

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

ST. LUKE TECHNOLOGIES, LLC,

Plaintiff,

v.

MICROSOFT CORPORATION,

Defendant.

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”); 8,566,247 (“the ‘247 patent”); 7,805,377 (“the ‘377 patent”); 7,587,368 (“the ‘368 patent”); 8,498,941 (“the ‘941 patent”); 8,830,630 (“the ‘630 patent”); and 8,600,895 (“the ‘895 patent”) (collectively, the “patents-in-suit”). Defendant Microsoft Corporation (“Microsoft” 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.*

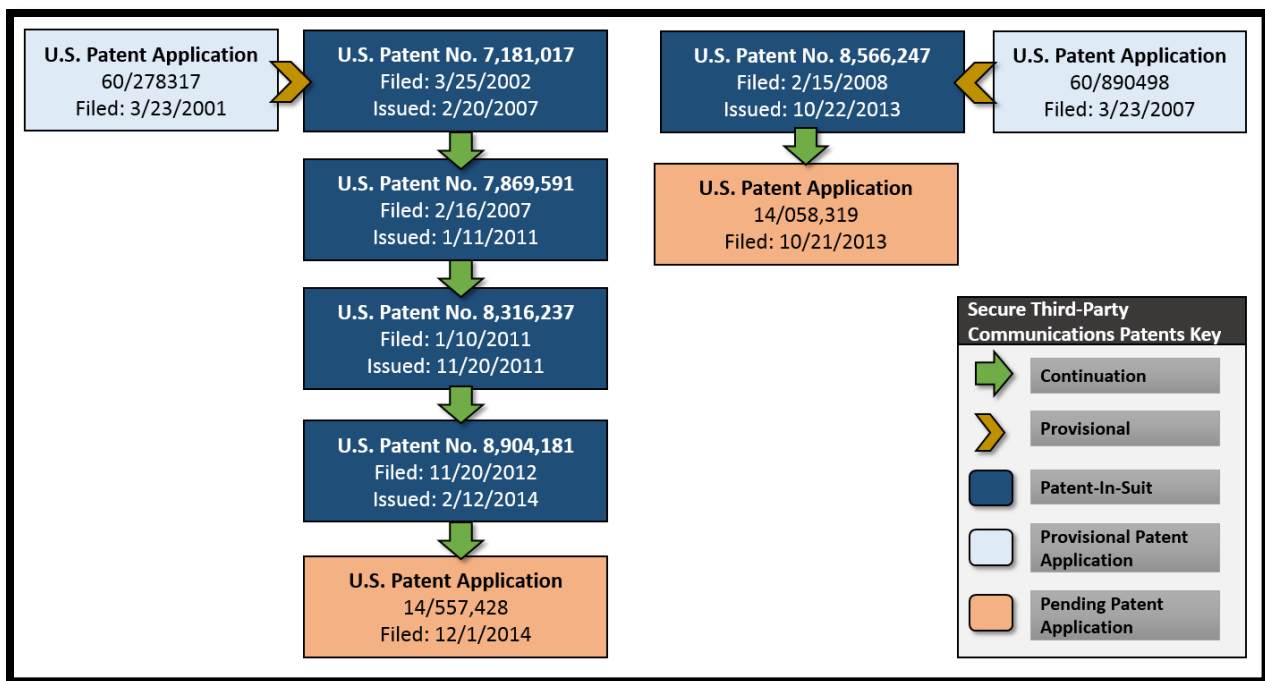
INTRODUCTION

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, Microsoft 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, ‘017, ‘591, ‘181, and ‘247 patents (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 Microsoft infringes.¹



4. Over a decade after Dr. Nagel and his co-inventors conceived of the inventions disclosed in the STPC patents, Microsoft executives have described systems such as Dr. Nagel,

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.

Mr. Felsher, and Mr. Hoffberg's secure third party communications system as "innovative" and "pace" setting.²

[C]onversations have increasingly become less about whether the Cloud can be trusted, and more about the *innovative security and privacy features* and functionality that are being constantly introduced into Microsoft's Cloud services. Many of the CISOs and CIOs I have talked to recently have come to the conclusion that their own datacenters will not keep pace with the level of innovation that they see happening in Microsoft's Cloud services.

Tim Rains (Chief Security Advisor, Microsoft Worldwide Cybersecurity & Data Protection), *Cloud security controls series: Azure Active Directory's Access and Usage Reports*, MICROSOFT CYBER TRUST BLOG (July 13, 2015) (emphasis added).

5. Scott Guthrie, Executive Vice President of Microsoft's Cloud and Enterprise Group, stated the use of encryption technologies is central to Microsoft's business, particularly where data is stored in the "cloud."

Needless to say, all of these capabilities need to be built on a foundation of trust. You know, *Microsoft continues to invest very, very heavily in delivering security*, privacy and transparency initiatives, and *ensuring that our cloud has the broadest set of regulatory compliance regulations* so customers and partners can deliver to any business environment.

Scott Guthrie, WORLDWIDE PARTNER CONFERENCE REMARKS (July 13, 2015) (emphasis added).

6. Recognizing the value of the inventions disclosed in the STPC patents, Microsoft has invested heavily in technology that enables the sharing of electronic data through intermediaries.

Organizations share information. The Microsoft Rights Management services (RMS) offering helps organizations keep their information secure, both inside and outside of the organization, by protecting documents both at rest and in motion. *Information protection is critical and, at this time, Microsoft is redoubling its investment in RMS.*

Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013), available at: <http://blogs.technet.com/b/rms> (emphasis added).

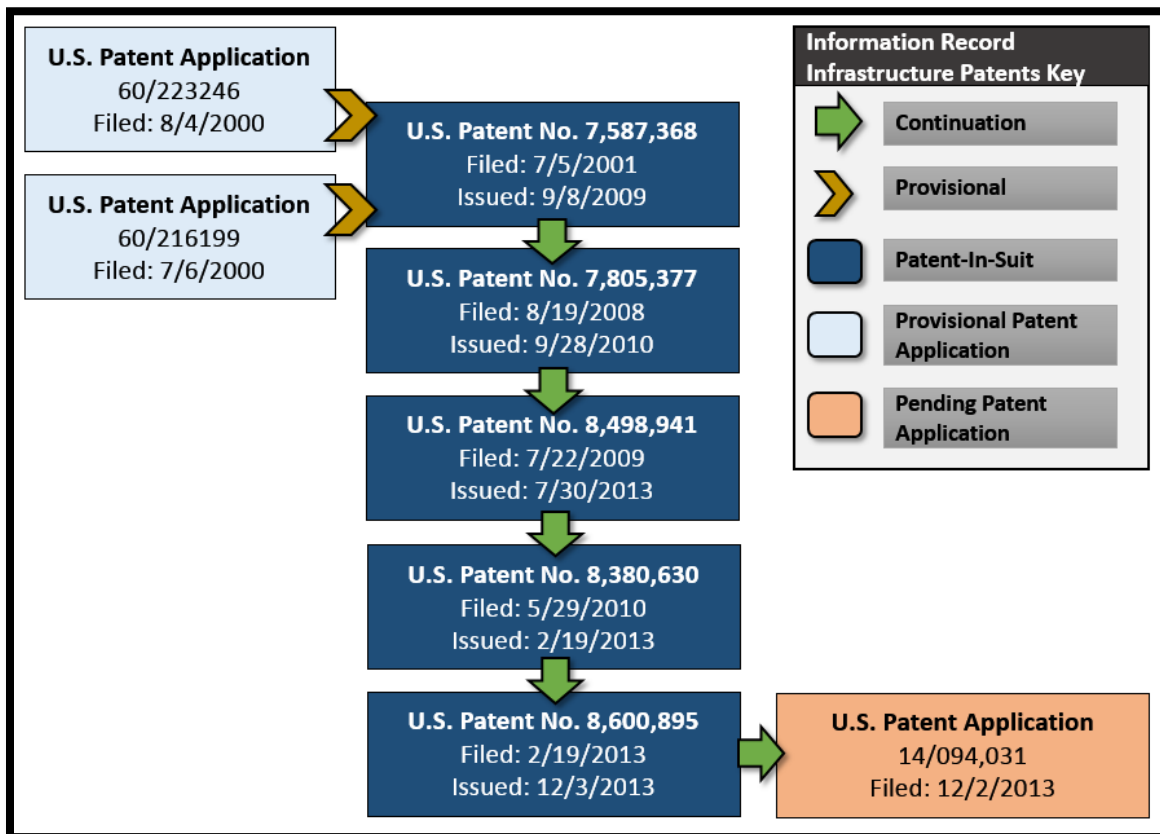
7. Mr. Felsher is the inventor of the '368 patent, the '377 patent, the '941 patent, the '630 patent, and the '895 patent (collectively, "Information Record Infrastructure Patents" or

² The STPC patents have been cited as prior art in six patents and published patent applications assigned to Microsoft. See U.S. Patent Nos. 8,667,292; 8,966,659; 9,087,039; and U.S. Patent App. Nos. 2012/0297198; 2013/0198618; 2014/0283054.

“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.³

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.

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



³ The IRI patents have been cited in 34 patents and published patent applications assigned to Microsoft. See U.S. Patent Nos. 7,162,473; 7,225,187; 7,318,238; 7,382,905; 7,539,682; 7,640,215; 7,676,454; 7,769,707; 7,788,131; 7,792,758; 7,818,335; 8,005,821; 8,140,502; 8,254,891; 8,316,227; 8,417,537; 8,473,612; 8,533,746; 8,689,058; 8,874,930 and U.S. Patent App. Nos. 2004/0098277; 2004/0098277; 2004/0098347; 2004/0267730; 2004/0268139; 2005/0157706; 2005/0175224; 2008/0104104; 2009/0177892; 2010/0125896; 2011/0138190; 2011/0239057; 2012/0029938; 2012/0060035; 2013/0326006.

THE INVENTORS' LANDMARK SECURE COMMUNICATION SYSTEMS

10. Mathematician Dr. Robert Nagel, the named inventor of five 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 Microsoft. 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).⁴

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.⁵

⁴ 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) led 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.

⁵ REUTERS TECHNICAL DEVELOPMENT CHRONOLOGY 1975-1979, THE BARON, July 13, 2015). <http://thebaron.info/archives/technology/reuters-technical-development-chronology-1975-1979>.

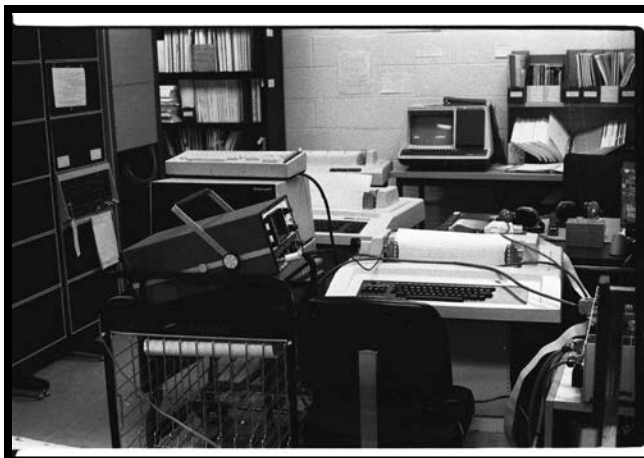
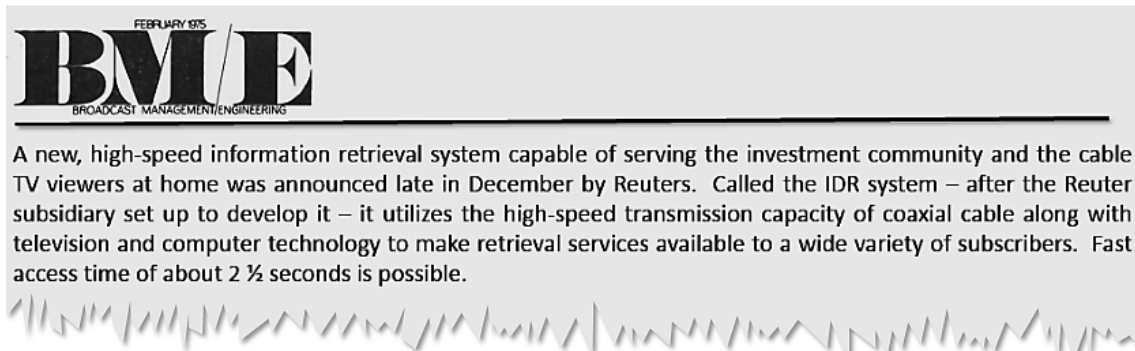


IMAGE OF THE DEC PDP-11/50 SYSTEM, COLUMBIA UNIVERSITY COMPUTING HISTORY ARCHIVE (circa 1976), <http://www.columbia.edu/cu/computinghistory/> (showing an installed PDP-11/50 device that was a component in Dr. Nagel's data distribution system).

13. Reuters sold thousands of information systems modeled on Dr. Nagel's patented inventions.⁶ 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.⁷

⁶ 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.”).

⁷ 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.”).



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.⁸ Publications including Fortune Magazine and ComputerWorld described Dr. Nagel as a “noted computer scientist” for his groundbreaking work⁹—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 Microsoft and many of the world’s largest corporations without attribution or compensation.

⁸ 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.

⁹ See Rick Tetzeli, et al., *Fortune Checks Out 25 Cool Companies For Products, Ideas, And Investments*, FORTUNE MAGAZINE, July 11, 1994.

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.¹⁰ 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 medical records, with wide applicability to the security of data on networks where an intermediary could have access to secure information.

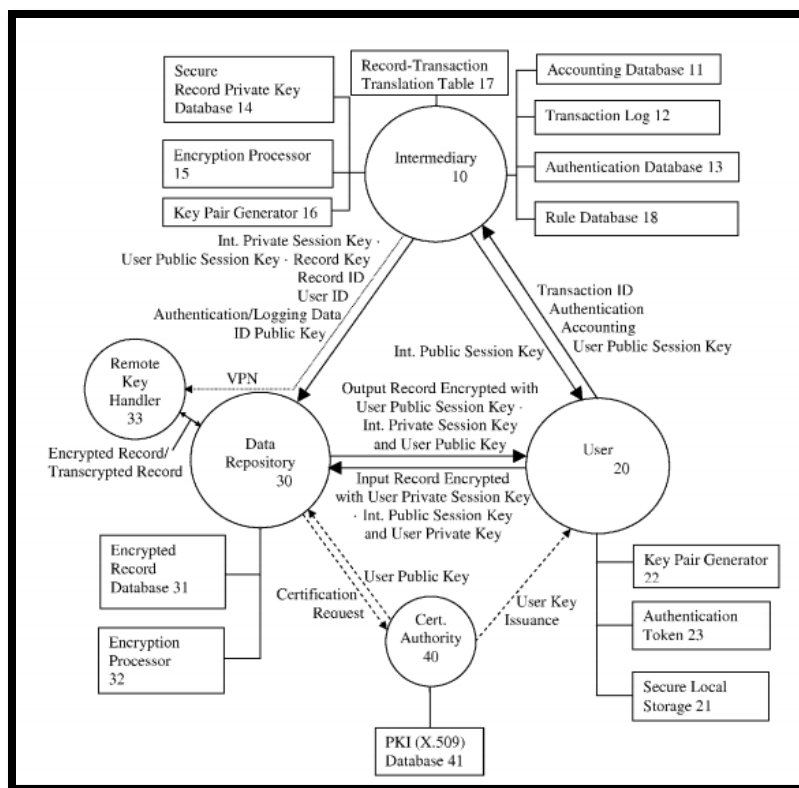
18. The rise of cloud computing (the delivery of on-demand computing resources over a distributed network), has made Dr. Nagel and his co-inventors' insights uniquely valuable. Medical records, financial information, email messages, and other forms of electronic data are now placed on remote servers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

¹⁰ 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/ccun-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.").

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.¹¹ 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.¹²

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

¹¹ During his legal career, Mr. Felsher has been counsel of record on seventeen briefs to the United States Supreme Court.

¹² 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.

- Hewlett-Packard Development Company, L.P.
- Verizon Patent and Licensing Inc.
- Visa U.S.A. Inc.
- Western Digital Technologies, Inc.
- 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

25. The inventions taught in the STPC patents relate to the encryption of data passed through an intermediary and have been recognized by Microsoft as important and valuable:

“[C]loud security is of greater importance than ever before. Customers want to know: ‘Can I trust Microsoft to protect my data?’, ‘Can I meet my organization’s compliance requirements in Microsoft Azure?’, and ‘How do I keep my virtual networks secure?’”¹³

26. The adoption of secure encryption technologies was critical to Microsoft’s current success, particularly in Texas. A 2013 press release from Microsoft directly attributed its ability to sell large cloud computing licenses to its investments in cloud security:

We’ve worked hard to provide security and privacy solutions the State of Texas can trust,” said Michael Donlan, vice president for Microsoft’s State and Local Government business. “The familiarity of Office backed by deep investments in cloud security, privacy and compliance play an important role in how Microsoft is enabling city, state and federal agencies to move to the cloud.”

State of Texas to Improve Communication and Collaboration by Adopting Office 365 for More Than 100,000 State Employees, MICROSOFT NEWS CENTER (February 15, 2013).

¹³ Scott Field, *Innovation in Cloud Security Enables Customers to Move to Microsoft Azure with Confidence*, MICROSOFT AZURE BLOG (November 4, 2014).

27. 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.¹⁴ Companies whose patents cite the IRI patents include:

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

28. 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

¹⁴ 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.

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.



29. 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 Microsoft, St. Luke relies on its intellectual property. In a 2015 complaint filed by Microsoft, alleging mobile device maker Kyocera Corporation infringed its patents, Microsoft detailed the importance it places on its intellectual property.

In the 1990s and 2000s, Microsoft developed numerous inventions which later became critical to the operation of today's small computing devices . . . Although research and development comes at great cost and risk, Microsoft was founded on innovation, and the company continues to choose the path of the innovator. But others have a different approach, waiting for innovators like Microsoft to bear the expense of developing new technologies and then incorporating the most successful inventions into their own products – without permission and without paying for the privilege. ***The patent laws prohibit such conduct***, and Microsoft brings this case to vindicate its rights.

Microsoft Technology Licensing, LLC v. Kyocera Corporation et al., 15-cv-00346 Dkt. No. 1 ¶¶ 2-3 (filed March 6, 2015 W.D. Wash.).

30. Microsoft has asserted its patents in numerous federal courts,¹⁵ including the Eastern District of Texas.¹⁶

¹⁵ *Microsoft Technology Licensing, LLC v. Kyocera Corporation et al.*, 15-cv-00346 (filed March 6, 2015 W.D. Wash.); *Microsoft Corporation v. 5009 8th Ave Corp. et al.*, 05-cv-04388 (filed Sept. 16, 2005 E.D.N.Y.); *Microsoft Corporation v. Alcatel-Lucent*, 06-cv-02696 (filed Dec. 12, 2006 S.D. Cal.); *Microsoft Corporation v. Alcatel-Lucent Enterprise et al.*, 07-cv-00090 (filed Feb. 16, 2007 D. Del.); *Microsoft Corporation v. Barnes & Noble, Inc. et al.*, 11-cv-

31. On information and belief, Microsoft Corporation is a Washington corporation with a principal place of business at 1 Microsoft Way, Redmond, Washington 98052. Microsoft is registered to do business in the State of Texas and it may be served with process by delivering a summons and a true and correct copy of this complaint to its registered agent for receipt of service of process, Corporation Service Company, 211 East Seventh Street, Suite 620, Austin, Texas 78701.

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

- A Microsoft Technology Center located in Irving, Texas.
- A Microsoft South Central District Court office for sales, licensing and product support located in Irving, Texas.
- Offices and retail locations in: Austin, Houston, San Antonio, Friendswood, Frisco, McAllen, Dallas, and Woodland, Texas.
- The supplier of numerous chips and servers used by Microsoft (via Samsung and HP Enterprise Services) are located in or near the Eastern District of Texas.
- Operating datacenters hosting Microsoft Azure in Texas.¹⁷

33. According to Microsoft's website, Microsoft offers infringing products for sale throughout the United States and Canada,¹⁸ including in the Eastern District of Texas. Further,

00485 (filed March 21, 2011 W.D. Wash.); *Microsoft Corporation v Dattel Design and Development Inc., et al.*, 10-cv-02065 (filed Dec. 23, 2010); *Microsoft Corporation v. Motorola Inc.*, 10-cv-01577 (filed Oct. 1, 2010 W.D. Wash.); *Microsoft Corporation v. Salesforce.com, Inc.*, 10-cv-00825 (filed May 18, 2010 W.D. Wash.); *Microsoft Corporation v. Robocast Inc.*, 13-cv-00313 (filed Feb. 25, 2013 D. Del.); *Microsoft Corporation v. TiVo, Inc.*, 10-cv-00240 (filed January 19, 2010 N.D. Cal.).

