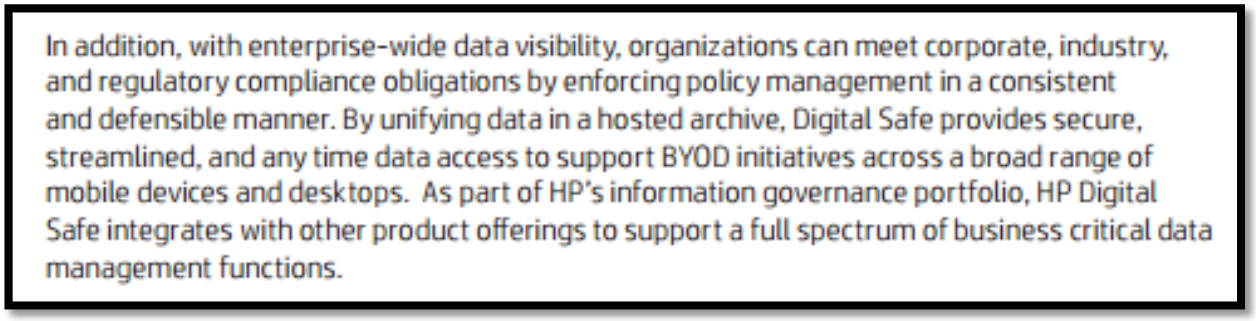


- **Information compliance and auditability:** As organizations are facing more and more information-specific regulations outside of their standard operating procedures, guaranteeing information integrity and a defensible position regarding compliance is challenging. The same analytics requirement listed earlier can also be used to address compliance and auditability. This can be done especially when defined policies use analytics services to validate information alignment to compliance policies before actions are taken on it. This is yet another value add of a centralized information hub. Lastly, to address compliance- and audit-related activities, these analytics can be used in the early case assessment phases to identify both the data and the information custodian without compromising the workforce productivity improvements that underpins the mobile workforce.

Mobile Information Management: An Introduction To The Need For Centrally Managed Endpoint Protection at 7, HP BUSINESS WHITE PAPER (2015).

477. On information and belief, HP Autonomy Compliance products are described in HP documentation as "proactively managing data across an entire enterprise."

478. On information and belief, HP Autonomy Compliance improves the performance of computer networks.



In addition, with enterprise-wide data visibility, organizations can meet corporate, industry, and regulatory compliance obligations by enforcing policy management in a consistent and defensible manner. By unifying data in a hosted archive, Digital Safe provides secure, streamlined, and any time data access to support BYOD initiatives across a broad range of mobile devices and desktops. As part of HP's information governance portfolio, HP Digital Safe integrates with other product offerings to support a full spectrum of business critical data management functions.

Archive Data In The Largest Secure Private Cloud at 6, HP DIGITAL SAFE BROCHURE (2014).

479. On information and belief, HP has directly infringed and continues to directly infringe the '941 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the HP '941 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP MX, HP Autonomy Compliance,

HP LiveVault, and HP Voltage DS, which are covered by one or more claims of the ‘941 patent, including but not limited to claims 8 and 16.

480. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP ‘941 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the ‘941 patent, including at least claims 8 and 16, pursuant to 35 U.S.C. § 271(a).

481. On information and belief, HP also infringes indirectly the ‘941 patent by active inducement under 35 U.S.C. § 271(b).

482. HP has had knowledge of the ‘941 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the ‘941 patent and knew of its infringement, including by way of this lawsuit.

483. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP ‘941 Products and had knowledge that the inducing acts would cause infringement and that its inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘941 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ‘941 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP ‘941 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘941 patent, including at least claims 8 and 16, and HP further provides documentation and training materials that cause customers and end users of the HP ‘941 Products to utilize the products in a manner that directly infringe one or more claims of the ‘941 patent. By providing instruction and training to customers and end-users on how to use the HP ‘941 Products in a manner that directly infringes one or more claims of the ‘941 patent, including at least claims 8 and 16, HP specifically intended to induce infringement of the ‘941 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP ‘941 Products, *e.g.*, through HP’s user manuals, product support, marketing materials, and training materials to

actively induce the users of the accused products to infringe the '941 patent.[57] Accordingly, HP 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 '941 patent, knowing that such use constitutes infringement of the '941 patent.

484. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '941 patent.

485. As a result of HP's infringement of the '941 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP's infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

COUNT VII
INFRINGEMENT OF U.S. PATENT NO. 8,380,630

486. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

487. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

488. HP makes, uses, sells, and/or offers for sale HP Digital Hospital Solution ("HP Digital Hospital").[58]

489. HP makes, sells, offers to sell, imports and/or uses HP Atalla Information Protection and Control ("HP Atalla IPC").

---

[57] *See e.g.*, Jackie Su, *Data Protection: HP LiveVault 7.75 Cloud Backup and Recovery Service is Here!*, HP BIG DATA BLOG (April 30, 2014); *HP LiveVault: Turnkey, Secure Cloud and Hybrid-Cloud Data Protection*, HP BRIEF (2014); *Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

[58] *HP Digital Hospital Solution: Transform Healthcare*, HP SOLUTION OVERVIEW (2013); *see also* Steve Ragan, *Cloud Security: What You Need to Know to Lock it Down*, DICE INSIGHTS WEBSITE (July 9, 2012) (discussing HP Voltage DS as a solution for 'data residency rules.'").

490. HP makes, sells, offers to sell, imports, and/or uses HP Connected MX Mobile Information Managements ("HP MX").

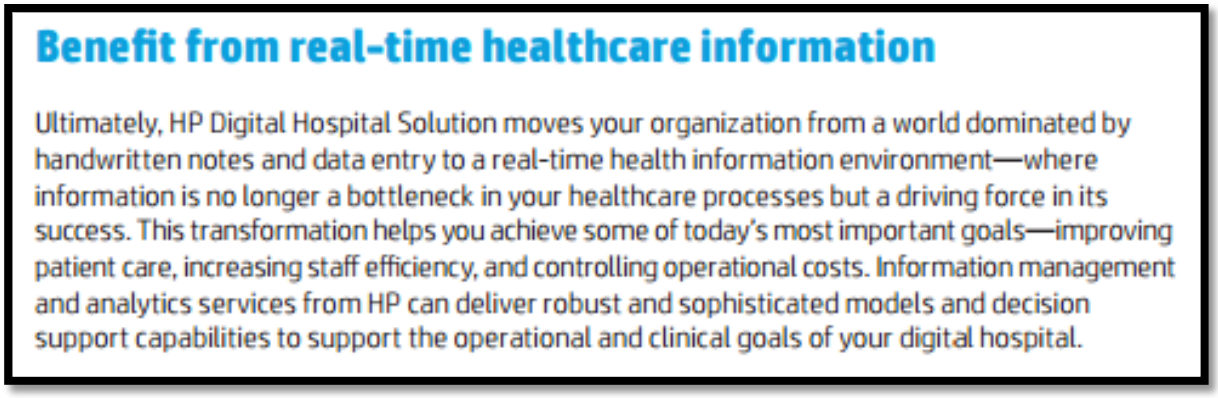
491. HP makes, sells, offers to sell, imports, and/or uses HP Autonomy Products for Compliance (HP Records Manager, HP Worksite Records Manager, HP Consolidated Archive, and HP DigitalSafe) (collectively, "HP Autonomy Compliance").

492. HP makes, sells, offers to sell, imports, and/or uses HP LiveVault ("HP LiveVault").

493. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security products (HP Voltage SecureData, HP Voltage SecureFile, HP Voltage SecureMail) (collectively, "HP Voltage DS").

494. HP makes, sells, offers to sell, imports, and/or uses HP Digital Hospital, HP Atalla IPC, HP MX, HP Autonomy Compliance, HP LiveVault, and HP Voltage DS (collectively, "HP '630 Products").

495. On information and belief, the inventions disclosed in the '630 patent improve the functioning of a computer network as described in HP documentation. These benefits include: reducing "bottlenecks," increased "efficiency," and "controlling costs."



Benefit from real-time healthcare information

Ultimately, HP Digital Hospital Solution moves your organization from a world dominated by handwritten notes and data entry to a real-time health information environment—where information is no longer a bottleneck in your healthcare processes but a driving force in its success. This transformation helps you achieve some of today's most important goals—improving patient care, increasing staff efficiency, and controlling operational costs. Information management and analytics services from HP can deliver robust and sophisticated models and decision support capabilities to support the operational and clinical goals of your digital hospital.