¹⁶ See *Alcatel USA Sourcing, Inc. v. Microsoft Corporation*, 06-cv-499 Dkt. No. 238 (claims filed on December 10, 2008 E.D. Tex.) (Microsoft asserted U.S. Patent Nos. 6,674,767 and 6,944,273); see also *Alcatel USA Sourcing, Inc. v. Microsoft Corporation*, 06-cv-00500 Dkt. No. 35 (Microsoft's claims filed on May 3, 2007 E.D. Tex.) (Microsoft asserted U.S. Patent Nos. 5,731,844 and 5,758,258).

¹⁷ *Microsoft Azure Regions*, MICROSOFT AZURE WEBSITE (2015), <https://azure.microsoft.com/en-us/regions/>.

¹⁸ *Moving State IT to Microsoft's Cloud for Government*. MICROSOFT GOVERNMENT BLOG (December 11, 2014) ("We've refined what datacenter services mean in Texas and we expect it to continue to expand in terms of the many workloads we can bring online to continuously improve services. Folding Azure Government into these services allows agencies to use a platform they trust.").

Microsoft advertises its infringing products throughout the Eastern District of Texas and claims financial benefits through its conducting of business in Texas, including: (1) accepting monies from the state of Texas relating to Microsoft's engagements with Texas entities;¹⁹ (2) ongoing contracts with the state of Texas;²⁰ (3) Microsoft's agreement to be subject to the laws and jurisdiction of Texas;²¹ (4) Microsoft's certification that it is licensed to conduct business in Texas;²² and (5) Microsoft's agreement (in prior contracts with the state of Texas) to make documentation available to residents of Texas.²³

34. On information and belief, Microsoft has acquired companies relevant to the accused products, including Winternals Software, based in Texas.

¹⁹ *Microsoft Corporation TX DIR Contracting Details*, MICROSOFT WEBSITE (2015), http://www.microsoft.com/en-us/government/texas-dir/default.aspx#fbid=w_pdDRfykFD; *State of Texas to Improve Communication and Collaboration by Adopting Office 365 for More Than 100,000 State Employees*, Microsoft New Center (February 15, 2013) (“We’ve worked hard to provide security and privacy solutions the State of Texas can trust.”); Michael Donlan, *Texas Moves To The Cloud With Microsoft*, MICROSOFT GOVERNMENT BLOG (August 7, 2012). (“Both Texas and Microsoft worked closely together to support the state’s requirements under the Health Insurance Portability and Accountability Act (HIPAA) and CJIS to ensure the highest standards for security and privacy.”).

²⁰ Microsoft Enterprise Agreement with the University of Texas System, University of Texas Campus Enterprise Agreement (2015), <http://uthscsa.edu/business/genservices/mscea.html>; *DIR Contract No. DIR-SDD-1922*, STATE OF TEXAS DEPARTMENT OF INFORMATION RESOURCES CONTRACT FOR PRODUCTS AND RELATED SERVICES MICROSOFT CORPORATION (2015), <http://publishingext.dir.texas.gov/portal/internal/contracts-and-services/Contracts/Contract%20DIR-SDD-1927.pdf>.

²¹ *Id.* at § 15(c) (“This master agreement together with the applicable statement of services will be governed by the laws of the State of Texas.”).

²² *Id.* at § 15(x) (“We certify that we are an entity authorized and validly existing under the laws of our state of organization, and we are authorized to do business in the State of Texas.”).

²³ *Id.* at § 5(b) (“We acknowledge that you are a government agency subject to the Texas Public Information Act. We also acknowledge that you will comply with the Public Information Act.” Pursuant to S.B. 1368 of the 83rd Texas Legislature, Regular Session, Microsoft is required to make any information created or exchanged with the State pursuant to this Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in a format that is accessible by the public at no additional charge to the State.”).

JURISDICTION AND VENUE

35. 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).

36. Upon information and belief, this Court has personal jurisdiction over Microsoft in this action because Microsoft has committed acts within the Eastern District of Texas giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Microsoft would not offend traditional notions of fair play and substantial justice. Defendant Microsoft, directly and/or through subsidiaries or intermediaries (including distributors, retailers, and others), has committed and continues to commit acts of infringement in this District by, among other things, offering to sell and selling products and/or services that infringe the patents-in-suit. Moreover, Microsoft is registered to do business in the State of Texas, and has appointed Corporation Service Company, 211 East Seventh Street, Suite 620, Austin, Texas 78701, as its agent for service of process.

37. Venue is proper in this district under 28 U.S.C. §§ 1391(b)-(d) and 1400(b). Defendant Microsoft 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.

TECHNOLOGY BACKGROUND

38. 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

39. Microsoft prizes systems that provide secure third party communications through an intermediary. Recently, Microsoft has come under criticism for providing end-to-end encryption as an intermediary, such that protected third-party electronic information on Microsoft's intermediary servers is not viewable to Microsoft in unencrypted form.

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>.

40. Microsoft's competitors such as Apple and Oracle have confirmed the importance and value of encryption systems that protect data in the Cloud. Tim Cook, Chief Executive Officer of Apple described the importance that Apple places on secure encryption in the cloud:

Removing encryption tools from our products altogether, as some in Washington would like us to do, would only hurt law-abiding citizens who rely on us to protect their data. The bad guys will still encrypt, it's easy to do and readily available.

Matthew Panzarino, *Apple's Tim Cook Delivers Blistering Speech on Encryption, Privacy*, TECHCRUNCH WEBSITE, June 2, 2015, <http://techcrunch.com/2015/06/02/apples-tim-cook-delivers-blistering-speech-on-encryption-privacy/#.wsy2vn:ybuV>.²⁴

41. 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

²⁴ See also 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> ("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.").

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.

42. 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.

43. 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. Bellovin²⁵ described in a 1996 academic article, contemporaneous to the development of the 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 announced¹ that widespread password monitoring was occurring 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.

²⁵ At the time, Professor Bellovin authored the above referenced article he was a Fellow at AT&T Labs Research.

44. 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.

45. 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.

46. ***Pre-Mechanical Encryption.*** The origin of cryptography has been around since the reign of Pharaohs; however, the problems that “pre-silicon” societies faced were markedly different from those the patents-in-suit are directed at solving. The unique solutions taught by the patents-in-suit 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.²⁶

²⁶ 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*.”).



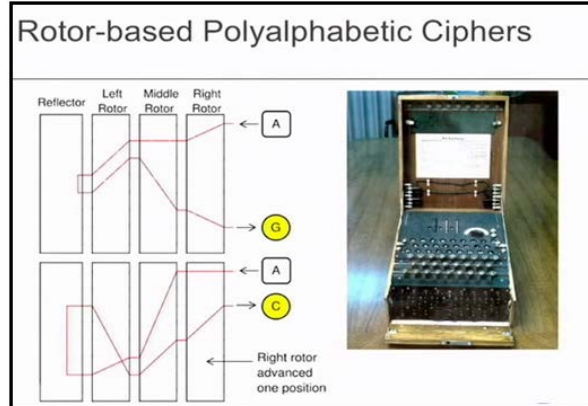
Alexander Stanoyevitch, INTRODUCTION TO CRYPTOGRAPHY WITH MATHEMATICAL FOUNDATIONS AND COMPUTER IMPLEMENTATIONS PRESS (2002).

47. 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.²⁷ 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 attacks that would try various permutations of the code.

48. ***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 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

²⁷ 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.").

of an Enigma device and the “crib” or the symmetric key that was used to program the device.²⁸ Alan Turing (among others) wanted a technique to break Enigma that did not rely on the key, which could (and frequently did) change.²⁹ 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).

49. ***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 a sender 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

²⁸ 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.).

²⁹ 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.).

specifically tailored toward encrypting and decrypting electronic messages communicated using a computer.

50. 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).

51. 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.

52. 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.

53. 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).

54. 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 cryptanalytic 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.

55. 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 and IRI 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.

56. 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).

57. 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 237 (1998).

58. 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 $i-1, \dots, n$, the i^{th} special piece can be individually verified to be correct.

59. 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

60. 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."³⁰ The development of secure communications systems and methods, such as the inventions taught in the STPC patents, was motivated by the unique problems created by the internet where secured data is often transmitted through untrusted intermediaries.

Achieving secure communications in networks has been one of the most important problems in information technology. . . . If there is a private and authenticated channel between two parties, then secure communication between them is guaranteed. However, in most cases, many parties are only indirectly connected, as elements of an incomplete network of private and authenticated channels. ***In other words they need to use intermediate or internal nodes.***

Yvo Desmedt and Yongee Wang, *Perfectly Secure Message Transmission Revisited* at 502, *Advances in Cryptology EUROCRYPT* Vol. 2332 (2002) (emphasis added).

61. 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).

³⁰ 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>.

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

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

62. 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.

The growing demand for cloud computing stems from the need to securely store, manage, share and analyze immense amounts of complex data in many areas, including health care, national security and alternative energy. And although several companies have launched commercially available cloud systems, two areas still need significant improvements, [Dr. Bhavani] Thuraisingham said: the security mechanisms needed to protect sensitive data as well as the capability to process huge amounts of both geospatial data and what's known as semantic Web data.

Investment in Cloud Computing Research Pays Off, UT Dallas Computer Scientists Make Advances in Key Aspects of Growing Field, UNIVERSITY OF TEXAS AT DALLAS NEWS CENTER (April 19, 2011).³¹

³¹ See also Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY Vol. 4(2) (April-June 2010) (“Because of the critical nature of the applications, it is important that clouds be secure. The major security challenge with clouds is that the owner of the data may not have control of where the data is placed.”); Ryan Layfield, Murat Kantarcioglu, and Bhavani Thuraisingham, *Enforcing Honesty in Assured Information Sharing within a Distributed System*, IFIP WG 11.3 CONFERENCE ON

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* at 1, in INFOTECH SEMINAR ADVANCED COMMUNICATION SERVICES (ACS) (2005) (emphasis added).

63. On information and belief, contemporaneous to, and following conception of the inventions disclosed in the STPC patents, academics, and businesses headquartered in Texas actively entered the field of secure encrypted communications. Computer researchers at the University of Texas at Austin founded the Security Research Group. The University of Texas at Dallas founded the Data Security and Privacy Lab, a center for research on security issues raised by dissemination of data over computer networks.

64. Texas based companies incorporated secure communications technologies into numerous products and many of these same companies cite STPC patents in their own patents. Texas based businesses that developed products incorporating secure communications technologies included: HP Enterprise Services, LLC of Plano, Texas; Texas Instruments, Inc. of Dallas, Texas; Rocksteady Technologies, LLC of Austin, Texas; Dell, Inc. of Round Rock,

DATABASE AND APPLICATIONS SECURITY (2007) ("The growing number of distributed information systems such as the internet has created a need for security in data sharing."); Safwan M. Khan and Kevin W. Hamlen, *AnonymousCloud: A Data Ownership Privacy Provider Framework in Cloud Computing* at 170, in PROCEEDINGS OF THE 11TH IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS (June 2012) ("Revolutionary advances in hardware, middleware, and virtual machines over the past few years have elevated cloud computing to a thriving industry . . . A significant barrier to the adoption of cloud services is customer fear of privacy loss in the cloud.").

Texas; AT&T Intellectual Property whose inventors were based in various locations in Texas; Gazzang, Inc. of Austin, Texas, Net.Orange, Inc. of Dallas, Texas; and Futurewei Technologies, Inc. of Plano, Texas. The STPC patents are cited by at least 50 patents that were either initially assigned to or are currently assigned to entities headquartered in Texas.

1. U.S. Patent No. 8,316,237

65. 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 transcribing 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.

66. 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.

67. 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.

68. 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).

69. 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.

- Security was not a major issue, even for Oracle
 - Standard passwords (scott/tiger, system/manager, ...)
 - Oracle standard users were installed and left open (though not at SAP!)
 - There are some recommendations, but not much more.
 - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts, ..., 10.2: CONNECT roles)

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

70. 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.³² “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).

³² See Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) (“The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes.”); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) (“very little work has been devoted to security”); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) (“The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.”).

71. 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 transcribing electronic information that is transmitted over a computer network via an intermediary.

72. 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 transcribing electronic information that is transmitted over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

73. The inventive concepts claimed in the '237 patent are technological, not “entrepreneurial.” For example, transcribing 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.

74. 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*

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].

of Leading Cloud Service Providers, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).³³

75. 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 transcribing 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.

76. 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 cipher text (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

³³ See also Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham. *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) (“The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider’s site.”).

the cipher text. *Id.* In other words, using the same key repeatedly 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.

77. 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 transcription 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 transcription 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 transcription key, automatically transcribe 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 transcription any decrypted representation of the encrypted communication, and the transcription key is employed without revealing any secret cryptographic information usable for decrypting the first message or the second message.

78. 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.

79. 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.

80. 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.

81. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”³⁴ the ‘237 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

82. 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.

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

84. The ‘237 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”³⁵

³⁴ *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).

³⁵ *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); *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015); see also *Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

85. The '237 patent claims require the use of a computer system.

86. 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) (emphasis added).

87. 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.³⁶

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

89. 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

³⁶ 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."³⁷

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 (emphasis added).

90. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, the '237 patent teaches 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."³⁸

91. 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.

92. '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.


93. IBM in its computer reference guides ("redbooks") refers to encryption as "transform[ing] data that is unprotected.

³⁷ 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.").

³⁸ 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).

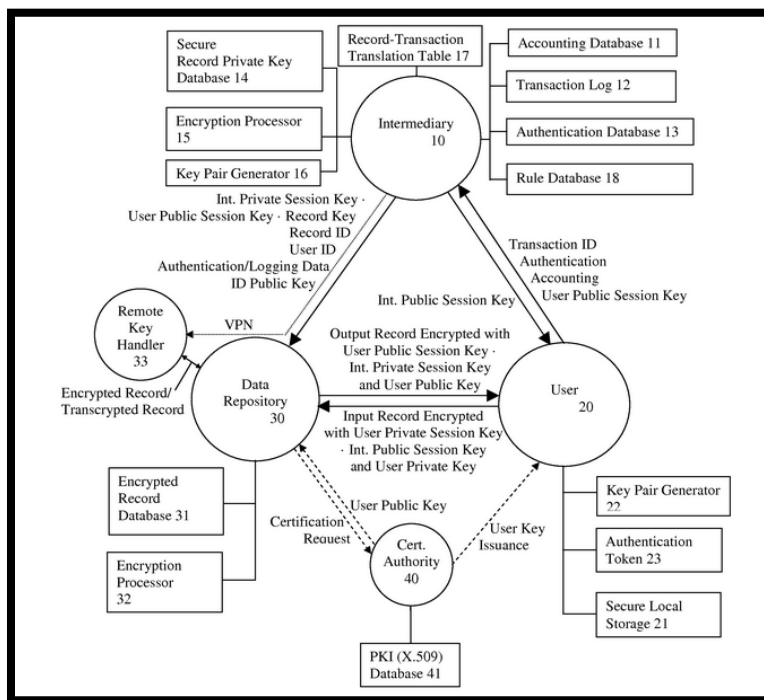
Encryption concepts and terminology

Encryption transforms data that is unprotected, or *plain text*, into encrypted data, or *ciphertext*, by using a *key*. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text.



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

94. 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

95. 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.

96. 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.
- Telecom Italia S.P.A.
- General Electric Company
- Fuji Xerox Co., Ltd.
- Massachusetts Institute Of Technology
- Netapp, inc.
- Koninklijke 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.

97. 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.

98. 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).

99. 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.

Simon Blake-Wilson, *Information Security, Mathematics and Public-Key Cryptography*, in

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.

Designs, Codes and Cryptography, 19, 81 (2000).

100. 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.³⁹ “Third parties, however,

³⁹ See Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) (“The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes.”); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) (“very little work has been devoted to security”); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) (“The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. 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).

101. 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 transcribing electronic information that is transmitted over a computer network via an intermediary.

102. 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 transcribing electronic information that is transmitted over a computer network via an intermediary. This type of method and system is unique to the Internet age.

103. The inventive concepts claimed in the ‘017 patent are technological, not “entrepreneurial.” For example, transcribing 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.

this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.”).

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

- Security was not a major issue, even for Oracle
 - Standard passwords (scott/tiger, system/manager, ...)
 - Oracle standard users were installed and left open (though not at SAP!)
 - There are some recommendations, but not much more.
 - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts, ..., 10.2: CONNECT roles)

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

105. 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).⁴⁰

106. 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

⁴⁰ See also Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham. *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) ("The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.").

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.

107. 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 repeatedly 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.

108. 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.

109. 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.

110. 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.

111. 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.

112. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁴¹ the claims in the ‘017

⁴¹ *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

patent do not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

113. 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

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

115. The ‘017 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁴²

116. 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.” 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) (emphasis added).

WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

⁴² *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); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

117. 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.

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

119. 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.”⁴³

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 (emphasis added).

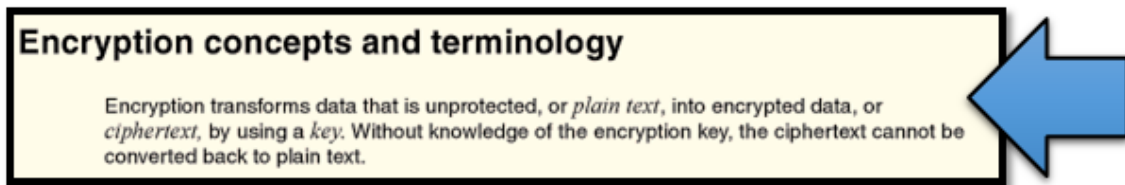
120. The asserted claims do not involve a method of doing business implemented on a computer; instead, they involve a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '017 patent is directed at were new and 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.”⁴⁴

⁴³ 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.”).

⁴⁴ 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).

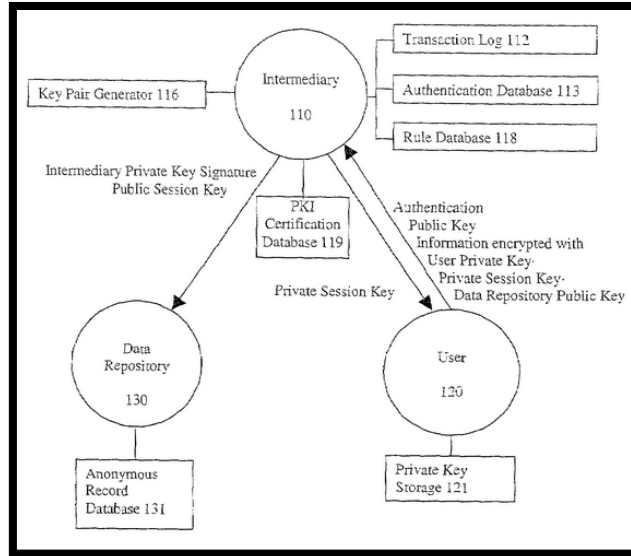
121. The '017 patent claims are not directed to a mathematical relationship or formula. The '017 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

122. 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.)

123. 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.



'017 patent, Fig. 2.

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

124. 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.

125. 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.
- Koninklijke 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.

126. 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.

127. 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.

128. 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).

129. 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).

130. 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.⁴⁵ “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.

⁴⁵ See Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) (“The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes.”); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) (“very little work has been devoted to security”); Elisa Bertino et al., *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) (“The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.”).

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

131. 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 transcribing electronic information that is transmitted over a computer network via an intermediary.

132. 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 transcribing electronic information that is transmitted over a computer network via an intermediary. This type of method and system is unique to the Internet age.

133. The inventive concepts claimed in the '591 patent are technological, not “entrepreneurial.” For example, transcribing 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.

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

- Security was not a major issue, even for Oracle
 - Standard passwords (scott/tiger, system/manager, ...)
 - Oracle standard users were installed and left open (though not at SAP!)
 - There are some recommendations, but not much more.
 - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts, ..., 10.2: CONNECT roles)

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

135. 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*

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].

of Leading Cloud Service Providers, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).⁴⁶

136. 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.

137. 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 cipher text (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 cipher

⁴⁶ See also Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham, *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) (“The emergence of cloud computing has created a paradigm shift by allowing parallel processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider’s site.”).

text. *Id.* In other words, using the same key repeatedly 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.

138. 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 transcribing 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 transcription key for transforming the received encrypted information to transcribed 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) transcribing the stored encrypted information into transcribed information using the transcription key, wherein the generating a transcription key step and the transcribing the encrypted information step are performed without either requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcribed information.

139. 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.

140. 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.

141. 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.

142. 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 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).

143. 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

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

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).

145. The '591 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁴⁸

146. 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.” 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).

147. 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.

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

149. 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

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); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

time the inventions disclosed in the '591 patent were conceived, the use of asymmetric encryption keys was described by Oracle as "relatively new."⁴⁹

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

150. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, they involve 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."⁵⁰

151. 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.


152. '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.

⁴⁹ 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.").

⁵⁰ 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).

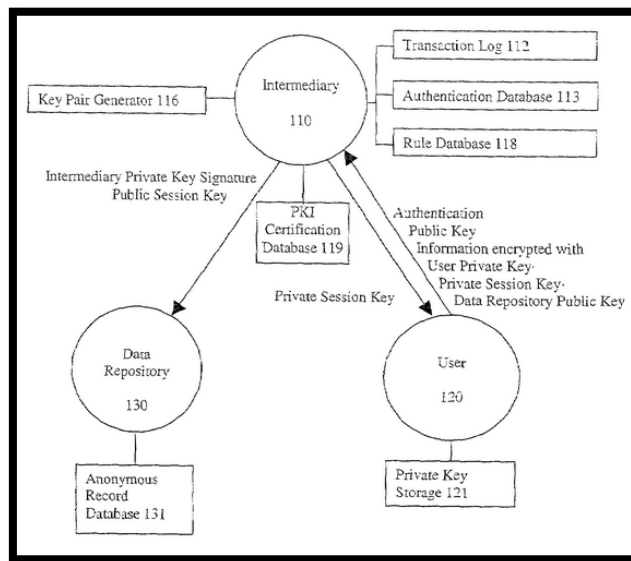
Encryption concepts and terminology

Encryption transforms data that is unprotected, or *plain text*, into encrypted data, or *ciphertext*, by using a *key*. Without knowledge of the encryption key, the ciphertext cannot be converted back to plain text.



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

153. 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 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

154. 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 transcribing 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.

155. 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.

156. 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).

157. 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.

- Security was not a major issue, even for Oracle
 - Standard passwords (scott/tiger, system/manager, ...)
 - Oracle standard users were installed and left open (though not at SAP!)
 - There are some recommendations, but not much more.
 - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts, ..., 10.2: CONNECT roles)

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

158. 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.⁵¹ “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).

⁵¹ See Kevin Hamlen et al., *Security Issues For Cloud Computing* at 39, INTERNATIONAL JOURNAL OF INFORMATION SECURITY AND PRIVACY VOL. 4(2) (April-June 2010) (“The major security challenge with clouds is that the owner of the data may not have control of where the data is placed. . . . Therefore, we need to safeguard the data in the midst of untrusted processes.”); Elana Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web Databases and Services* at 17, PROCEEDINGS OF THE EDBT CONFERENCE (March 2003) (“very little work has been devoted to security”); Elisa Bertino et al.; *Selective and Authentic Third-Party Distribution of XML Documents* at 1263, IEEE TRANSACTIONS ON KNOWLEDGE AND DATA ENGINEERING, Vol. 16 No. 10 (October 2004) (“The most intuitive solution is that of requiring Publishers to be trusted with regard to the considered security properties. However, this solution could not always be feasible in the Web environment since large Web-based systems cannot be easily verified to be secure.”).

159. 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 transcribing electronic information that is transmitted over a computer network via an intermediary.

160. 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 transcribing electronic information that is transmitted over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

161. The inventive concepts claimed in the '181 patent are technological, not “entrepreneurial.” For example, transcribing 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.

162. 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).⁵²

⁵² See also Vaibhav Khadilkar, Murat Kantarcioglu, and Bhavani Thuraisingham. *Secure Data Processing in a Hybrid Cloud* at 1-2, Computing Research Repository (CoRR) abs/1105.1982 (2011) (“The emergence of cloud computing has created a paradigm shift by allowing parallel

163. 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 transcribing 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.

164. 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 cipher text (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.

165. Both attacks exploit the fact that some encryption systems use static keys to create the cipher text. *Id.* In other words, using the same key repeatedly 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.

166. 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:

processing of massive amounts of data. . . . [H]ow do users protect themselves from cloud service providers who may be able to access their data? This issue is related to data security and is relevant for users since their data is placed at the provider's site.”).

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 transcribe the encrypted message to a transcribed message in an integral process substantially without intermediate decryption, using a transcription 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 transcribed record.

167. 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.

168. 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.

169. 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.

170. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁵³ the ‘181 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

171. 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.

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

173. The ‘181 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁵⁴

174. The ‘181 patent claims require the use of a computer system.

175. 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.” Companies have described the use of encryption in the cloud as important to improve the security and functioning of systems.

⁵³ *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).

⁵⁴ *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); see also *Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

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) (emphasis added).

176. 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.⁵⁵

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

178. 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.”⁵⁶

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 (emphasis added).

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

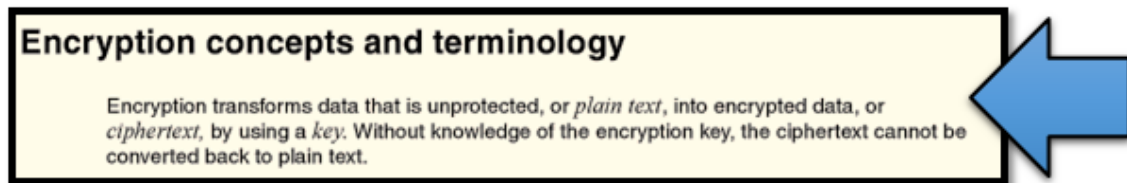
⁵⁵ Limitations in the prior art that the '181 patent was directed to solving included: computer systems where a “third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key” (*Id.*, col. 2:6-9); “[p]asswords may be written 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).

⁵⁶ 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.”).

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.”⁵⁷

180. 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.

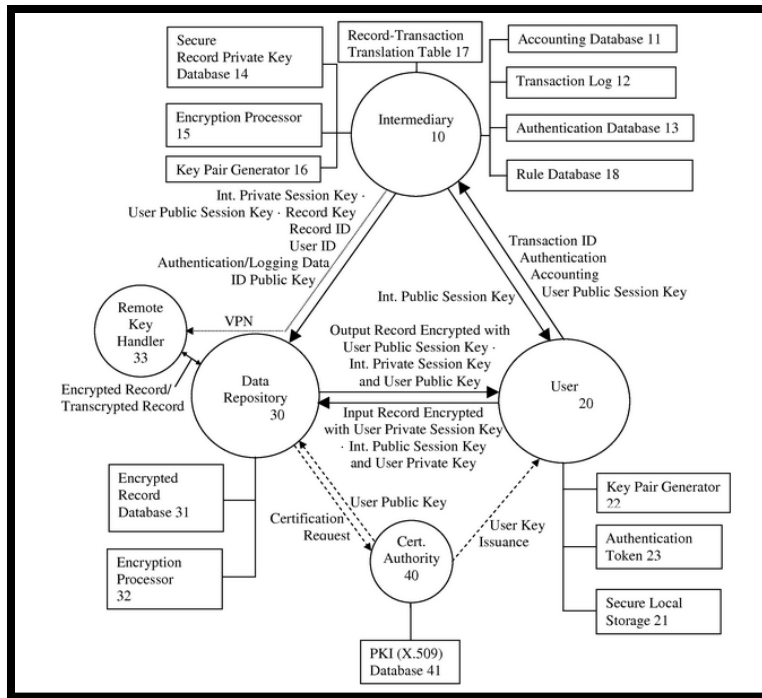
181. '181 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides (“redbooks”), refers to encryption as “transform[ing] data that is unprotected.



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

182. 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 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.

⁵⁷ 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).



‘181 patent, Fig. 1.

5. U.S. Patent No. 8,566,247

183. U.S. Patent No. 8,566,247 (the “‘247 patent”) entitled, System and Method for Secure Communications Involving and Intermediary, was filed on February 15, 2008, and claims priority to February 19, 2007. St. Luke is the owner by assignment of the ‘247 patent. A true and correct copy of the ‘247 patent is attached hereto as Exhibit E. The ‘247 patent claims specific methods and systems for communicating information which is encrypted from a first party to a second party, involving an intermediary that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information, and wherein the asymmetric delivery comprehension function comprises a function of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions.

184. The ‘247 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.

185. The '247 patent has been cited by nineteen issued United States patents and published patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the '247 patent.

- General Electric Company
- Microsoft Corporation
- PivotCloud, Inc.
- Futurewei Technologies, Inc.
- Ingenico Group SA
- Telefonaktiebolaget LM Ericsson

186. At the time of the inventions claimed in the '247 patent, securely communicating information which is encrypted from a first party to a second party, involving an intermediary, without the intermediary itself being enabled to comprehend the information presented new and unique issues over the state of the art. Systems and methods existing at the time the inventions taught in the '247 patent were conceived, failed to provide for “an intermediary perform[ing] 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.” '247 patent, col. 9:8-12.

187. The '247 patent “provides enhancements to traditional secure communications by providing involvement of a third party, or intermediary, who need not, and preferably does not, have access to the communicated information, while providing transaction-support services between the two parties involved in the communication.” '247 patent, col. 9:58-63.


188. The inventions taught in the '247 patent improve the function of the computer system itself, by making the system more secure. Researchers at Technische Universität Berlin concluded that securing data from decryption by an intermediary improved the security of computer systems.

The application of end-to-end encryption *carries security benefits for any solution architecture, e.g., by preventing the access to communication plaintext by intermediaries*. Applying such a security measure is especially meaningful within shared environments, such as public cloud offerings, as those are

associated with extensive ramifications of security breaches of those intermediaries, where a potentially large number of tenants would be affected.

Mathias Slawik, et al., *Securing Medical SaaS Solutions Using a Novel End-To-End Encryption Protocol* at 3, in TWENTY SECOND EUROPEAN CONFERENCE ON INFORMATION SYSTEMS (2014) (emphasis added).

189. Although the systems and methods taught in the ‘247 patent have been adopted by some major corporations, at the time of invention, the technologies taught in the ’247 patent claims were innovative and novel. Existing systems dealing with three-party communications “place[d] 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.” ‘247 patent, col. 1:42-47. Companies such as Oracle recognized that, until recently, security for distributed systems was not a primary concern.⁵⁸

- Security was not a major issue, even for Oracle
 - Standard passwords (scott/tiger, system/manager, ...)
 - Oracle standard users were installed and left open (though not at SAP!)
 - There are some recommendations, but not much more.
 - From Oracle9i, the issue of security was increasingly addressed by Oracle (DBCA: locking of default accounts, ..., 10.2: CONNECT roles)
- 

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

190. The ’247 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. Further, the inventions disclosed in the ‘247 patent teach how an intermediary may perform a requisite function with respect to the communication of encrypted information without possessing sufficient information to unilaterally decrypt the encrypted information. The ‘247 patent teaches ways the intermediary can be used to implement rules (e.g., authenticate access to encrypted

⁵⁸ See also Kevin T. Smith, *Big Data Security: The Evolution of Hadoop’s Security Model*, INFOQ (2013) (In 2005 when Hadoop, an open source framework for distributed storage and processing of data sets that is now widely used in the cloud computing instances, “security was not a factor.”).

information) without placing the intermediary in the position of being able to decrypt the communication. “[B]y exerting this control over the critical function outside the direct communication channel, the intermediary maintains a low communication bandwidth requirement and poses little risk of intrusion on the privacy of the secure communication.” ‘247 patent, col. 9:21-25. This improves the security of the computer system and allows the computer system to operate more efficiently.

191. The ‘247 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 communicating information which is encrypted from a first party to a second party, involving an intermediary which selectively authorizes the second party to comprehend the information, without the intermediary itself able to comprehend the information, using an asymmetric delivery comprehension function of the information which is encrypted, different from the associated cryptographic comprehension function.

192. The ‘247 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 transmitting encrypted electronic information over a computer network via an intermediary. These methods and systems are technologies unique to the Internet age.

193. The inventive concepts claimed in the ‘247 patent are technological, not “entrepreneurial.” For example, encrypting from a first party to a second party, involving an intermediary which selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information 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.

194. Patents cited on the face of the ‘247 patent identify the problems the ‘247 patent is directed at solving arising from challenges arising from, and unique to the internet.

This increase in *Internet communications has necessitated the development of security systems to insure protection for information transmitted over the Internet*. Encryption is a basic technique used to scramble information to prevent unsolicited access to that information. One well-known encryption scheme is secret key encryption.

U.S. Patent No. 6,061,448 to Smith (Issued May 9, 2000) (emphasis added).

Internet-based payment solutions require additional security measures that are not found in conventional POS terminals. This additional requirement is necessitated *because Internet communication is done over publicly-accessible, unsecured communication line in stark contrast to the private, secure, dedicated phone or leased line service utilized between a traditional merchant and an acquiring bank*. Thus, it is critical that any solution utilizing the Internet for a communication backbone, employ some form of cryptography.

U.S. Patent No. 6,072,870 to Nguyen (Issued June 6, 2000) (emphasis added).

195. The '247 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 '247 patent require information being encrypted with an associated cryptographic comprehension function and the use of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions so that the second party can decrypt the encrypted information but an intermediary does not have the ability to decrypt the information—a result that overrides the routine and conventional sequence of events in electronic communications, even encrypted electronic communications.

196. The preemptive effect of the claims of the '247 patent are concretely circumscribed by specific limitations. For example, claim 10 of the '247 patent requires:

A system for communicating information which is encrypted from a first party to a second party, involving an intermediary that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information, comprising:

a communication port which receives information which is encrypted to be communicated or an identification thereof, the information being encrypted with an associated cryptographic comprehension function;

at least one automated processor which conducts a negotiation between the second party and the intermediary through the communication port of an asymmetric delivery comprehension

function of the information which is encrypted, different from the associated cryptographic comprehension function, wherein the asymmetric delivery comprehension function comprises a function of at least three asymmetric key components of at least three distinct respective asymmetric delivery comprehension functions, wherein the second party possesses an ability to decrypt the information which is encrypted with the asymmetric delivery comprehension function, and the intermediary possesses a portion of the asymmetric delivery comprehension function which does not impart an ability to decrypt the information which is encrypted;

the at least one automated processor further transforms a comprehension function of the information which is encrypted to be communicated from the associated cryptographic comprehension function to the asymmetric delivery cryptographic comprehension function, comprising using the negotiated asymmetric delivery comprehension function of the at least three key asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions in an integral process which does not have as an intermediate state a decrypted representation of the information and does not itself require at any time during the transformation, knowledge sufficient for decrypting the information which is encrypted; and

said communication port communicating the information which is encrypted with the asymmetric delivery cryptographic comprehension function to the second party.

197. The '247 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.

198. The '247 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 '247 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.

199. For example, the '247 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:

- Blind Signatures. See David Chaum, “Blind Signatures for Untraceable Payments”, Proceedings of Crypto 82, August 1982, p. 199-203. According to the system proposed by David Chaum, a server assists a user in decrypting a message without releasing its secret key or gaining access to the encrypted message.
- Use of a Trusted Intermediary. U.S. Patent No. 6,199,052 to Mitty, describing the use of a trusted intermediary with archive and verification request services for secure electronic transactions.
- Use Of Transaction Certificates. U.S. Patent No. 6,687,822 to Jakobsson, teaching the use of verifiable translation certificates comprising the steps of receiving an input encryption having a first secret key; outputting an output re-encryption of the input encryption, the output re-encryption having a second secret key
- Proxy Key Cryptography. In typical proxy key systems, a proxy receives a private key from a sender of an asymmetrically encrypted message, and a public key from a recipient of the transformed encrypted message, and computes a transform key (e.g., a product of p and q in an RSA type PKI algorithm) which is applied to the asymmetrically encrypted message. See Susan Hohenberger, “Advances in Signatures, Encryption, and E-Cash from Bilinear Groups,” (Ph.D. Thesis, MIT, May 2006).

200. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁵⁹ the ‘247 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

201. The ‘247 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

202. The claimed subject matter of the ‘247 patent is not a pre-existing but undiscovered algorithm.

⁵⁹ *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).

203. The '247 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁶⁰

204. The '247 patent claims require the use of a computer system.

205. The claims in the '247 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 '247 patent improves the security of computer systems. Prior art systems that the '247 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) (emphasis added).

206. The '247 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.⁶¹

207. The claimed invention in the '247 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

⁶⁰ *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); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

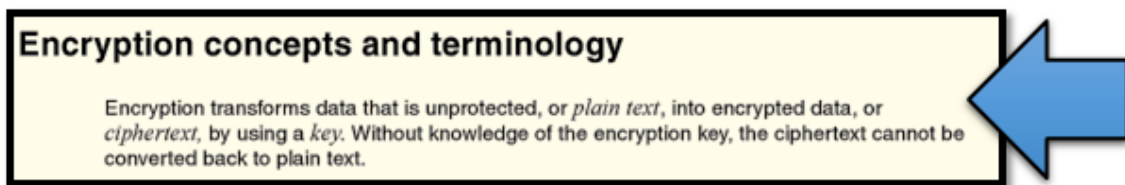
⁶¹ Limitations in the prior art that the '247 patent was directed to solving included: computer systems where a “third party plays a requisite role in the transaction but which need not be trusted with access to the information or the cryptographic key” (*Id.*, col. 2:6-9); “[p]asswords may be written 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).

208. The systems and methods claimed in the '247 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.

209. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, they involve 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 '247 patent are 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.”⁶²

210. The '247 patent claims are not directed at a mathematical relationship or formula. The '247 patent claims concrete, specific computer systems and methods for cryptographically protecting and managing access to secure data in multi-party communications.

211. '247 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).

212. One or more claims of the '247 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure

⁶² 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).

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 '247 patent illustrates a specific configuration of hardware disclosed in the patent.

C. Information Record Infrastructure Patents

213. 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.

214. 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.

215. 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.

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

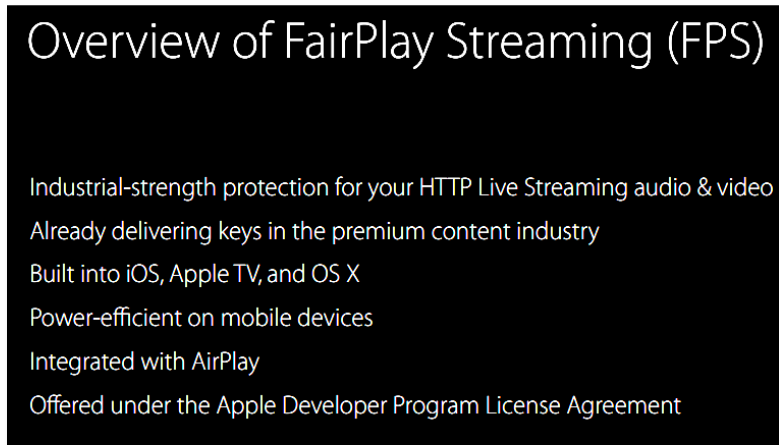
Such cloud adoption within the healthcare industry is gaining momentum because the economic, clinician productivity and care team collaboration advantages of the cloud are undeniable. However, as was the case for UCHealth, there's ***one fundamental concern that continues to weigh heavily on the minds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

217. Microsoft's competitors, such as Apple and Hewlett Packard, 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).



Roger Pantos, *Content Protection for HTTP Live Streaming*, APPLE WWDC15 PRESENTATION at 9 (2015).

218. 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).⁶³

⁶³ See also Murat Kantarcioglu, Wei Jiang, and Bradley Malin, *A Privacy-Preserving Framework for Integrating Person-Specific Databases* at 299, PRIVACY IN STATISTICAL

219. 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).⁶⁴

220. 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.

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).⁶⁵

DATABASES LNCS 5262 (2008) (Describing the difficulty in managing medical records stored in multiple electronic databases “in the healthcare realm, patients are mobile and their data can be collected by multiple locations, such as when a patient visits one hospital for primary care and a second hospital to participate in a clinical trial.”).

⁶⁴ 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”).

⁶⁵ *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

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/>.

221. 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.

222. 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.

223. 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.

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

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."); Arun Kulkarni, Harikrishna Gunturu, and Srikanth Datla, *Association-Based Image Retrieval* at 183, WSEAS TRANS. SIG. PROC. Vol.4(4) (April 2008) ("With advances in computer technology and the World Wide Web there has been an explosion in the amount and complexity of multimedia data that are generated, stored, transmitted, analyzed, and accessed.").

225. **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.

226. 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).⁶⁶

227. 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.

228. Apple's iTunes software, released in January 2001, was indicative of the state of information rights management systems available at the time. Apple's 2001 iTunes release lacked information rights management software and was marketed to users who wanted to convert compact discs into MP3s. The product was marketed with the tagline "Rip. Mix. Burn."⁶⁷

⁶⁶ 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.").

⁶⁷ Jacqui Cheng, *iTunes Through The Ages: We Look Back At 12 Years Of iTunes Releases*, ARS TECHNICA, May 23, 2012, <http://arstechnica.com/apple/2012/11/itunes-through-the-ages/>.

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



Screenshot of Windows Media Player 7.1 (released in May 2001).⁶⁸

230. ***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.⁶⁹ These systems included: (1)

⁶⁸ Windows Media Player 7.1 did not incorporate Microsoft’s PlayForSure DRM technology.