HP Digital Hospital Solution: Transform Healthcare at 4, HP SOLUTION OVERVIEW (2013).

496. On information and belief, the HP '630 Products enable receiving an information request from a plurality of external databases.

497. On information and belief, the HP '630 Products enable authenticating a user. For example, HP MX "enables customers to leverage their own secure source of identify for authentication. Security Assertion Markup Language (SAML)/OAuth support enables integration with a customer-federated authentication strategy to improve security and manageability."[59]

498. On information and belief, the HP '630 Products apply access rules associated with located request information. For example, the HP MX documentation describes its functionality as "deliver[ing] information control and management through policy 'drift' compliance, policy-based protection, ***rule-based file sharing***, and information access scoping policies."[60]

499. On information and belief, the HP '630 Products include functionality for automatically communicating through an automated security mediator to a plurality of external databases. For example, the HP Atalla IPC includes the HP Atalla IPC Exchange Agent which "without disturbing normal business processes, Exchange Agent facilitates secure collaboration with external partners, enforcing security policy even on devices and endpoints not directly protected by the HP Atalla IPC Suite."[61]

500. On information and belief, the HP '630 Products automatically communicate to each of the external databases storing located requested information: a query corresponding to the information request, and information sufficient to apply a set of native access rules of the respective external databases storing the located request information. For example, "HP Atalla IPC Exchange Agent allows companies to benefit from the flexibility of cloud-based services, while keeping their users' identities and security keys safely within the organization."[62]

---

[59] *HP Connected MX, Delivering Mobile Workforce Productivity At The Edge And Business Assurance At The Core* at 2, HP DATA SHEET (2015).
[60] *Id*. at 1 (emphasis added).
[61] *HP Atalla IPC Exchange Agent* at 3, HP DATA SHEET (2015).
[62] *Id*. at 3.

501. On information and belief, the HP ‘630 Products include a security mediator and/or practices methods for security mediation. The HP ‘630 Products receive a request from a user for information records stored within a plurality of external databases (e.g. various external medical record systems) and stores location information and associated access rules for the health information stored in the plurality of external databases.

502. On information and belief, HP has directly infringed and continues to directly infringe the ‘630 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the HP ‘630 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP Digital Hospital, HP Atalla IPC, HP MX, HP Autonomy Compliance, HP LiveVault, and HP Voltage DS.

503. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP ‘630 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the ‘630 patent, including at least claims 1, 8, and 16, pursuant to 35 U.S.C. § 271(a).

504. On information and belief, HP also infringes indirectly the ‘630 patent by active inducement under 35 U.S.C. § 271(b).

505. HP has had knowledge of the ‘630 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the ‘630 patent and knew of its infringement, including by way of this lawsuit.

506. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP ‘630 Products and had knowledge that the inducing acts would cause infringement and that its inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘630 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ‘630 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP ‘630 Products

that have the capability of operating in a manner that infringe one or more of the claims of the '630 patent, including at least claims 1, 8, and 16, and HP further provides documentation and training materials that cause customers and end users of the HP '630 Products to utilize the products in a manner that directly infringe one or more claims of the '630 patent. By providing instruction and training to customers and end-users on how to use the HP '630 Products in a manner that directly infringes one or more claims of the '630 patent, including at least claims 1, 8, and 16, HP specifically intended to induce infringement of the '630 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP '630 Products, *e.g.,* through HP's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '630 patent.[63] Accordingly, HP 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 '630 patent, knowing that such use constitutes infringement of the '630 patent.

507. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '630 patent.

508. As a result of HP's infringement of the '630 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP's infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

[63] *See e.g.*, Jackie Su, *Data Protection: HP LiveVault 7.75 Cloud Backup and Recovery Service is Here!*, HP BIG DATA BLOG (April 30, 2014); *HP LiveVault: Turnkey, Secure Cloud and Hybrid-Cloud Data Protection*, HP BRIEF (2014); *Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

COUNT VIII
INFRINGEMENT OF U.S. PATENT NO. 8,600,895

509. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

510. HP makes, uses, sells, and/or offers for sale in the United States products and/or services for secure three-party communications.