⁶⁹ 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.”); see also Bhavani Thuraisingham, *Data and Applications Security: Developments and Directions* at 2, PROCEEDINGS IEEE COMPSAC (2002) (Discussing issues with electronic medical records “There are numerous security issues for such systems including secure information sharing and collaboration.

Anonymizing Records. A method used in contemporaneous systems to the IRI patents is the maintenance of anonymous medical records. However, anonymizing techniques did not provide patients and medical professionals the ability to access patient specific records. (2) Indexing. Systems contemporaneous to the IRI patents indexed medical records with anonymous identification codes.⁷⁰ While these systems preserved privacy, these systems 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.

231. 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.

232. 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 Epic System Corporation's CareWeb⁷¹ 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

Furthermore, data is no longer only in structured databases. . . . Security for such data has not received much attention.”).

⁷⁰ See also Murat Kantarcioglu and Chris Clifton, *Security Issues in Querying Encrypted Data* at 2, TECHNICAL REPORT CSD TR 04-013, Purdue University Computer Sciences Department (2004) (“methods that quantize or “bin” values reveal data distributions. Methods that hide distribution, but preserve order, can also disclose information if used naively”).

⁷¹ 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.).

backend database, the databases accessed through CareWeb were basically opaque to the “CareWeb” system; and CareWeb’s fixed structure was expressly limited to a particular, monolithic front-end architecture for secure implementation.

233. 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 external databases. Further, 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).

234. The need for a secure system for providing access to medical records was specifically required in the cloud computing context 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>.

235. On information and belief, contemporaneous to, and following conception of the inventions disclosed in the IRI patents, Texas educational institutions, Texas governmental entities, and businesses headquartered in Texas actively entered the field of electronically structuring and controlling access to protected health data stored in a plurality of external databases. In 2006, Texas Gov. Rick Perry called for widespread adoption of health information

technology (“HIT”).⁷² Governor Perry signed Senate Bill 45, which created the Health Information Technology Advisory Committee (HITAC) within the Texas Statewide Health Coordinating Council in the Department of State Health Services.⁷³ In addition, various universities studied and implemented systems for securely managing access to distributed medical records.⁷⁴

236. Microsoft has expended significant energy marketing and selling its cloud security products to the state of Texas. Michael Donlan, Vice President of State and Local Government at Microsoft stated “We’ve worked hard to provide security and privacy solutions the State of Texas can trust.”⁷⁵ Microsoft in a blog directed specifically to Texas customers explained:

[W]e will also be *highlighting uplifting stories about the work Microsoft is doing to give back to businesses and residents in Dallas-Fort Worth* as well as throughout Texas. As a business, Microsoft is as much a part of the community as the individuals who devote their own time to supporting nonprofits and worthy causes. In this blog and in our day-to-day activities, we want to acknowledge our fellow corporate citizens who are giving back, and help other businesses get involved in their communities.

A Big Texas Hello, MICROSOFT TEXAS BLOG (October 20, 2014) (emphasis added).

237. Texas based companies incorporated systems and methods for electronically structuring and controlling access to protected data in a plurality of external databases into numerous products. Many of these same companies cite the IRI patents in their own patents.

⁷² Gov. Rick Perry, *State-of-the-State Speech*; February 6, 2007, available at: <http://governor.state.tx.us/news/speech/5567/>.

⁷³ Texas Senate Bill 45, Texas 79th Regular Legislative Session (25 TAC §§571.11-571.13); see also Texas Executive Order RP-61, *Relating to the Creation, Composition, and Operation of the Governor's Health System Integrity Partnership for the State of Texas* (October 9, 2006) (The Partnership was directed to develop a method for secure exchange of electronic health information.).

⁷⁴ See David E. Gerber et al., Predictors and Intensity of Online Access to Electronic Medical Records Among Patients with Cancer, *J Oncol Pract.* Vol. 10(5) (Sept. 2014) (studying electronic medical record infrastructure implementations at and Texas hospitals).

⁷⁵ *State of Texas to Improve Communication and Collaboration by Adopting Office 365 for More Than 100,000 State Employees*, MICROSOFT NEWS CENTER (February 15, 2013); see also Michael Donlan, *Texas Moves to the Cloud with Microsoft*, MICROSOFT GOVERNMENT BLOG (August 7, 2012) (“Both Texas and Microsoft worked closely together to support the state’s requirements under the Health Insurance Portability and Accountability Act (HIPAA).”).

Texas based businesses that developed products and/or technologies incorporating these systems included: HP Enterprise Services, LLC of Plano, Texas; Hospitalists Now, Inc. of Austin, Texas; StandardCall, LLC of Frisco, Texas; Security First Corp whose inventors were based in various locations in Texas; Huawei Technologies Co., Ltd. of Plano, Texas; Omnyx LLC whose inventors included individuals based in Texas; Electronic Data Systems Corporation of Plano, Texas; and South Texas Accelerated Research Therapeutics, LLC of San Antonio, Texas.

1. U.S. Patent No. 7,805,377

238. U.S. Patent No. 7,805,377 (the “377 patent”) entitled, Information Record Infrastructure, System and Method, was filed on August 19, 2008, and claims priority to July 6, 2000. St. Luke is the owner by assignment of the ‘377 patent. A true and correct copy of the ‘377 patent is attached hereto as Exhibit F. The ‘377 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer.

239. The ‘377 patent has been cited by over 30 United States patents and patent applications as relevant prior art. Specifically, patents issued to the following companies have cited the ‘377 patent as relevant prior art.

- Symantec Corporation
- Siemens Medical Solutions USA, Inc.
- AT&T Corporation
- Hospitalists Now, Inc.
- MasterCard International Incorporated
- J.D. Power And Associates
- Middlegate, Inc.
- Cardiac Pacemakers, Inc.
- Robert Bosch GmbH

240. The ‘377 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.

241. At the time of the inventions claimed in the ‘377 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 ‘377 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.” ‘377 patent, col. 54:27-33.

242. Although the systems and methods taught in the ‘377 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the ‘377 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.” ‘377 patent, col. 5:8-20.

243. Further, the ‘377 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.” ‘377 patent, col. 69:28-30.

244. The ‘377 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.

245. The ‘377 patent claims are not directed at the broad concept/idea of “managing digital records.” Instead, the ‘377 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.⁷⁶

⁷⁶ See *Trusted Cloud: Microsoft Azure Security, Privacy, and Compliance* at 5, MICROSOFT WHITE PAPER (April 2015) (“Cloud services raise unique privacy challenges for businesses. As

246. The '377 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 '377 patent require a database adapted to store information for determining patient-controlled access control criteria, authenticate the requestor and determine sufficiency of the patient-provided access control authorization, and generating an electronic payment authorization.

247. The '377 patent is directed to specific problems in the field of digital record access and transmission.

248. The preemptive effect of the claims of the '377 patent are concretely circumscribed by specific limitations. For example, claim 7 of the '377 patent requires:

A system adapted to control access to a patient medical record hosted by at least one medical record repository comprising a plurality of record portions, each record portion being associated with different patient-controlled access control criteria, said system comprising an automated processor, a database adapted to store information for authenticating requestors, a database adapted to store information for determining patient-controlled access control criteria for respective record portions of a patient medical record, and a computer network interface, said processor being controlled by instructions stored on a computer readable storage medium to:

- (a) receive a request for a medical record from a requestor, said request comprising a medical record identifier, a requestor identifier, requestor authentication information, and patient-provided access control authorization;
- (b) process the request for the medical record, to authenticate the requestor and determine sufficiency of the patient-provided access control authorization to meet the patient-controlled access control criteria for each respective record portion encompassed by the request;

companies look to the cloud to save on infrastructure costs and improve their flexibility, they also worry about losing control of where their data is stored, who is accessing it, and how it gets used.”).

(c) selectively communicate through the computer network interface to the at least one medical record repository, an identification of each record portion for which access control criteria are determined to be sufficient for access by the requestor; and

(d) generating an electronic payment authorization associated with the request, for compensation of at least one of said system and the at least one medical record repository.

249. The '377 patent does not attempt to preempt every application of the idea of controlling access to an electronic medical record over a computer network.

250. The '377 patent does not preempt the field of electronically structuring and controlling access to protected medical records in a plurality of external databases. For example, the '377 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.

251. For example, the '377 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.
- Security Tokens. U.S. Patent No. 5,978,918 to Scholnick, discloses a back-end process returns a time sensitive token that the “sender” sends to the “receiver.” The “receiver” takes the time sensitive token and uses it to retrieve the private data.⁷⁷

⁷⁷ See also Arindam Khaled et al., *A Token-based Access Control System for RDF Data in the Clouds* at 104, in PROCEEDINGS OF THE 2ND IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE (2010) (discussing the use of a “token-based access control system . . . implemented in Hadoop (an open source cloud computing framework)”).

- 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, are encrypted by a public key encryption system using a private key.
- 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).⁷⁸

252. The '377 patent does not claim, or attempt to preempt, the performance of an abstract business practice on the Internet or using a conventional computer.

253. The '377 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁷⁹

254. The '377 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

255. The claimed inventions in the '377 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

256. The systems and methods claimed in the '377 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.

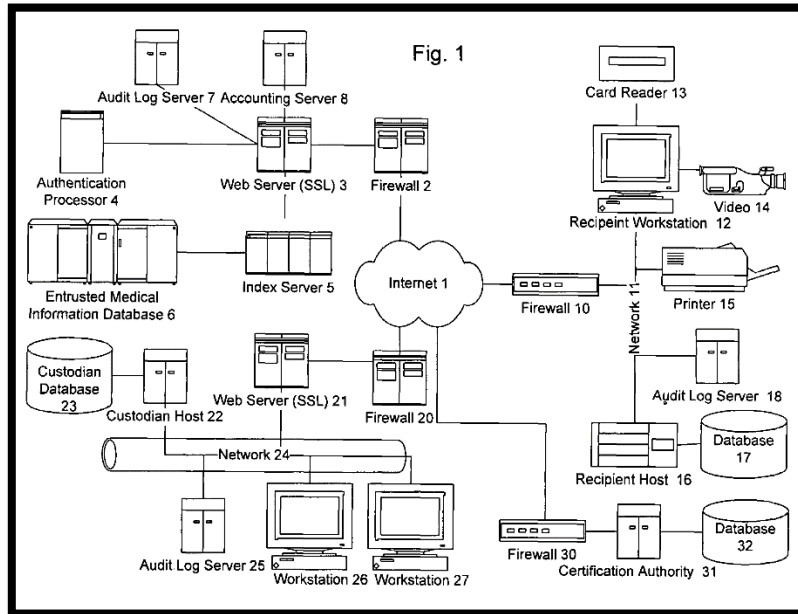
257. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, they involve a method for changing digital records in a way that will affect the communication system itself, by making it more secure.

258. One or more claims of the '377 patent require a specific configuration of electronic devices, a network configuration, external databases, a computer network interface, etc.. These are meaningful limitations that tie the claimed methods and systems to specific

⁷⁸ Nary Subramanian, *Biometric Authentication*, in *ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY* (S. Jajodia and H.C.A. van Tilborg 2nd ed. 2011) (“Biometric authentication is a technique for identifying the person accessing a secured asset . . . by comparing their unique biological features . . . [an] issue with biometric authentication is privacy of personal data.”).

⁷⁹ *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); *see also Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

machines. For example, the below diagram from the '377 patent illustrates a specific configuration of hardware disclosed in the patent.



'377 patent, Fig. 1.

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

259. 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 G. The '368 patent claims specific methods and systems for securely controlling access to a plurality of digital records by a remote computer.

260. 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 Philips Electronics N.V.
- Huawei Technologies Co., Ltd.
- Ricoh Co., Ltd.
- Massachusetts Institute Of Technology

261. 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.

262. 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.

263. 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.

264. 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.

265. 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.

266. 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.

267. 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.

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

269. 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.

270. 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.

271. 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.

272. 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.
- Security Tokens. U.S. Patent No. 5,978,918 to Scholnick, discloses a back-end process returns a time sensitive token that the "sender" sends to the "receiver." The "receiver" takes the time sensitive token and uses it to retrieve the private data.⁸⁰

⁸⁰ See also Arindam Khaled et al., *A Token-based Access Control System for RDF Data in the Clouds* at 104, in PROCEEDINGS OF THE 2ND IEEE INTERNATIONAL CONFERENCE ON CLOUD

- 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.

COMPUTING TECHNOLOGY AND SCIENCE (2010) (discussing the use of a “token-based access control system . . . implemented in Hadoop (an open source cloud computing framework)”).

- 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).⁸¹

273. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁸² the ‘368 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

274. 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.

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

276. The ‘368 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁸³

277. The ‘368 patent claims require the use of a computer system.

278. 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.

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

⁸¹ Nary Subramanian, *Biometric Authentication*, in ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY (S. Jajodia and H.C.A. van Tilborg 2nd ed. 2011) (“Biometric authentication is a technique for identifying the person accessing a secured asset . . . by comparing their unique biological features . . . [an] issue with biometric authentication is privacy of personal data.”).

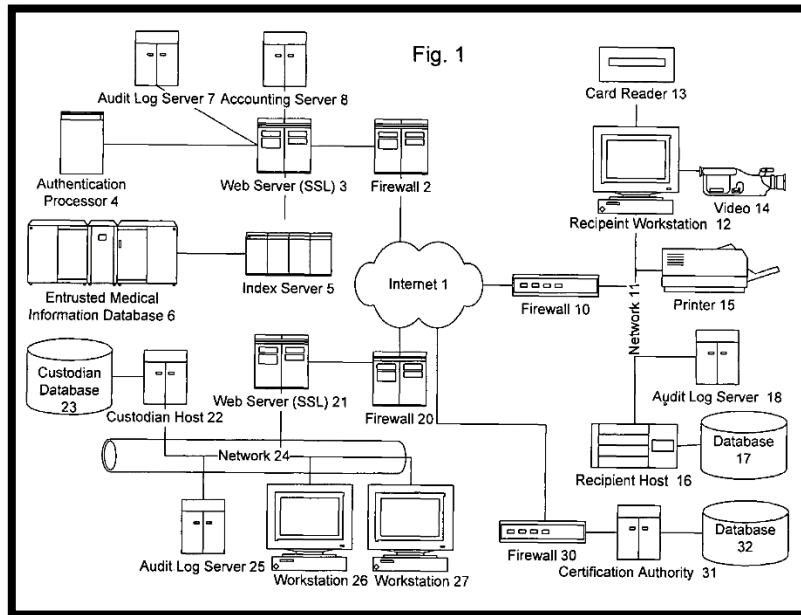
⁸² *Paone v. Broadcom Corp.*, Case No. 15 CIV. 0596 BMC GRB, 2015 WL 4988279, at *7 (E.D.N.Y. Aug. 19, 2015) (citing *Fid. Nat'l Info. Servs., Inc.*, Petitioner, CBM2014-00021, 2015 WL 1967328, at *8 (Apr. 29, 2015) (both upholding the patent eligibility of patents directed toward encryption).

⁸³ *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); see also *Prism Technologies, LLC v. T-Mobile USA, Inc.*, 12-cv-124, Dkt. No. 428 at 7 (D. Neb. Sept. 22, 2015) (Finding on cross motions for summary judgment that patents directed at delivering resources over an untrusted network were patent eligible. “The problems addressed by Prism’s claims are ones that ‘arose uniquely in the context of the Internet.’”).

280. 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.

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

282. 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.

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

283. 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 H. 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.

284. 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

285. 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.

286. 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.

287. 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.

288. 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.

289. 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.

290. 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.

291. 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.

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

293. 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.

294. 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.

295. 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.

296. 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.
- Security Tokens. U.S. Patent No. 5,978,918 to Scholnick, discloses a back-end process returns a time sensitive token that the “sender” sends to the “receiver.” The “receiver” takes the time sensitive token and uses it to retrieve the private data.⁸⁴
- 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.

⁸⁴ See also Arindam Khaled et. al, *A Token-based Access Control System for RDF Data in the Clouds* at 104, in PROCEEDINGS OF THE 2ND IEEE INTERNATIONAL CONFERENCE ON CLOUD COMPUTING TECHNOLOGY AND SCIENCE (2010) (discussing the use of a “token-based access control system . . . implemented in Hadoop (an open source cloud computing framework)”).

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).⁸⁵

297. 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.

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

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

300. 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.

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

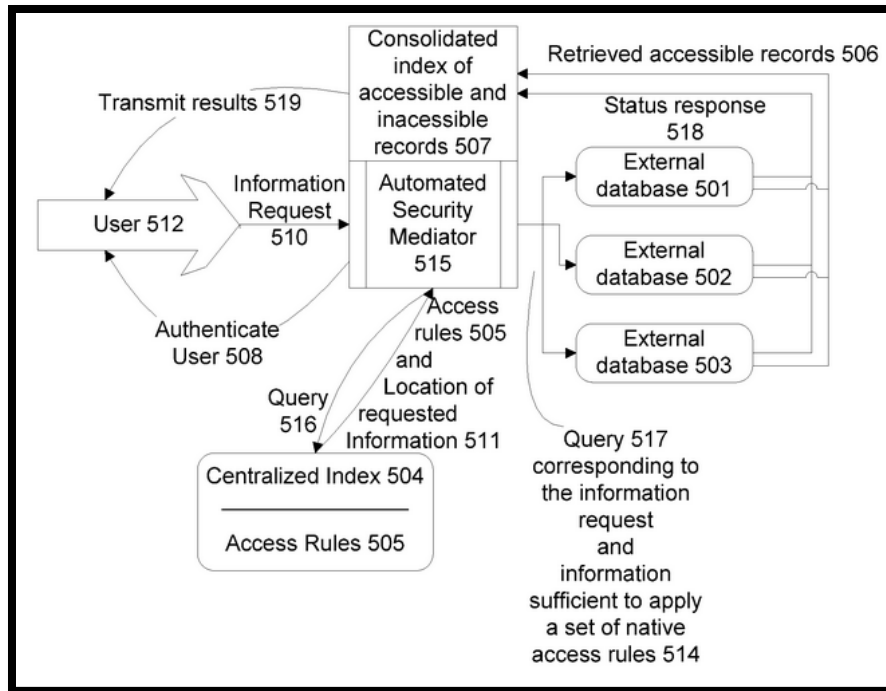
302. The systems and methods claimed in the '941 patent were not a longstanding or fundamental economic practice at the time of patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general.

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

304. 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

⁸⁵ Nary Subramanian, *Biometric Authentication*, in *ENCYCLOPEDIA OF CRYPTOGRAPHY AND SECURITY* (S. Jajodia and H.C.A. van Tilborg 2nd ed. 2011) (“Biometric authentication is a technique for identifying the person accessing a secured asset . . . by comparing their unique biological features . . . [an] issue with biometric authentication is privacy of personal data.”).

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.

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

305. 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 I. 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.

306. 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

307. 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.

308. 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.

309. 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.

310. 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.

311. The '630 patent claims require an automated security mediator (“ASM”).

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

313. 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.

314. 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.

315. 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.

316. 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.

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

318. 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.

319. 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.

320. 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.

321. 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).

322. 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.

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

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

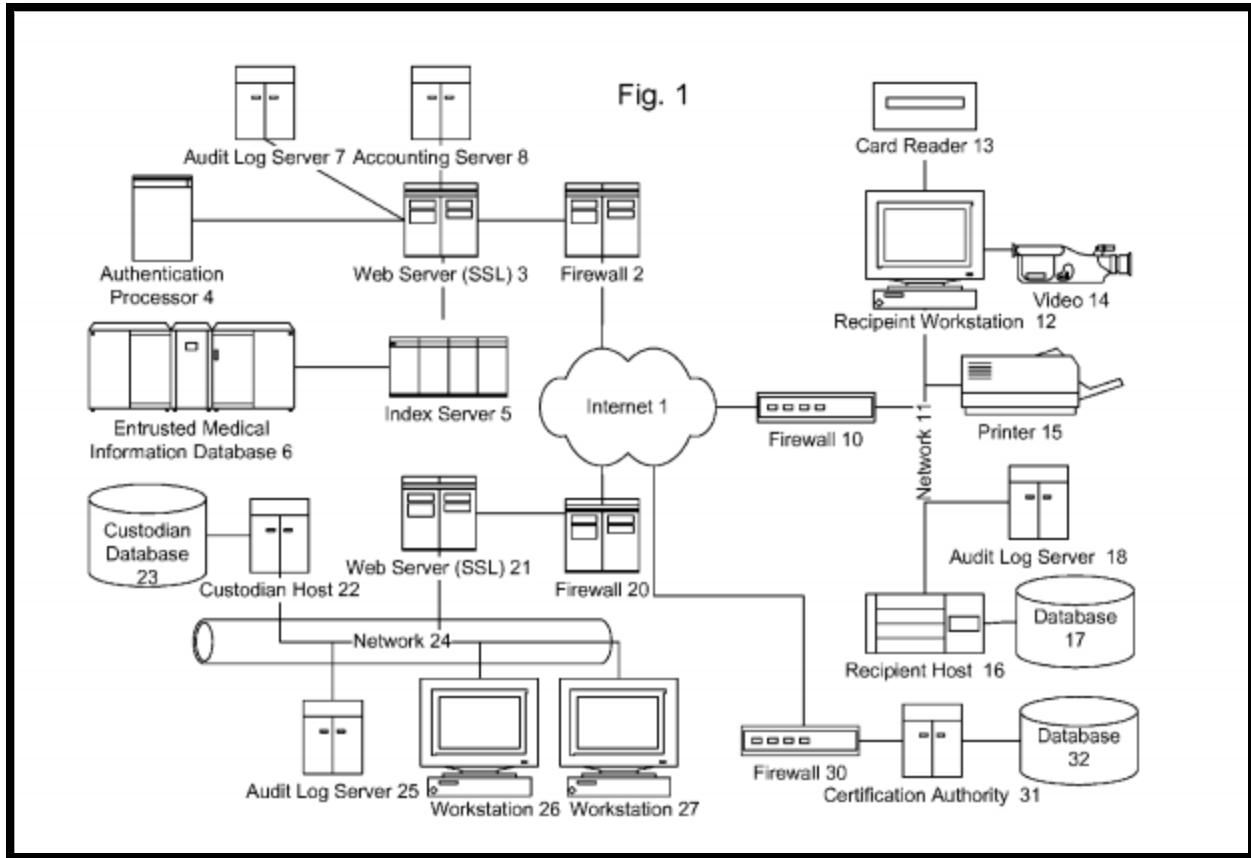
325. The '630 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

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

327. 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.

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

329. 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.

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

330. 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 J. 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.

331. The ‘895 patent has been cited by four United States patents and patent applications as relevant prior art.⁸⁶ Specifically, patents issued to the following companies have cited the ‘895 patent as relevant prior art.

⁸⁶ 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

332. 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.

333. 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.

334. 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.

335. 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.

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

337. 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).

338. 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.

339. 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.

340. 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.

341. 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.

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

343. 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.

344. 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.

345. 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.

346. 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).

347. 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.

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

349. The '895 patent claims require the use of a computer system.

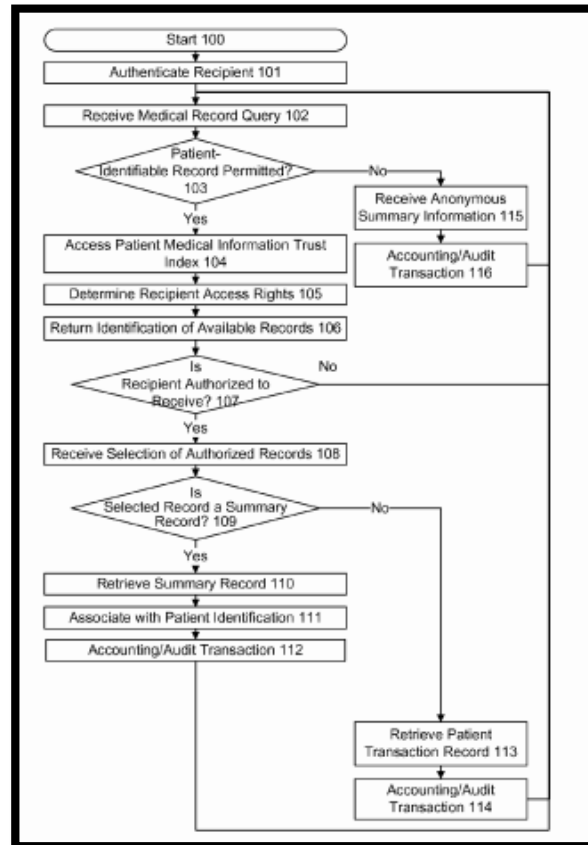
350. The '895 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

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

352. 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.

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

354. 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

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

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

357. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management (“Microsoft Azure RMS”), Microsoft Azure Media Services (“Microsoft Azure Media Services”); Microsoft Office 365 (“Microsoft Office 365”); and Microsoft Azure RMS Enlightened Client programs and services (“Microsoft Azure RMS Clients”)⁸⁷ (collectively, the “Azure and Office 365 RMS System”).

358. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure StorSimple (“StorSimple”).⁸⁸

359. On information and belief, Azure and Office 365 RMS System and StorSimple (collectively, the “Microsoft ‘237 Products’) include encryption technology.

360. On information and belief, the Microsoft ‘237 Products comprise a transcription device. For example, the Azure and Office 365 RMS System includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual Hardened Security Appliance in the Azure cloud) that is configured to transcribe information (e.g., Office 365 information).

361. On information and belief, the Microsoft ‘237 Products include at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual Hardened Security Appliance in the Azure cloud) comprising an automated communication port configured to receive a first message representing an encrypted communication associated with a first set of asymmetric keys

⁸⁷ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as “enlightened” clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

⁸⁸ Microsoft Azure StorSimple is storage product that manages storage tasks between on-premises devices and Microsoft Azure cloud storage. The accused Microsoft Azure StorSimple product is comprised of one or more of the following components: a StorSimple device (StorSimple series 8000 devices), a StorSimple virtual device, Windows PowerShell for StorSimple, Azure PowerShell StorSimple cmdlets, StorSimple Manager Service, StorSimple Snapshot Manager, and StorSimple Adapter for SharePoint. A description of the components of Microsoft Azure StorSimple is available at: <https://azure.microsoft.com/en-us/documentation/articles/storsimple-components/>.

(e.g., an encrypted Office 365 document, the encryption associated with a first Azure RMS user's set of RSA keys), to receive a transcription key (e.g., a cryptographic key for transcribing the first message into the second message as claimed), and to transmit a second message representing the encrypted communication associated with a second set of asymmetric keys (e.g., the encrypted Office 365 document, the encryption (now) associated with a second Azure RMS user's set of RSA keys), the first and second sets of encryption keys being distinct.

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

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

364. On information and belief, the Microsoft '237 Products include memory. For example, the Azure and Office 365 RMS System includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual Hardened Security Appliance in the Azure cloud) comprising a memory.

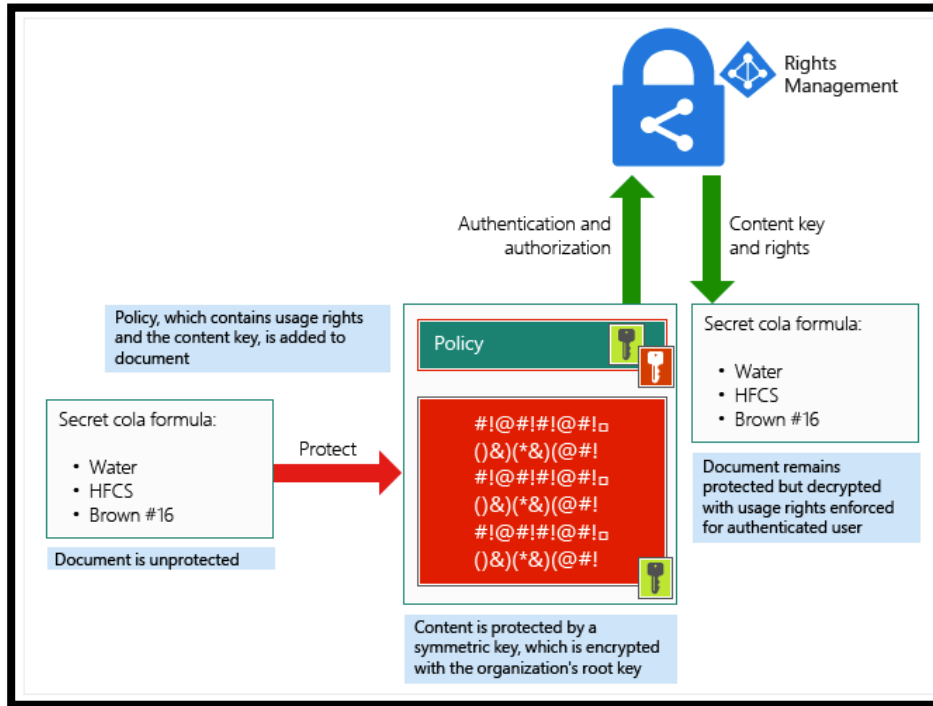
365. On information and belief, the Microsoft '237 Products include a transcription device comprising an automated processor, configured to communicate through the automated communication port and with the memory, to receive the first message, receive the transcription key, and automatically transcribe the first message into the second message, wherein the automated processor does not store as a part of the transcription any decrypted representation of the encrypted communication, and the transcription key is employed without revealing any secret cryptographic information usable for decrypting the first message or the second message.

366. On information and belief, the Azure and Office 365 RMS System includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual Hardened Security Appliance in the Azure cloud) comprising an automated processor configured to communicate through the automated communication port and with the memory, to receive the first message (e.g., the encrypted Office 365 communication, the encryption associated with the first Azure RMS user's set of RSA keys), receive the transcription key (e.g., the cryptographic

key for automatically transcribing the first message into the second message), automatically transcribe the first message into the second message (e.g., the encrypted Office 365 communication, the encryption (now) associated with the second Azure RMS user’s set of RSA keys).

367. On information and belief, the Microsoft ‘237 Products enable sending encrypted information through an intermediary where the intermediary is not able to access the unencrypted message.

368. On information and belief, the below diagram shows the encryption system used by Microsoft Azure RMS.



What is Azure Rights Management?, MICROSOFT TECHNET ARTICLE (July 1, 2015).

369. On information and belief, the Microsoft ‘237 Products include an automated processor that does not store as a part of the transcription any decrypted representation of the encrypted communication, and the transcription key is employed without revealing any secret cryptographic information usable for decrypting the first message or the second message (e.g.,

the first and second Microsoft Azure RMS users' respective RSA private keys, which are computationally infeasible to determine from their public keys).

370. On information and belief, one or more of the Microsoft '237 Products enable the use of a transcription key that is communicated through the automated communication port, encrypted with an ephemeral/PFS transport session key interactively negotiated for a communication session between the transcription device and a communication counterpart (e.g., the second Microsoft Azure RMS user).

371. On information and belief, the Azure and Office 365 RMS System comprises a transcription device capable of interfacing with, and in many cases does interface with, a public access network (e.g., the Internet) to communicate with a Microsoft Azure RMS Client.

372. On information and belief, the Azure and Office 365 RMS System comprises a transcription device capable of interfacing with, and in many cases does interface with, a private network (e.g., a corporate intranet) to communicate with a Microsoft Azure RMS Client.

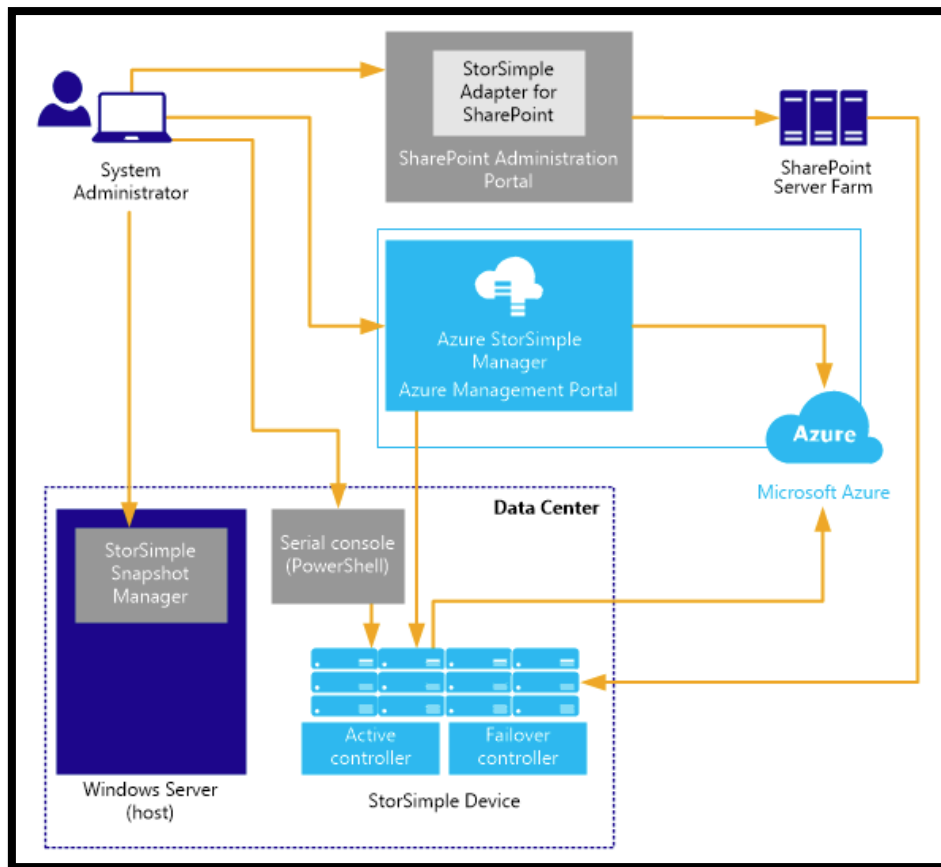
373. On information and belief, the Azure and Office 365 RMS System comprises a transcription device capable of interfacing with, and in many cases does interface with, a virtual private network (e.g., a corporate SSL VPN) to communicate with a Microsoft Azure RMS Client.

374. On information and belief, StorSimple uses a system of asymmetric key pairs to prevent unauthorized access to stored information.

375. On information and belief, data entering the StorSimple system is encrypted using the public key and decrypted using the private key stored on the device. This ensures that the Azure service cannot decrypt the data flowing to the device.

376. On information and belief, StorSimple uses RSA-2048 encryption keys to encrypt StorSimple device configurations, cloud storage encryption keys, and StorSimple account credentials. StorSimple uses AES-256 encryption keys to encrypt data before the data is sent to storage in the cloud.

377. The below diagram from Microsoft's StorSimple documentation shows the Microsoft Azure StorSimple architecture.



Sharon Smith, *StorSimple 8000 Series: A Hybrid Cloud Storage Solution*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (Sept. 25, 2015).

378. On information and belief, the Microsoft '237 Products use a transcription key that comprises at least a first portion dependent on the identity (via unique RSA keypair) of an intended recipient, and a second portion dependent on the identity (via unique RSA keypair) of a document author/originator/owner/etc.

379. On information and belief, the Azure and Office 365 RMS system enables the use of a transcription key that comprises a function of the first message decryption key (because it is already encrypted with a function of the first Azure RMS user's RSA private key), and a function of the second message encryption key (because the message needs to be encrypted by

the intermediary for later decryption by the second RMS user. In RSA, an encryption key is a complement of a decryption key.

380. On information and belief, Microsoft has directly infringed and continues to directly infringe the '237 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, Microsoft '237 Products, which include infringing encryption technologies.

381. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to Microsoft '237 Products, Microsoft 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 1-2, 4-6, 8, 10-11, 14-19, pursuant to 35 U.S.C. § 271(a).

382. On information and belief, Microsoft also indirectly infringes the '237 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of 2012.

383. On information and belief, Microsoft had knowledge of the '237 patent since at least 2012. Microsoft cited the '237 patent in the following issued United States patents and published patent applications:

- U.S. Patent No. 8,667,292 issued on March 4, 2014 entitled "Privacy-Preserving Metering with Low Overhead," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2012/0297198 published on November 22, 2012 entitled "Privacy-Preserving Metering with Low Overhead," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2013/0198618 published on August 1, 2013 entitled "Educating Users and Enforcing Data Dissemination Policies," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2014/0283054 published on September 18, 2014 entitled "Automatic Fraudulent Digital Certificate Detection," and assigned to Microsoft Corporation.
- U.S. Patent No. 8,966,659 issued on February 15, 2015 entitled "Automatic Fraudulent Digital Certificate Detection," and assigned to Microsoft Technology Licensing, LLC.
- U.S. Patent No. 9,087,039 issued on July 21, 2015 entitled "Language Independent Probabilistic Content Matching," and assigned to Microsoft Technology Licensing, LLC.

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

385. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft ‘237 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘237 patent. Microsoft 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, Microsoft provides the Microsoft ‘237 Products which have the capability of operating in a manner that infringes one or more of the claims of the ‘237 patent, including at least claims 1-2, 4-6, 8, 10-11, 14-19, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft ‘237 Products to utilize the product in a manner that directly infringes one or more claims of the ‘237 patent. By providing instruction and training to customers and end-users on how to use the Microsoft ‘237 Products in a manner that directly infringes one or more claims of the ‘237 patent, including at least claims 1-2, 4-6, 8, 10-11, 14-19, Microsoft specifically intended to induce infringement of the ‘237 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft ‘237 Products, *e.g.*, through Microsoft manuals, product support, marketing materials, blog postings, and training materials to actively induce the users of the Microsoft ‘237 Products to infringe the ‘237 patent.⁸⁹ Accordingly, Microsoft has induced and

⁸⁹ *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Sharon Smith, *Microsoft Azure StorSimple Security*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Sharon Smith, *StorSimple 8000 Series: A Hybrid Cloud Storage Solution*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION

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.

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

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

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

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

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

390. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Media Services ("Microsoft Azure Media Services"); Microsoft Office 365 ("Microsoft Office 365"); and Microsoft Azure RMS

(September 16, 2015); *Microsoft StorSimple: Hybrid Cloud Storage Security*, MICROSOFT STORSIMPLE SECURITY BRIEF (2014); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); Ben Watson, *StorSimple & Windows Azure Cloud-Integrated Storage*, MSDN CHANNEL 9 PRESENTATION (June 18, 2014); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015); Meghan Liese et al., *StorSimple: Extending Your Datacenter Into Microsoft Azure With Hybrid Cloud Storage*, MICROSOFT IGNITE PRESENTATION (May 5, 2015); Chris McNulty and Pracheeti Nagarkar Desai, *Elastic SharePoint Storage with StorSimple and Microsoft Azure*, MICROSOFT IGNITE PRESENTATION (May 8, 2015); Sharon Smith, *StorSimple Security and Data Protection*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (September 25, 2015).

Enlightened Client programs and services (“Microsoft Azure RMS Clients”)⁹⁰ (collectively, the “Azure and Office 365 RMS System”).

391. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure StorSimple (“StorSimple”).⁹¹

392. On information and belief, Azure and Office 365 RMS System and StorSimple (collectively, the “Microsoft ‘017 Products”) include encryption technology.

393. On information and belief, on or more of the Microsoft ‘017 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

394. On information and belief, the Microsoft ‘017 Products are available to businesses and individuals throughout the United States.

395. On information and belief, the Microsoft ‘017 Products are available to businesses and individuals located in the Eastern District of Texas.

396. On information and belief, one or more of the Microsoft ‘017 Products receive information to be processed from a sending device.

397. On information and belief, the Azure and Office 365 RMS System enables a first Microsoft Azure RMS user (e.g., a Word document author/owner or Outlook message sender) to

⁹⁰ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as “enlightened” clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

⁹¹ Microsoft Azure StorSimple is storage product that manages storage tasks between on-premises devices and Microsoft Azure cloud storage. The accused Microsoft Azure StorSimple product is comprised of one or more of the following components: a StorSimple device (StorSimple series 8000 devices), a StorSimple virtual device, Windows PowerShell for StorSimple, Azure PowerShell StorSimple cmdlets, StorSimple Manager Service, StorSimple Snapshot Manager, and StorSimple Adapter for SharePoint. A description of the components of Microsoft Azure StorSimple is available at: <https://azure.microsoft.com/en-us/documentation/articles/storsimple-components/>.

protect Office 365 information (e.g., a Word document or Outlook message). Microsoft Azure RMS defines a cryptographic comprehension function for the information based on, e.g., a symmetric (e.g., AES) content key encrypted with an asymmetric (e.g., RSA) public key of the first Microsoft Azure RMS user. The cryptographic comprehension function is adapted for making at least a portion of the Office 365 information (e.g., at least a portion of the Word document or Outlook message) incomprehensible.

398. On information and belief, the Azure and Office 365 RMS system enables a second Azure RMS user (e.g., a recipient and/or requestor of the Office 365 information (e.g., Word document or Outlook message)) to consume the protected Office 365 information (e.g., Word document or Outlook message). To allow a second RMS user to consume the protected information the Azure and Microsoft 365 RMS system receives asymmetric cryptographic key information (e.g., RSA public key information for the first Azure RMS user and the second Azure RMS user, respectively). The asymmetric cryptographic key information comprises at least asymmetric encryption key information (e.g., RSA public key information for the second Azure RMS user) and asymmetric decryption key information (e.g., RSA public key information for the first Azure RMS user).