511. HP makes, sells, offers to sell, imports, and/or uses HP Connected MX Solution for Mobile Information Management ("HP MX").

512. HP makes, sells, offers to sell, imports, and/or uses HP Autonomy Products for Compliance (HP Records Manager, HP Worksite Records Manager, HP Consolidated Archive, and HP DigitalSafe) (collectively, "HP Autonomy Compliance").

513. HP makes, sells, offers to sell, imports, and/or uses HP LiveVault ("HP LiveVault").

514. HP makes, sells, offers to sell, imports, and/or uses HP Atalla Information Protection and Control ("HP Atalla IPC").

515. HP makes, sells, offers to sell, imports, and/or uses HP Voltage Data Security products (HP Voltage SecureData, HP Voltage SecureFile, HP Voltage SecureMail) (collectively, "HP Voltage DS").

516. HP makes, sells, offers to sell, imports, and/or uses HP MX, HP Autonomy Compliance, HP LiveVault, HP Atalla IPC, and HP Voltage DS (collectively, "HP '895 Products").

517. On information and belief, HP '895 Products perform a method for controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

518. On information and belief, HP '895 Products enable a system where electronic records have an associated set of access rules.

519. On information and belief, HP ‘895 Products search a plurality of automated electronic databases to find records relating to an entity corresponding to the request, and records having connections to records corresponding to the request, relating to transactions relationships or communications between the entity and another entity.

520. On information and belief, HP ‘895 Products implement metadata based search to enable users and administrator to find critical information “fast.”[64]

521. On information and belief, HP ‘895 Products by at least one automated processor, apply a set of access rules associated with each found record. For example, “HP Connected MX employs an information-based policy engine. It controls more corporate data at a granular level than file types and folder paths. This enables organizations to deliver the appropriate information, which is protected and accessible by users and administrators.”[65]

522. On information and belief, the HP ‘895 Products search a plurality of automated electronic databases to find records in dependence on the request and on connections between respective records.

523. On information and belief, the HP ‘895 Products apply a set of access rules associated with each record located within an automated electronic database.

524. On information and belief, HP MX incorporates policy-based endpoint backup with rule-based file synchronization and sharing capabilities.[66]

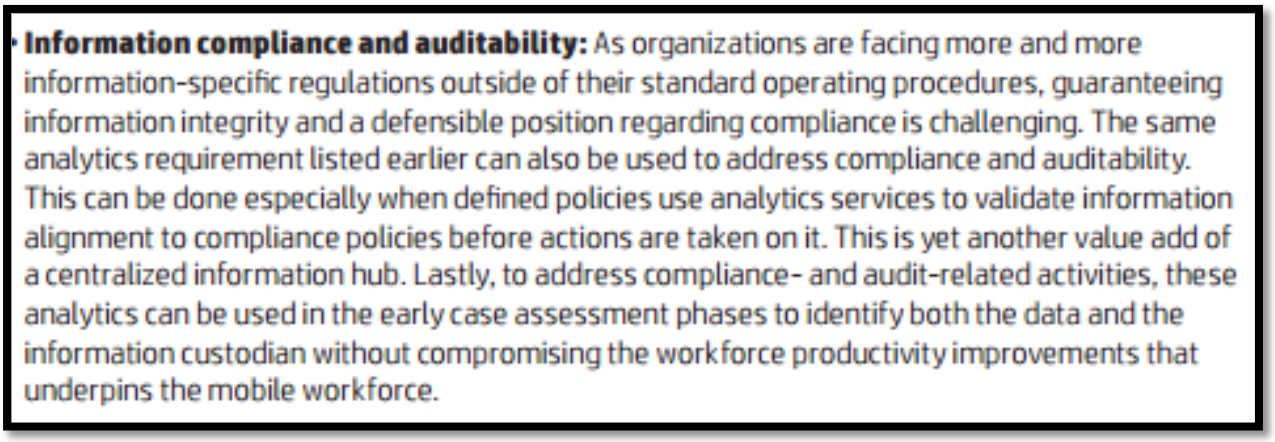
525. On information and belief, HP MX is described in HP documentation as employing an information-based policy engine. “It controls more corporate data at a granular

[64] *HP Connected MX, Delivering Mobile Workforce Productivity At The Edge And Business Assurance At The Core* at 2, HP DATA SHEET (2015) (“User’s search offers a single view of all of a user’s information regardless of the originating device. Responsive information to search criteria can immediately be viewed in place, downloaded, restored, or shared.”).
[65] *Id*. at 1.
[66] *Id.* at 2 (“Improve and enhance organizational productivity with end-user conveniences that do not compromise business assurance requirements.”).

level than file types and folder paths. This enables organizations to deliver the appropriate information, which is protected and accessible by users and administrators."[67]

526. On information and belief, HP MX enables role based access control and granular audit trails that log and reports activity as well as information activity such as sharing and information flow.

527. HP MX documentation describes HP MX as enabling "address compliance" and "auditability."

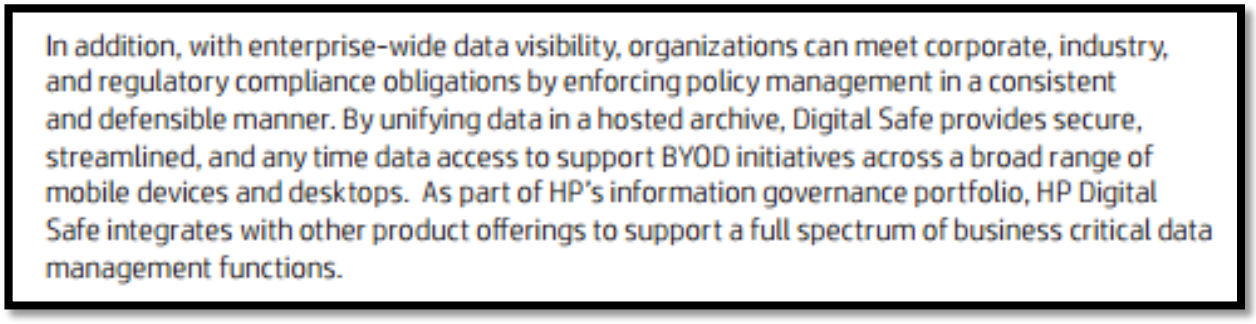


- **Information compliance and auditability:** As organizations are facing more and more information-specific regulations outside of their standard operating procedures, guaranteeing information integrity and a defensible position regarding compliance is challenging. The same analytics requirement listed earlier can also be used to address compliance and auditability. This can be done especially when defined policies use analytics services to validate information alignment to compliance policies before actions are taken on it. This is yet another value add of a centralized information hub. Lastly, to address compliance- and audit-related activities, these analytics can be used in the early case assessment phases to identify both the data and the information custodian without compromising the workforce productivity improvements that underpins the mobile workforce.

Mobile Information Management: An Introduction To The Need For Centrally Managed Endpoint Protection at 7, HP BUSINESS WHITE PAPER (2015).

528. On information and belief, HP Autonomy Compliance products are described in HP documentation as "proactively managing data across an entire enterprise."

529. On information and belief, HP Autonomy Compliance improves the performance of computer networks.



In addition, with enterprise-wide data visibility, organizations can meet corporate, industry, and regulatory compliance obligations by enforcing policy management in a consistent and defensible manner. By unifying data in a hosted archive, Digital Safe provides secure, streamlined, and any time data access to support BYOD initiatives across a broad range of mobile devices and desktops. As part of HP's information governance portfolio, HP Digital Safe integrates with other product offerings to support a full spectrum of business critical data management functions.

Archive Data In The Largest Secure Private Cloud at 6, HP DIGITAL SAFE BROCHURE (2014).

[67] *HP Connected MX* at 1, HP DATA SHEET (2015).

530. On information and belief, HP has directly infringed and continues to directly infringe the ‘895 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for secure three-party communications, including but not limited to, the HP ‘895 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, HP MX, HP Autonomy Compliance, HP LiveVault, and HP Voltage DS.

531. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the HP ‘895 Products, HP has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the ‘895 patent, including at least claims 1, 8, and 16, pursuant to 35 U.S.C. § 271(a).

532. On information and belief, HP also infringes indirectly the ‘895 patent by active inducement under 35 U.S.C. § 271(b).