399. On information and belief, the Azure and Office 365 RMS System negotiates a new cryptographic comprehension function between two parties (e.g., the first Azure RMS user and the second Azure RMS user) to a communication (e.g., communicating the Office 365 information (e.g., the Word document or Outlook message) between the first Azure RMS user and the second Azure RMS user). The Azure RMS service acts as an intermediary between the first Azure RMS user and the second Azure RMS user with respect to the communication.

400. On information and belief, the Azure and Office 365 RMS System inverts the cryptographic comprehension function and imposes 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. For example, Microsoft Azure RMS processes

the Office 365 information (e.g., the Word document or Outlook message) 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 (e.g., the RSA public key information of the first Azure RMS user and the second Azure RMS user, respectively), without providing the Azure RMS intermediary with sufficient asymmetric cryptographic key information to decrypt the processed information.

401. On information and belief, the second Microsoft Azure RMS user's RSA public key information to decrypt the processed Office 365 information (e.g., the processed Word document or Outlook message) can change dynamically.

402. On information and belief, the Azure and Office 365 RMS System includes robust logging functionality.

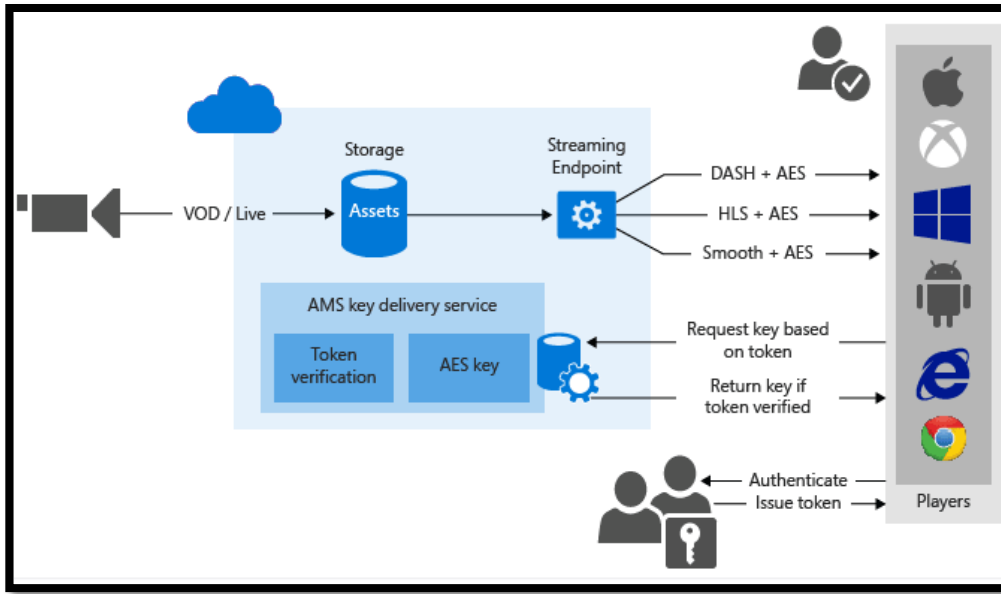
403. On information and belief, the Azure and Office 365 RMS System enables time-based restrictions on cryptographic access by the second Microsoft Azure RMS user—i.e., time-based restrictions on the ability of the asymmetric decryption key information to decrypt the processed information.

404. On information and belief, one or more the Microsoft '017 Products support RSA Transcription where the security is derived from prime factoring asymmetry.

405. On information and belief, Microsoft Azure Media Services enables content to be encrypted dynamically with Advanced Encryption Standard (AES) (using 128-bit encryption keys).

406. On information and belief, the Azure and Office 365 RMS System enables AES content key information to be received by Microsoft Azure RMS. The comprehension function comprises an RSA type encryption algorithm employing a composite key defined by a function of a public key and a private key

407. The below diagram from Microsoft's Azure Media Services documentation shows how Azure Media Services encrypts data using AES-128 and delivers keys for controlling authorized access.



Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015).

408. On information and belief, Microsoft Azure Media Services encrypts an asset by associating an encryption key with the asset (CommonEncryption or Envelope Encryption) and configuring authorization policies for the key.

409. On information and belief, Microsoft Azure RMS stores a record (e.g., an Office 365 document) in a first encrypted format—e.g., an encrypted format based on a symmetric (AES) content key and a first Microsoft Azure RMS user's asymmetric (RSA) public-private key pair, wherein the first Microsoft Azure RMS user's asymmetric (RSA) private key is used for encryption in the first encrypted format.

410. On information and belief, Microsoft Azure RMS financially accounts for a transaction (e.g., a request by an identified Azure user) involving the record (e.g., the Office 365 document) by implementing an Microsoft Azure RMS license check and (depending on the result) enabling an RMS license purchase/transfer or logging a licensed RMS request.

411. On information and belief, Microsoft Azure RMS, acting as an intermediary, securely negotiates with the second Azure RMS user a decryption key for the record (e.g., Office 365 document). The decryption key is based on the second Azure RMS user's RSA private key, and is thereby different than an associated decryption key for the record (e.g., Office 365

document) in the first encrypted format (for example, a decryption key based on the first Azure RMS user's RSA public key).

412. On information and belief, the Microsoft '017 Products convert a record to a second encrypted format, without being represented in an unencrypted state during transition from the first encrypted format to the second encrypted format, and without providing sufficient information at the site of the conversion to enable decryption of the record from the first or second encrypted format before, during or after conversion, such that the negotiated decryption key is selectively operative to decrypt the record in the second encrypted format.

413. On information and belief, the Azure and Office 365 RMS System converts the record (e.g., Office 365 document) to a second encrypted format (an encrypted format based on a symmetric (AES) content key and the second Azure RMS user's asymmetric (RSA) public key), without being represented in an unencrypted state during transition from the first encrypted format to the second encrypted format, and without providing sufficient information at the site of the conversion (e.g., an Azure RMS client) to enable decryption of the record from the first or second encrypted format before, during or after conversion, such that the negotiated decryption key (e.g., the decryption key based on the second Azure RMS user's RSA private key) is selectively operative to decrypt the record in the second encrypted format.

414. On information and belief, the Azure and Office 365 RMS System communicates the record (e.g., Office 365 document) encrypted in the second encrypted format (e.g., an encrypted format based on the second Azure RMS user's RSA public key) to the requestor (e.g., the second Azure RMS user), without passing the record (e.g., Office 365 document) through the intermediary (e.g., the Azure RMS server).

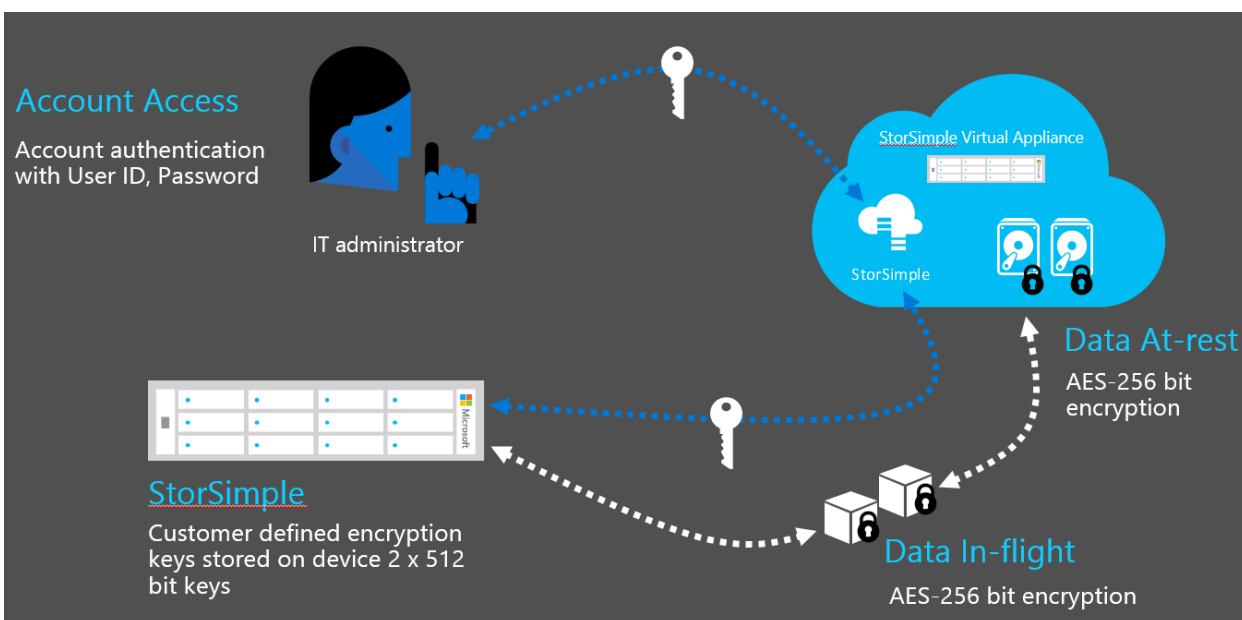
415. On information and belief, the Azure and Office 365 RMS System enables the Microsoft Azure RMS agent on a requestor's (e.g., second Azure RMS user's) computer or mobile device decrypts the record (e.g., Office 365 document) in the second encrypted format (e.g., the encrypted format based on the second Azure RMS user's RSA public key) based on the

negotiated decryption key (e.g., the decryption key based on the second Azure RMS user's RSA private key).

416. On information and belief, Microsoft Azure Media Services decrypts protected media content by sending (via the key delivery service) a key (requested by the client device) to the client.

417. On information and belief, Microsoft Azure Media Services enable content authorization using (in part) AES Clear Key Encryption.

418. On information and belief, StorSimple encrypts data in transit and at rest in the "cloud" using (in part) the AES-256 encryption algorithm. For example, StorSimple transmission of data between the StorSimple system and Windows Azure Storage is encrypted using AES-256 encryption. StorSimple's encryption of data in transit is distinct from the storage access keys and data at-rest encryption. Data at rest is encrypted by the StorSimple system with a customer-provided encryption key using standard AES-256 encryption that is derived from a customer passphrase or generated by a key management system.

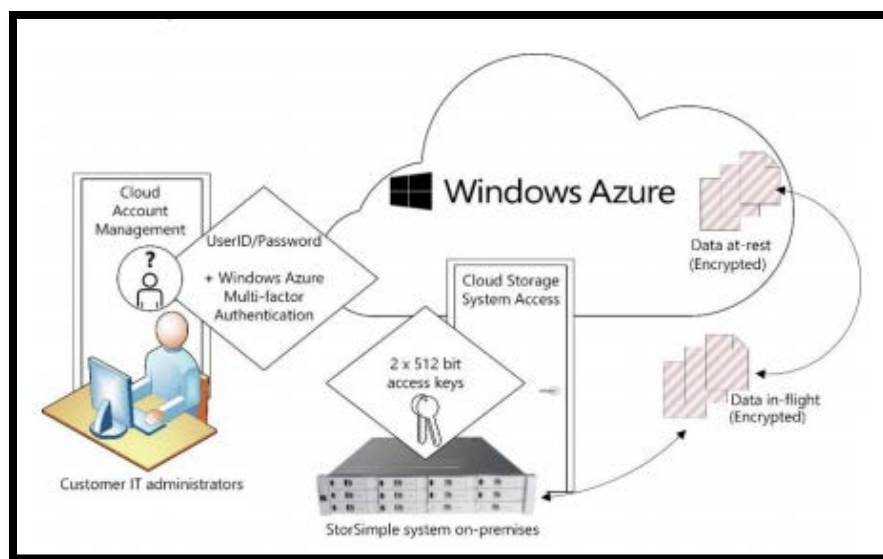


Chris McNulty and Pracheeti Nagarkar Desai, *Elastic SharePoint Storage with StorSimple and Microsoft Azure* at 10, MICROSOFT IGNITE PRESENTATION (May 8, 2015) (showing how StorSimple encrypts data "in-flight" and "at-rest").

419. On information and belief, StorSimple encrypts CHAP passwords and data encryption keys using the RSA-2048 encryption algorithm (an asymmetric public-private key).

420. On information and belief, StorSimple uses a system of asymmetric key pairs to prevent compromising stored information if the Azure service is compromised. Specifically, a client device in StorSimple system generates a data encryption certificate that uses an asymmetric public and private key pair to protect data. The asymmetric keys are generated when a client device is registered. The data encryption certificate is then exported into a Personal Information Exchange (.pfx) file that is protected by the service data encryption key, which is a strong 128-bit key randomly generated by the first device during registration. The StorSimple system then makes the public key of the data encryption certificate available to the StorSimple Manager service (the private key remains on the StorSimple client device). Secure data entering the StorSimple system is then encrypted using the public key and decrypted using the private key stored on the StorSimple client device - ensuring Microsoft Azure (the intermediary) cannot decrypt the data flowing to the StorSimple client device.

421. The below diagram from Microsoft's Azure StorSimple Security Brief shows the high-level architecture of StorSimple.



Microsoft StorSimple: Hybrid Cloud Storage Security at 1, MICROSOFT AZURE STORSIMPLE SECURITY BRIEF (2014).

422. On information and belief, Microsoft has directly infringed and continues to directly infringe the '017 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 Microsoft '017 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure Media Services, Microsoft Azure RMS, Microsoft Office 365, Microsoft Azure RMS Clients, and StorSimple.

423. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Microsoft '017 Products, Microsoft has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '017 patent, including at least claims 1-5, 8-9, 11-12, 14, and 20-21, pursuant to 35 U.S.C. § 271(a).

424. On information and belief, Microsoft also indirectly infringes the '017 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint.

425. On information and belief, Microsoft has had knowledge of the '017 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '017 patent and knew of its infringement, including by way of this lawsuit.

426. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '017 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '017 patent. Microsoft 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, Microsoft provides the Microsoft '017 Products that have the capability of operating in a manner that infringe one or more of the claims of the '017 patent, including at least claims 1-5, 8-9, 11-12, 14, and 20-21, and Microsoft further provides

documentation and training materials that cause customers and end users of the Microsoft '017 Products to utilize the products in a manner that directly infringe one or more claims of the '017 patent. By providing instruction and training to customers and end-users on how to use the Microsoft '017 Products in a manner that directly infringes one or more claims of the '017 patent, including at least claims 1-5, 8-9, 11-12, 14, and 20-21, Microsoft specifically intended to induce infringement of the '017 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '017 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '017 patent.⁹² Accordingly, Microsoft 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.

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

428. As a result of Microsoft's infringement of the '017 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's

⁹² *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Sharon Smith, *Microsoft Azure StorSimple Security*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Sharon Smith, *StorSimple 8000 Series: A Hybrid Cloud Storage Solution*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); *Microsoft StorSimple: Hybrid Cloud Storage Security*, MICROSOFT STORSIMPLE SECURITY BRIEF (2014); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); Ben Watson, *StorSimple & Windows Azure Cloud-Integrated Storage*, MSDN CHANNEL 9 PRESENTATION (June 18, 2014); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015); Meghan Liese et al., *StorSimple: Extending Your Datacenter Into Microsoft Azure With Hybrid Cloud Storage*, MICROSOFT IGNITE PRESENTATION (May 5, 2015); Chris McNulty and Pracheeti Nagarkar Desai, *Elastic SharePoint Storage with StorSimple and Microsoft Azure*, MICROSOFT IGNITE PRESENTATION (May 8, 2015); Sharon Smith, *StorSimple Security and Data Protection*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (September 25, 2015).

infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

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

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

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

431. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management (“Microsoft Azure RMS”), Microsoft Azure Media Services (“Microsoft Azure Media Services”); Microsoft Office 365 (“Microsoft Office 365”); and Microsoft Azure RMS Enlightened Client programs and services (“Microsoft Azure RMS Clients”)⁹³ (collectively, the “Azure and Office 365 RMS System” or “Microsoft ‘591 Products”).

432. On information and belief, the Azure and Office 365 RMS System includes encryption technology.

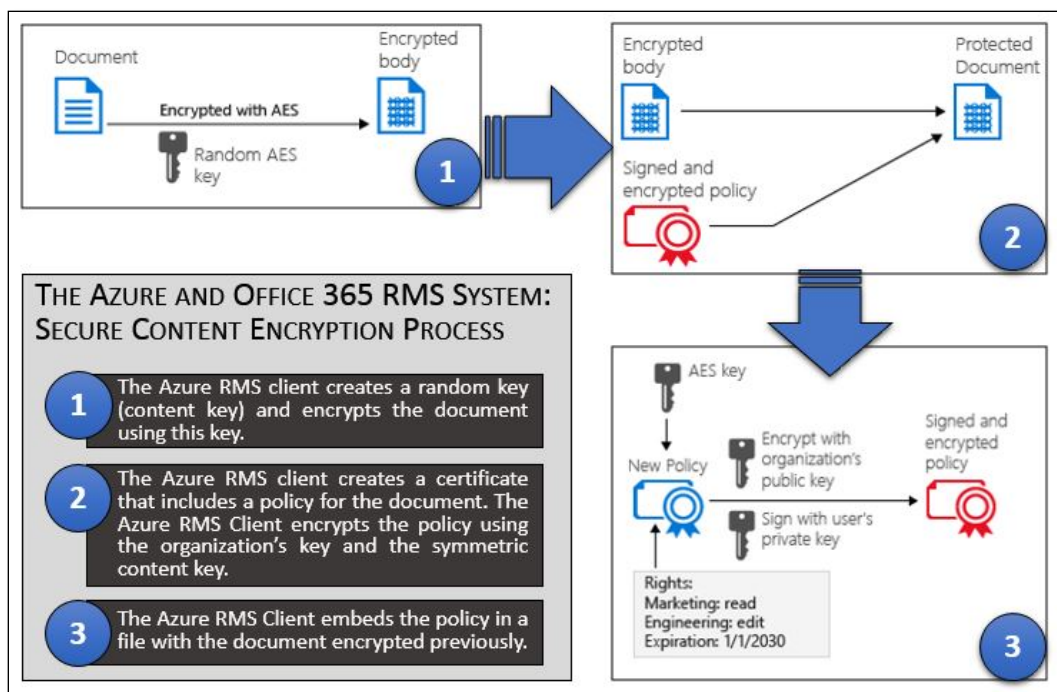
433. On information and belief, the Azure and Office 365 RMS System performs a method for transcribing information. For example, through Microsoft Azure RMS and integrated applications and/or services (e.g., Office 365),⁹⁴ Microsoft transcribes information (e.g., an Office 365 document) from a form associated with a first set of cryptographic keys (e.g.,

⁹³ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as “enlightened” clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

⁹⁴ Although this chart focuses specifically on Microsoft Azure RMS, on information and belief other Microsoft cloud services—including, e.g., at least Azure Media Services and Office 365—operate materially similar to Azure RMS with respect to infringement of this patent. *See, e.g.*, <https://technet.microsoft.com/en-us/library/jj585004.aspx> (describing how Microsoft cloud applications, including Office 365, support Azure Rights Management).

a first Microsoft Azure RMS user's RSA public-private keys) to a form associated with a second set of cryptographic keys (e.g., a second Microsoft Azure RMS user's RSA public-private keys).

434. On information and belief, the Azure and Office 365 RMS System receives and stores 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.

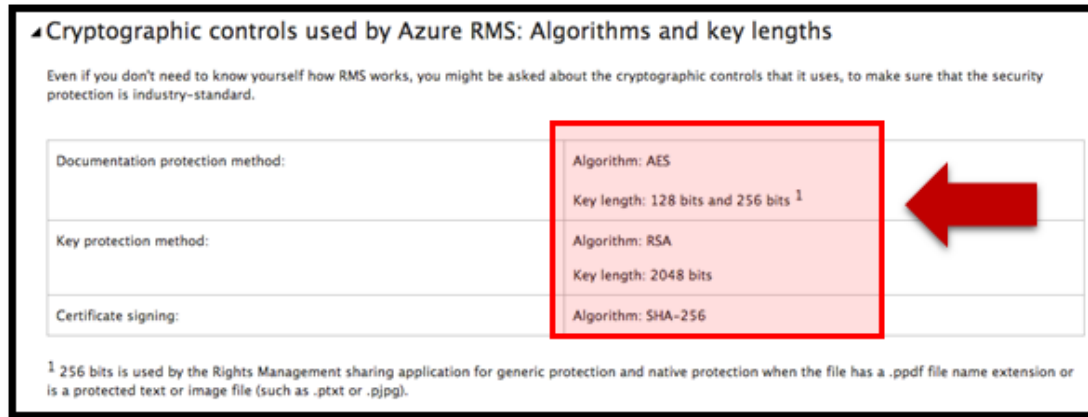


The above figure is based on information contained in *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

435. On information and belief, Microsoft Azure RMS receives and stores in a first memory (e.g., a first Microsoft Azure RMS client) information (e.g., an Office 365 document) encrypted based on a first set of cryptographic keys (e.g., a first Microsoft Azure RMS user's set of RSA asymmetric keys), a first portion of the first set of cryptographic keys (e.g., a private key portion of the first Microsoft Azure RMS user's set of RSA asymmetric keys) having been employed to produce the encrypted information and a second portion of the first set of cryptographic keys (e.g., a public key portion of the first Microsoft Azure RMS user's set of

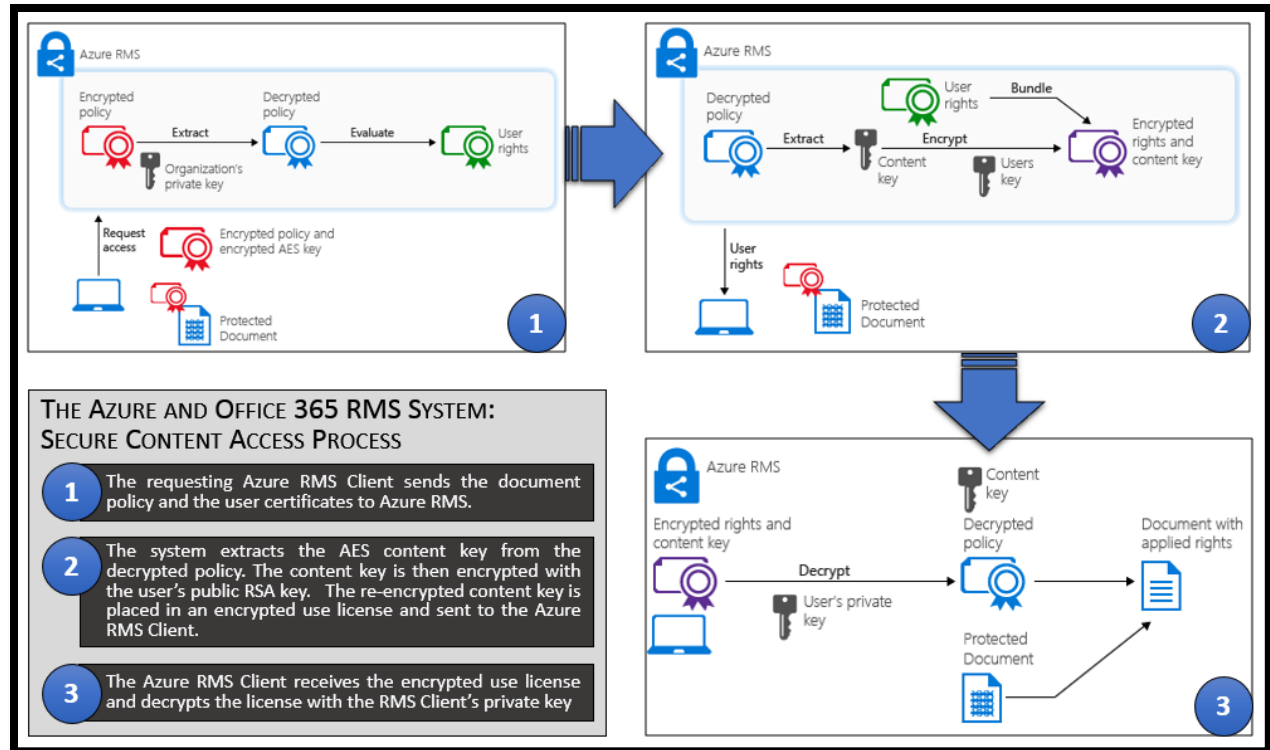
RSA asymmetric keys) being required to decrypt the information encrypted with the first portion of the first set of cryptographic information.

436. The below excerpt from Microsoft Azure RMS documentation shows the encryption algorithms used by Microsoft Azure RMS to protect secure data.



What is Azure Rights Management?, Microsoft TechNet Article (July 1, 2015) (red arrow indicating the algorithms and key lengths employed by Microsoft Azure RMS).

437. On information and belief, the Azure and Office 365 RMS System receives and stores 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 with the first portion of the second set of cryptographic keys. For example, Microsoft Azure RMS receives and stores in a second memory (e.g., a second Microsoft Azure RMS client) a first portion of a second set of cryptographic keys (e.g., a second Microsoft Azure RMS user's set of RSA asymmetric keys), a having a corresponding second portion of the second set of cryptographic keys (e.g., a private key portion of the second Microsoft Azure RMS user's set of RSA asymmetric keys) being required for decryption of a message (e.g., an Office 365 document message) encrypted with the first portion of the second set of cryptographic keys (e.g., a public key portion of the second Microsoft Azure RMS user's set of RSA asymmetric keys).



The above figure is based on information contained in *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

438. On information and belief, Microsoft Azure RMS negotiates a set of session keys (e.g., ephemeral/PFS transport keys) through a communication port.

439. On information and belief, the Azure and Office 365 RMS System generates a transcription key for transforming the received encrypted information to transcribed information in dependence on at least information representing the second portion of the first set of cryptographic keys, information representing the first portion of the second set of cryptographic keys, and a first portion of the set of session keys.

440. On information and belief, Microsoft Azure RMS generates a transcription key for transforming the received encrypted information (e.g., Office 365 document) to transcribed information in dependence on at least information representing the second portion of the first set of cryptographic keys (e.g., the public key portion of the first Microsoft Azure RMS user's set of RSA asymmetric keys), information representing the first portion of the second set of cryptographic keys (e.g., the public key portion of the second Microsoft Azure RMS user's set of

RSA asymmetric keys), and a first portion of the set of session keys (e.g., the negotiated ephemeral/PFS transport keys).

441. On information and belief, the Azure and Office 365 RMS System transcribes the stored encrypted information into transcribed information using the transcription key. For example, Microsoft Azure RMS transcribes the stored encrypted information (the stored Office 365 document information, encrypted based on the first Microsoft Azure RMS user's set of RSA keys) into transcribed information (e.g., the Office 365 document information, encrypted based on the second Microsoft Azure RMS user's set of RSA keys) using the transcription key.

442. On information and belief, the Azure and Office 365 RMS System generates a transcription key and transcribes the encrypted information without either requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcribed information. For example, Microsoft Azure RMS generates a transcription key and transcribes the encrypted information without either requiring or employing sufficient information either to decrypt the encrypted information (e.g., the encrypted Office 365 document information) or to comprehend the transcribed information (e.g., the transcribed Office 365 document information).

443. On information and belief, the first and second set of cryptographic keys employed by the Azure and Office 365 RMS System are each key pairs related through RSA.

444. On information and belief, the Azure and Office 365 RMS system enables a second Microsoft Azure RMS user to ultimately decrypt information, using (at least) the recited RSA-plus-session key information.

445. On information and belief, the Azure and Office 365 RMS System is configured so that a first and second Microsoft Azure RMS user does not exchange sufficient cryptographic information with one another to decrypt the encrypted information or comprehend the transcribed information.

446. On information and belief, session keys in the Azure and Office 365 RMS System are dynamically generated for use in conjunction with communication session. It is

computationally infeasible to compute first Microsoft Azure RMS user's RSA private key from the transcription key (derived only from the public key portion of the first Microsoft Azure RMS user's RSA key pair) and the second Microsoft Azure RMS user's set of RSA keys.

447. On information and belief, session keys in the Azure and Office 365 RMS System are negotiated through a communication port with second Microsoft Azure RMS user.

448. On information and belief, Microsoft Azure Media Services receives and stores 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).

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

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

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

452. On information and belief, Microsoft has directly infringed and continues to directly infringe the '591 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 Microsoft '591 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure RMS, Microsoft Azure Media Services, Microsoft Office 365, and Microsoft Azure RMS Enlightened Client programs and services. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Microsoft '591

Products, Microsoft has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '591 patent, including at least claims 13-14, 17-18 and 20-21, pursuant to 35 U.S.C. § 271(a).

453. On information and belief, Microsoft also indirectly infringes the '591 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint. Microsoft has had knowledge of the '591 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '591 patent and knew of its infringement, including by way of this lawsuit.

454. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '591 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '591 patent. Microsoft 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, Microsoft provides the Microsoft '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 claims 13-14, 17-18 and 20-21, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '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 Microsoft '591 Products in a manner that directly infringes one or more claims of the '591 patent, including at least claims 13-14, 17-18 and 20-21, Microsoft specifically intended to induce infringement of the '591 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '591 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused

products to infringe the '591 patent.⁹⁵ Accordingly, Microsoft 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.

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

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

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

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

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

459. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Key Vault ("Microsoft Azure Key Vault").

460. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Media Services ("Microsoft Azure Media Services"); Microsoft Office 365 ("Microsoft Office 365"); and Microsoft Azure RMS

⁹⁵ *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015).

Enlightened Client programs and services (“Microsoft Azure RMS Clients”)⁹⁶ (collectively, the “Azure and Office 365 RMS System”).

461. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure StorSimple (“StorSimple”).⁹⁷

462. On information and belief, Microsoft Azure Key Vault, the Azure and Office 365 RMS System, and StorSimple (collectively, the “Microsoft ‘181 Products’”) include encryption technology.

463. On information and belief, the Microsoft ‘181 Products are available to businesses and individuals throughout the United States.

464. On information and belief, the Microsoft ‘181 Products are available to businesses and individuals located in the Eastern District of Texas.

465. On information and belief, Microsoft Azure Key Vault includes encryption technology.

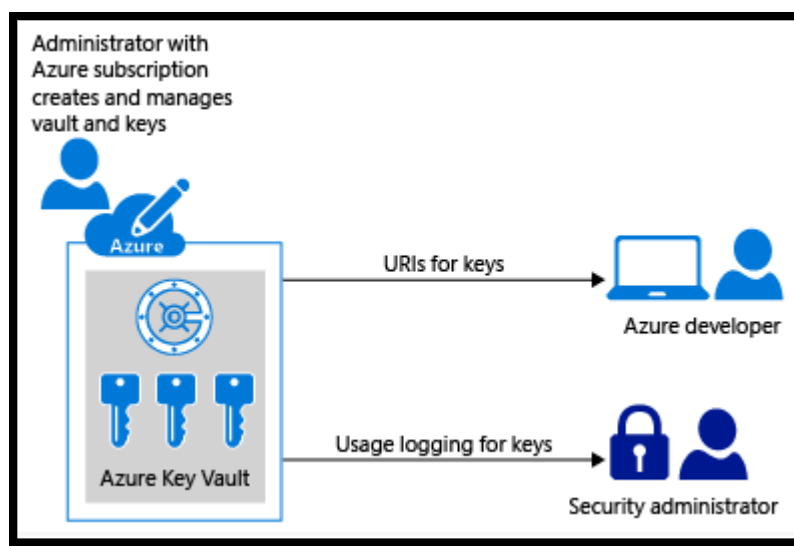
466. On information and belief, Microsoft Azure Key Vault enables sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

⁹⁶ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as “enlightened” clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

⁹⁷ Microsoft Azure StorSimple is storage product that manages storage tasks between on-premises devices and Microsoft Azure cloud storage. The accused Microsoft Azure StorSimple product is comprised of one or more of the following components: a StorSimple device (StorSimple series 8000 devices), a StorSimple virtual device, Windows PowerShell for StorSimple, Azure PowerShell StorSimple cmdlets, StorSimple Manager Service, StorSimple Snapshot Manager, and StorSimple Adapter for SharePoint. A description of the components of Microsoft Azure StorSimple is available at: <https://azure.microsoft.com/en-us/documentation/articles/storsimple-components/>.

467. On information and belief, the Microsoft Azure Key Vault comprises a key handler. For example, the Microsoft Azure Key Vault includes logic and hardware for securely handling customers' cryptographic keys in the cloud.

468. On information and belief, the Microsoft Azure Key Vault 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. For example, the Microsoft Azure Key Vault comprises an interface to a memory (e.g., an encrypted data store on a Microsoft Azure Key Vault server) that stores a plurality of encrypted cryptographic key records.



Carol Bailey, *What is Azure Key Vault?*, MICROSOFT AZURE KEY VAULT DOCUMENTATION (Sept. 22, 2015).

469. Upon information and belief, Microsoft Azure Key Vault comprises a system where each encrypted cryptographic key record has at least one associated asymmetric encryption key pair (e.g., an associated ElGamal, RSA, and/or Diffie-Hellman public key-secret key pair) and is encrypted with a first component of the associated asymmetric encryption key pair. For example, upon information and belief, Microsoft Azure Key Vault uses asymmetric encryption keys to “wrap” stored cryptographic key records in a manner that facilitates identity-based access controls and usage auditing for the keys. Additionally and/or in the alternative,

upon information and belief, each Microsoft Azure Key Vault cryptographic key record has at least one associated digital signature comprising information (e.g., a cryptographic hash of the record contents) encrypted with a first component of an associated asymmetric key pair (e.g., an RSA private key).

470. On information and belief, the Microsoft Azure Key Vault 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 transcription key derived at least in part from the at least one asymmetric session key. For example, the Microsoft Azure Key Vault includes at least one automated processor operating in a privileged processing environment to securely retrieve, provision, and communicate cryptographic key information on behalf of remote customers. More specifically, upon information and belief, the Microsoft Azure Key Vault system includes at least one privileged-mode automated processor in the Azure Key Vault system key server that is configured to:

- retrieve a selected encrypted key record from the memory (e.g., the encrypted data store on an Microsoft Azure Key Vault key server);
- negotiate at least one asymmetric session key with a remote customer system (e.g., an authenticated cloud consumer virtual machine environment), and transcrypt the encrypted key record from its server-encrypted (e.g., “wrapped”) form into a session-encrypted form suitable for secure encryption/decryption of customer data.

471. On information and belief, Microsoft Azure Key Vault transcrypts the encrypted key record from server-encrypted (e.g., “wrapped”) form into session-encrypted form in an integral process substantially without intermediate decryption. More specifically, the Microsoft Azure Key Vault key server uses a transcription key derived at least in part from the at least one asymmetric session key to securely transcrypt the encrypted key record from server-encrypted (e.g., “wrapped”) form into session-encrypted form.

472. On information and belief, the Microsoft Azure Key Vault comprises a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcribed record. For example, Microsoft Azure Key Vault comprises at least one communication port configured to conduct the negotiation between the Microsoft Azure Key Vault key server and the authenticated cloud consumer virtual machine environment for the at least one asymmetric session key

473. On information and belief, the Microsoft Azure Key Vault comprises a communication port configured to communicate the transcribed record—e.g., by transmitting the transcribed cryptographic key record from the privileged processing environment in the Microsoft Azure Key Vault key server to a remote stream processor for transparent encryption/decryption of cloud data.

474. On information and belief, the Microsoft Azure Key Vault key server is configured to communicate with the Azure Key Vault key store server through one of at least two types of virtual private networks (e.g., SSL VPN and IPsec VPN).

475. On information and belief, the Azure and Office 365 RMS System comprises a key handler. For example, Microsoft Azure RMS includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual Hardened Security Appliance (“HSA”) in the Microsoft Azure cloud) that is configured to handle keys (e.g., Microsoft Azure RMS cryptographic keys).

476. On information and belief, the Azure and Office 365 RMS System includes a key handler comprising 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. For example, the Microsoft Azure RMS includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual HSA in the Microsoft Azure cloud) comprising an interface to a memory (e.g., a wired and/or wireless network interface to a Microsoft Azure RMS Key Vault) which stores a plurality of encrypted records (e.g., a plurality of encrypted Microsoft Azure RMS content key

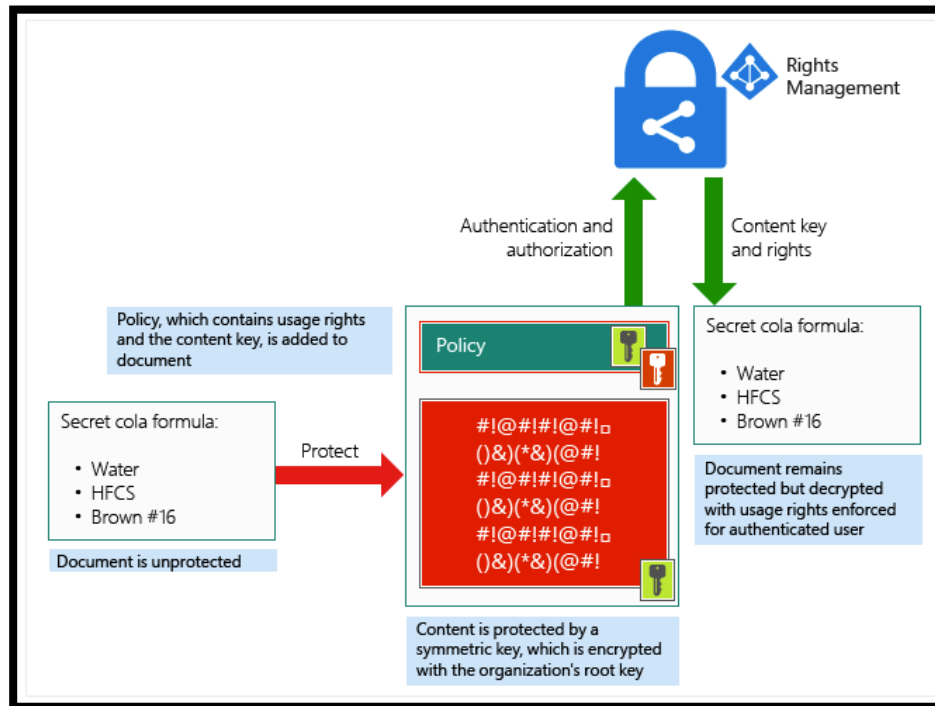
records). Each encrypted record (e.g., encrypted Microsoft Azure RMS content key record) has an associated asymmetric encryption key pair (e.g., a first Microsoft Azure RMS user's RSA key pair) and is encrypted with a first component of the associated asymmetric encryption key pair (e.g., a private key component of the first Microsoft Azure RMS user's RSA key pair).

477. On information and belief, the Azure and Office 365 RMS System includes a 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 transcribe the encrypted message to a transcribed message in an integral process substantially without intermediate decryption, using a transcription key derived at least in part from the at least one asymmetric key.

478. On information and belief, the Azure and Office 365 RMS System includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual HSA in the Azure cloud) comprising at least one automated processor, operating in a privileged processing environment (e.g., a privileged Security World in the HSA), configured to receive a selected encrypted record (e.g., a selected encrypted Microsoft Azure RMS content key record) from the memory (e.g., the Microsoft Azure RMS Key Vault) through the interface, to negotiate at least one asymmetric session key (e.g., an asymmetric session key having as components information associated with the second Microsoft Azure RMS user's RSA public key and information associated with a set of ephemeral/PFS transport keys interactively negotiated between the Microsoft Azure RMS key handler and the second Microsoft Azure RMS user), and to transcribe the encrypted message (e.g., the encrypted Microsoft Azure RMS content key, encrypted with a private key component of the first Microsoft Azure RMS user's RSA key pair) to a transcribed message (e.g., the transcribed Microsoft Azure RMS content key, (now) encrypted with a public key component of the second Microsoft Azure RMS user's RSA key pair) in an integral process substantially without intermediate decryption, using a transcription key (e.g., a cryptographic key having as components information associated with the first Microsoft Azure

RMS user's RSA public key; information associated with the second Microsoft Azure RMS user's RSA public key; and information associated with the set of ephemeral/PFS transport keys interactively negotiated between the Microsoft Azure RMS key handler and the second Microsoft Azure RMS user).

479. The below diagram from Microsoft technical documentation shows the encryption system used by the Azure and Office 365 RMS System.



What is Azure Rights Management?, MICROSOFT TECHNET ARTICLE (July 1, 2015).

480. On information and belief, the Azure and Office 365 RMS System generates a transcription key (e.g., the cryptographic key having as components information associated with the first Microsoft Azure RMS user's RSA public key; information associated with the second Microsoft Azure RMS user's RSA public key; and information associated with the set of ephemeral/PFS transport keys interactively negotiated between the Microsoft Azure RMS key handler and the second Microsoft Azure RMS user) is derived at least in part from the at least one asymmetric session key (e.g., the asymmetric session key having as components information associated with the second Microsoft Azure RMS user's RSA public key and information

associated with the set of ephemeral/PFS transport keys interactively negotiated between the Microsoft Azure RMS key handler and the second Microsoft Azure RMS user).

481. On information and belief, the Azure and Office 365 RMS System includes a key handler comprising a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcribed record.

482. On information and belief, Microsoft Azure RMS includes at least one device (e.g., a Microsoft-designed and -managed physical and/or virtual HSA in the Microsoft Azure cloud) comprising a communication port (e.g., a wired and/or wireless network interface to at least the second Microsoft Azure RMS user (via, e.g., Microsoft Azure RMS client programming on the second Microsoft Azure RMS user's computer or mobile device)) configured to conduct the negotiation for the at least one asymmetric session key (e.g., the asymmetric session key having as components information associated with the second Microsoft Azure RMS user's RSA public key and information associated with the set of ephemeral/PFS transport keys interactively negotiated between the Microsoft Azure RMS key handler and the second Microsoft Azure RMS user), and to communicate the transcribed record (e.g., the transcribed Microsoft Azure RMS content key, (now) encrypted with a public key component of the second Microsoft Azure RMS user's RSA key pair).