533. HP has had knowledge of the ‘895 patent since at least service of this Complaint or shortly thereafter, and on information and belief, HP knew of the ‘895 patent and knew of its infringement, including by way of this lawsuit.

534. On information and belief, HP intended to induce patent infringement by third-party customers and users of the HP ‘895 Products and had knowledge that the inducing acts would cause infringement and that its inducing acts would cause infringement. HP specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘895 patent. HP performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the ‘895 patent and with the knowledge, that the induced acts would constitute infringement. For example, HP provides the HP ‘895 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘895 patent, including at least claims 1, 8 and 16, and HP further provides documentation and training materials that cause customers and end users of the HP ‘895 Products to utilize the products in a manner that directly infringe one or more claims of the ‘895 patent. By providing instruction and training to customers and end-users on how to use the HP ‘895 Products in a

manner that directly infringes one or more claims of the ‘895 patent, including at least claims 8 and 16, HP specifically intended to induce infringement of the ‘895 patent. On information and belief, HP engaged in such inducement to promote the sales of the HP ‘895 Products, *e.g.*, through HP’s user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘895 patent.[68] Accordingly, HP 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 ‘895 patent, knowing that such use constitutes infringement of the ‘895 patent.

535. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the ‘895 patent.

536. As a result of HP’s infringement of the '895 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for HP’s infringement, but in no event less than a reasonable royalty for the use made of the invention by HP together with interest and costs as fixed by the Court.

[68] *See e.g.*, Jackie Su, *Data Protection: HP LiveVault 7.75 Cloud Backup and Recovery Service is Here!*, HP BIG DATA BLOG (April 30, 2014); *HP LiveVault: Turnkey, Secure Cloud and Hybrid-Cloud Data Protection*, HP BRIEF (2014); *Choosing an Architecture for Securing Data in The Cloud*, TECHNICAL WHITE PAPER: HP ATALLA CLOUD ENCRYPTION ARCHITECTURE (2015); *HP Atalla Cloud Encryption: Securing Data in the Cloud*, HP DATASHEET (2014); *The Identity-Based Encryption Advantage: HP Security Voltage*, HP TECHNICAL BRIEF (2015); *HP SecureMail: HP Security Voltage*, HP DATA SHEET (2015); David Strom, *Adventure in Secure Mobile eMail*, VOLTAGE SECURITY WHITE PAPER (2013).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff St. Luke respectfully requests that this Court enter:

A. A judgment in favor of Plaintiff St. Luke that HP has infringed, either literally and/or under the doctrine of equivalents, the ‘237 patent, the ‘017 patent, the ‘591 patent, the ‘181 patent, the ‘368 patent, the ‘941 patent, the ’630 patent, and/or the ‘895 patent;

B. An award of damages resulting from HP’s acts of infringement in accordance with 35 U.S.C. § 284;

C. A judgment and order requiring HP to provide accountings and to pay supplemental damages to St. Luke, including, without limitation, prejudgment and post-judgment interest; and

D. Any and all other relief to which St. Luke may show itself to be entitled.

JURY TRIAL DEMANDED

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

Dated: September 22, 2015

Respectfully submitted,

/s/ Elizabeth L. DeRieux

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: 903-236-9800
Facsimile: 903-236-8787
E-mail: ederieux@capshawlaw.com
E-mail: jrambin@capshawlaw.com

OF COUNSEL:

Matt Olavi (CA SB No. 265945)
Brian J. Dunne (CA SB No. 275689)
OLAVI & DUNNE LLP
816 Congress Ave., Ste. 1620
Austin, Texas 78701
Telephone: 512-717-4485
Facsimile: 512-717-4495
E-mail: molavi@olavidunne.com
E-mail: bdunne@olavidunne.com

Dorian S. Berger (CA SB No. 264424)
Daniel P. Hipskind (CA SB No. 266763)
OLAVI & DUNNE LLP
1880 Century Park East, Ste. 815
Los Angeles, CA 90067
Telephone: 213-516-7900
Facsimile: 213-516-7910
E-mail: dberger@olavidunne.com
E-mail: dhipskind@olavidunne.com

Attorneys for St. Luke Technologies, LLC