483. Documentation for the Azure and Office 365 RMS System describes the rights management functionality of the Azure and Office 365 RMS system as preventing Microsoft from gaining access to decrypted secure data.

One important thing to understand about how Azure RMS works is that the Rights Management service (and Microsoft) do not see or store your data as part of the information protection process. Information that you protect is never sent to or stored in Azure unless you explicitly store it in Azure or use another cloud service that stores it in Azure. Azure RMS simply makes the data in a document unreadable to anyone other than authorized users and services:

- The data is encrypted at the application level and includes a policy that defines the authorized use for that document.
- When a protected document is used by a legitimate user or it is processed by an authorized service, the data in the document is decrypted and the rights that are defined in the policy are enforced.

What is Azure Rights Management?, Microsoft TechNet Article (July 1, 2015).

484. On information and belief, the Azure and Office 365 RMS System utilizes a transcription key that has as components at least a public key component of the first Microsoft Azure RMS user's associated RSA key pair, and the at least one asymmetric session key, to result in a transcribed message encrypted with at least one asymmetric session key.

485. On information and belief, the Azure and Office 365 RMS System comprises a Microsoft Azure RMS key handler configured to communicate with the Microsoft Azure RMS Key Vault through a Microsoft VPN.

486. On information and belief, the Azure and Office 365 RMS System comprises an associated asymmetric key pair that is a Rivest-Shamir-Adler type key. For example, the first Microsoft Azure RMS user's associated asymmetric key pair comprises an RSA-type key.

487. On information and belief, StorSimple comprises a key handler. For example, the StorSimple Manager service uses asymmetric key pairs to ensure that protected data is not comprised even if the Microsoft Azure system is compromised.

488. On information and belief, StorSimple comprises an interface to a memory which stores a plurality of encrypted records (e.g., storage account credentials, StorSimple device configuration, and cloud storage encryption keys). Each record has an associated asymmetric key pair (e.g., RSA-2048 key pair) and is encrypted with a first component of the associated asymmetric encryption key pair. StorSimple includes a network interface configuration menu that comprises an interface to a memory where the plurality of encrypted records are stored.



Alpa Kohli, *Deploy Your On-Premises StorSimple Device (Update 1)*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (September 17, 2015).

489. On information and belief, StorSimple comprises at least one processor that is configured to receive a selected encryption record from the memory. Specifically, a client device in the StorSimple system generates a data encryption certificate that uses an asymmetric public and private key pair to protect data. The asymmetric keys are generated when a client device is registered. The data encryption certificate is then exported into a Personal Information Exchange (.pfx) file that is protected by the service data encryption key, which is a strong 128-bit key randomly generated by the first device during registration. The StorSimple system then makes the public key of the data encryption certificate available to the StorSimple Manager service (the private key remains on the StorSimple client device). Secure data entering the StorSimple system is then encrypted using the public key and decrypted using the private key stored on the StorSimple client device - ensuring Microsoft Azure (the intermediary) cannot decrypt the data flowing to the StorSimple client device.

490. On information and belief, StorSimple comprises a communication port configured to conduct the negotiation for the at least one asymmetric session key and communicate the transcribed record. For example, StorSimple documentation establishes that StorSimple comprises a communication port configured to receive the asymmetric session key and communicate the transcribed record.

The primary purpose of the StorSimple Manager service is to manage and configure the StorSimple device. The StorSimple Manager service runs in Microsoft Azure. You use the Azure Management Portal to enter device configuration data, and then Microsoft Azure uses the StorSimple Manager service to send the data to the device. The StorSimple Manager service uses a system of asymmetric key pairs to help ensure that a compromise of the Azure service will not result in a compromise of stored information. The asymmetric key system helps protect the data that flows through the service as follows:

Sharon Smith, *StorSimple Security and Data Protection*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (September 25, 2015).

491. On information and belief, Microsoft has directly infringed and continues to directly infringe the '181 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 Microsoft '181 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure Key Vault, Microsoft Azure Rights Management, Microsoft Azure Media Services, Microsoft Office 365, Microsoft Azure RMS Enlightened Client programs and services, and Microsoft Azure StorSimple.

492. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Microsoft '181 Products, Microsoft 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 1-2, 6, 9, and 18, pursuant to 35 U.S.C. § 271(a).

493. On information and belief, Microsoft also indirectly infringes the '181 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint. Microsoft has had knowledge of the '181 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '181 patent and knew of its infringement, including by way of this lawsuit.

494. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '181 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal

and customary use of the accused products would infringe the ‘181 patent. Microsoft 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, Microsoft provides the Microsoft ‘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 1-2, 6, 9, and 18, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft ‘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 Microsoft ‘181 Products in a manner that directly infringes one or more claims of the ‘181 patent, including at least claims 1-2, 6, 9, and 18, Microsoft specifically intended to induce infringement of the ‘181 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft ‘181 Products, *e.g.*, through Microsoft’s user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘181 patent.⁹⁸ Accordingly, Microsoft has induced and continues to induce users

⁹⁸ See *e.g.*, Carol Bailey, *What is Azure Key Vault?*, MICROSOFT AZURE KEY VAULT DOCUMENTATION (Sept. 22, 2015); Dan Plastina, *Azure Key Vault – Making the Cloud Safer*, THE OFFICIAL AZURE KEY VAULT TEAM BLOG (January 8, 2015); Dan Plastina, *Azure Key Vault – Step by Step*, THE OFFICIAL AZURE KEY VAULT TEAM BLOG (June 2, 2015); *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Sharon Smith, *Microsoft Azure StorSimple Security*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Sharon Smith, *StorSimple 8000 Series: A Hybrid Cloud Storage Solution*, MICROSOFT TECHNICAL DOCUMENTATION (September 25, 2015); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); *Microsoft StorSimple: Hybrid Cloud Storage Security*, MICROSOFT STORSIMPLE SECURITY BRIEF (2014); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); Ben Watson, *StorSimple & Windows Azure Cloud-Integrated Storage*, MSDN CHANNEL 9 PRESENTATION (June 18, 2014); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015); Meghan Liese et al., *StorSimple: Extending Your Datacenter Into Microsoft Azure With Hybrid Cloud Storage*, MICROSOFT IGNITE PRESENTATION (May 5, 2015); Chris McNulty and Pracheeti Nagarkar Desai, *Elastic SharePoint Storage with StorSimple and Microsoft Azure*, MICROSOFT

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.

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

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

COUNT V
INFRINGEMENT OF U.S. PATENT NO. 8,566,247

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

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

499. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Media Services ("Microsoft Azure Media Services"); Microsoft Office 365 ("Microsoft Office 365"); and Microsoft Azure RMS Enlightened Client programs and services ("Microsoft Azure RMS Clients")⁹⁹ (collectively, the "Azure and Office 365 RMS System" or "Microsoft '247 Products").

IGNITE PRESENTATION (May 8, 2015); Sharon Smith, *StorSimple Security and Data Protection*, MICROSOFT AZURE STORSIMPLE DOCUMENTATION (September 25, 2015).

⁹⁹ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as "enlightened" clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS "enlightened" client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS "enlightened" applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

500. On information and belief, the Azure and Office 365 RMS System includes encryption technology.

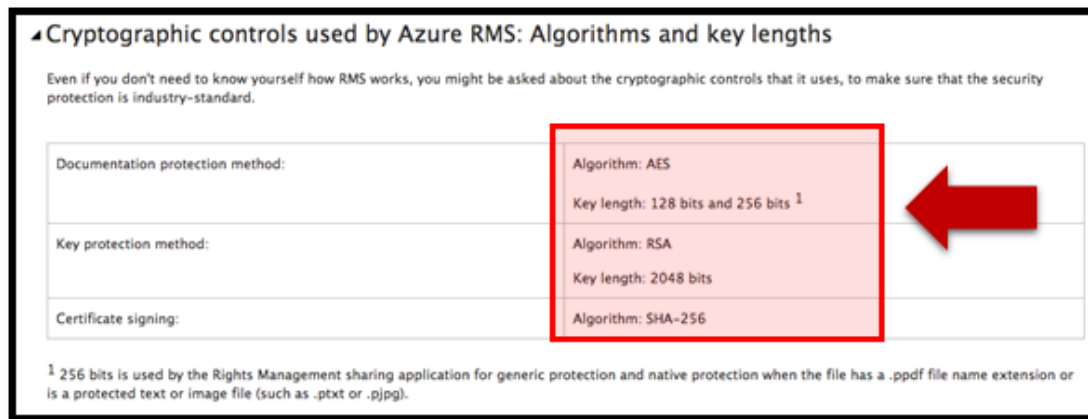
501. On information and belief, the Azure and Office 365 RMS System comprises a system for communicating information that is encrypted from a first party to a second party, involving an intermediary that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information. For example, the Microsoft Azure RMS communicates information which is encrypted (e.g., Office 365 information which is encrypted) from a first party (e.g., a first Microsoft Azure RMS user) to a second party (e.g., a second Microsoft Azure RMS user), involving an intermediary (e.g., the Microsoft Azure RMS key handler) that selectively authorizes the second party to comprehend the information, without the intermediary itself being enabled to comprehend the information.

502. On information and belief, the Azure and Office 365 RMS System contains a communication port which receives information which is to be encrypted to be communicated or an identification thereof, the information being encrypted with an associated cryptographic comprehension function. For example, the Microsoft Azure RMS system comprises a wired and/or wireless network communication port for receiving Office 365 information (or an identification thereof) from a first Microsoft Azure RMS user. The Office 365 information is encrypted to be communicated with an associated cryptographic comprehension function—for example, a cryptographic comprehension function comprising a function of a symmetric content key and a private key component of an RSA key pair associated with the first Microsoft Azure RMS user.

503. On information and belief, the Azure and Office 365 RMS System includes at least one automated processor which conducts a negotiation between the second party and the intermediary through the communication port of an asymmetric delivery comprehension function of the information which is encrypted, different from the associated cryptographic comprehension function, wherein the asymmetric delivery comprehension function comprises a function of at least three asymmetric key components of at least three distinct respective

asymmetric delivery comprehension functions, wherein the second party possesses an ability to decrypt the information which is encrypted with the asymmetric delivery comprehension function, and the intermediary possesses a portion of the asymmetric delivery comprehension function which does not impart an ability to decrypt the information which is encrypted. For example, Microsoft Azure RMS includes at least one automated processor (e.g., an automated processor in a physical and/or virtual HSA associated with the Microsoft Azure RMS key handler intermediary) which conducts a negotiation between the second party (e.g., the second Microsoft Azure RMS user) and the intermediary (e.g., the Microsoft Azure RMS key handler) through the communication port of an asymmetric delivery comprehension function of the information which is encrypted, different from the associated cryptographic comprehension function (e.g., the cryptographic comprehension function comprising a function of a symmetric content key and a private key component of an RSA key pair associated with the first Microsoft Azure RMS user).

504. The below excerpt from Microsoft Azure RMS documentation shows the encryption algorithms used by Microsoft Azure RMS to protect data.



What is Azure Rights Management?, MICROSOFT TECHNET (July 1, 2015) (red arrow indicating the algorithms and key lengths employed by Microsoft Azure RMS).

505. On information and belief, the negotiated asymmetric delivery comprehension function in the Azure and Office 365 RMS System comprises a function of at least three asymmetric key components of at least three different respective asymmetric delivery

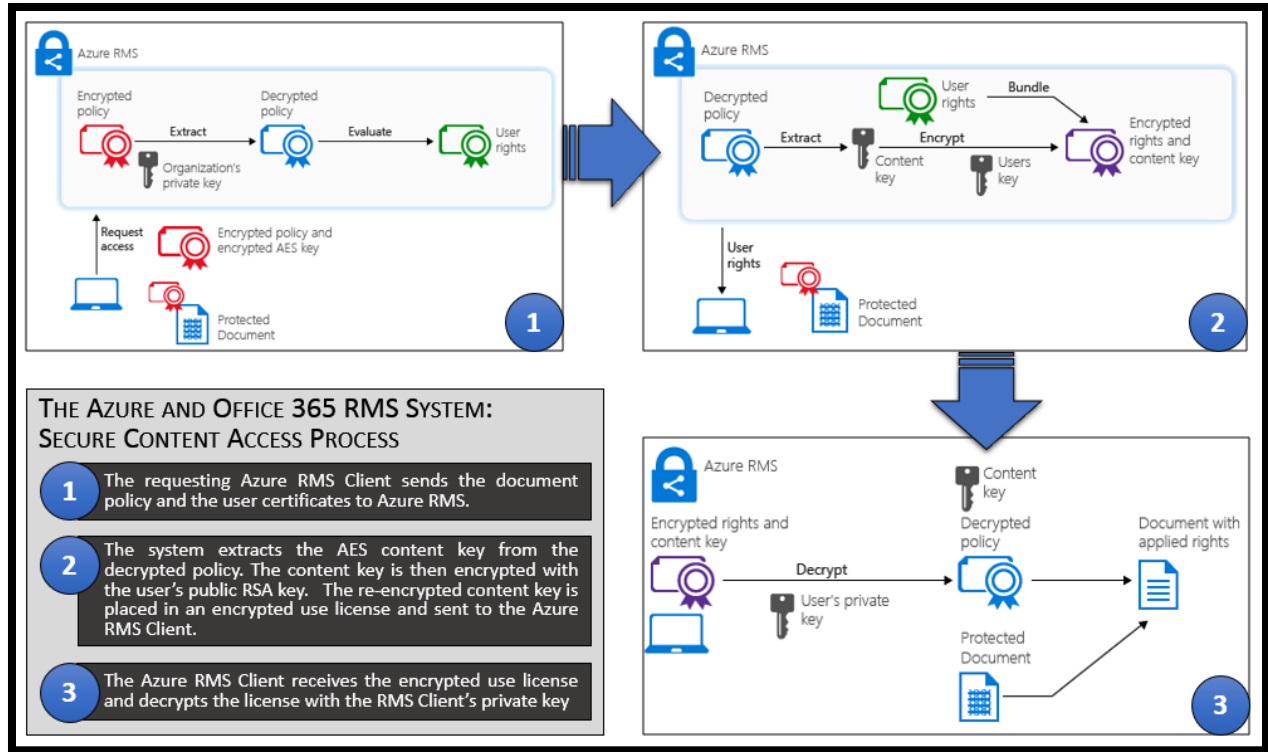
comprehension functions: (1) a public key component of an RSA key pair associated with the second Microsoft Azure RMS user; (2) a private key component of an RSA key pair associated with the first Microsoft Azure RMS user; and (3) a secret key component of an ephemeral/FPS asymmetric (e.g., DHE, ECDHE) session key pair dynamically generated between the Microsoft Azure RMS key handler intermediary and the second Microsoft Azure RMS user.

506. On information and belief, the Microsoft Azure RMS key handler intermediary possesses a portion of the asymmetric delivery comprehension function—the first Microsoft Azure RMS user’s RSA public key—which provides the ability to remove one asymmetric key component of the asymmetric delivery comprehension function (the first Microsoft Azure RMS user’s RSA private key component), but does not impart the ability to decrypt the information which is encrypted. For example, information is still encrypted with two asymmetric key components of the asymmetric delivery comprehension function: the second Microsoft Azure RMS user’s RSA public key component, and the second Microsoft Azure RMS user’s secret key component of the ephemeral/FPS asymmetric (e.g., DHE, ECDHE) session key pair dynamically generated between the Microsoft Azure RMS key handler intermediary and the second Microsoft Azure RMS user. Clearly, the second party (e.g., the second Microsoft Azure RMS user) possesses the ability to remove both remaining asymmetric key components of the asymmetric delivery comprehension function—and thereby possesses (unlike the Microsoft Azure RMS key handler) an ability to decrypt the information which is encrypted with the asymmetric delivery comprehension function.

507. On information and belief, the Azure and Office 365 RMS System includes an automated processor that is configured to transform a comprehension function of the information which is encrypted to be communicated from the associated cryptographic comprehension function to the asymmetric delivery cryptographic comprehension function, comprising using the negotiated asymmetric delivery comprehension function of the at least three asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions in an integral process which does not have as an intermediate state a decrypted representation of

the information and does not itself require at any time during the transformation knowledge sufficient for decrypting the information which is encrypted.

508. On information and belief, one or more automated processors in the Microsoft Azure RMS system (e.g., the automated processor in a physical and/or virtual HSA associated with the Azure RMS key handler intermediary) transforms a comprehension function of the encrypted to be communicated Office 365 information from the associated cryptographic comprehension function (e.g., the cryptographic comprehension function comprising a function of a symmetric content key and an a private key component of an RSA key pair associated with the first Azure RMS user) to the asymmetric delivery cryptographic comprehension function (e.g., the function of at least three asymmetric key components of at least three different respective asymmetric delivery comprehension functions, to wit—(1) a public key component of an RSA key pair associated with the second Azure RMS user; (2) a private key component of an RSA key pair associated with the first Azure RMS user; and (3) a secret key component of an ephemeral/FPS asymmetric (e.g., DHE, ECDHE) session key pair dynamically generated between the Azure RMS key handler intermediary and the second Azure RMS user). The transforming comprises using the negotiated asymmetric delivery comprehension function of the at least three asymmetric key components of the at least three distinct respective asymmetric delivery comprehension functions in an integral process which does not have as an intermediate state a decrypted representation of the information and does not itself require at any time during the transformation knowledge sufficient for decrypting the information which is encrypted. (Indeed, it should be rather clear that no single party to the communication possesses sufficient asymmetric decryption key information to unilaterally remove all three asymmetric delivery key components of the asymmetric delivery comprehension function.).



The above figure is based on information contained in *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

509. On information and belief, the Azure and Office 365 RMS System communicates information which is encrypted with the asymmetric delivery cryptographic comprehension function to the second party through a communications port.

510. On Information and belief, the Microsoft Azure RMS key handler intermediary communicates the information which is encrypted with the asymmetric delivery cryptographic comprehension function to the second party (e.g., the second Microsoft Azure RMS user) via the communication port of (e.g., the wired and/or wireless network communication port for sending and receiving encrypted Office 365 information (or an identification thereof) between the Microsoft Azure RMS key handler and respective Microsoft Azure RMS users).

511. On information and belief, the protected information in the Azure and Office 365 System can include medical records. Microsoft's documentation specifically identifies medical records as a paradigmatic use case for Microsoft Azure RMS.

512. On information and belief, at least one of the three asymmetric key components in the Azure and Office 365 RMS System comprises a dynamically generated secret key.

513. On information and belief, the Azure and Office 365 System creates a cryptographic audit trail.

514. On information and belief, the Microsoft '247 Products are available to businesses and individuals throughout the United States.

515. On information and belief, the Microsoft '247 Products are provided to businesses and individuals located in the Eastern District of Texas.

516. On information and belief, Microsoft has directly infringed and continues to directly infringe the '247 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 Microsoft '247 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure RMS, Microsoft Azure Media Services, Microsoft Office 365, and Microsoft Azure RMS Enlightened Client programs and services. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Microsoft '247 Products, Microsoft has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '247 patent, including at least claims 10-11, 13, and 16, pursuant to 35 U.S.C. § 271(a).

517. On information and belief, Microsoft also indirectly infringes the '247 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint. Microsoft has had knowledge of the '247 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '247 patent and knew of its infringement, including by way of this lawsuit.

518. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '247 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing

acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '247 patent. Microsoft performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '247 patent and with the knowledge, that the induced acts would constitute infringement. For example, Microsoft provides the Microsoft '247 Products that have the capability of operating in a manner that infringe one or more of the claims of the '247 patent, including at least claims 10-11, 13, and 16, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '247 Products to utilize the products in a manner that directly infringe one or more claims of the '247 patent. By providing instruction and training to customers and end-users on how to use the Microsoft '247 Products in a manner that directly infringes one or more claims of the '247 patent, including at least claims 10-11, 13, and 16, Microsoft specifically intended to induce infringement of the '247 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '247 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '247 patent.¹⁰⁰ Accordingly, Microsoft 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 '247 patent, knowing that such use constitutes infringement of the '247 patent.

519. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '247 patent.

¹⁰⁰ *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015).

520. As a result of Microsoft's infringement of the '247 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

COUNT VI
INFRINGEMENT OF U.S. PATENT NO. 7,805,377

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

522. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft HealthVault ("Microsoft HealthVault" or "Microsoft '377 Products").

523. On information and belief, Microsoft operates the Microsoft HealthVault website located at: <https://www.healthvault.com>.

524. On information and belief, Microsoft HealthVault is available to businesses and individuals throughout the United States.

525. On information and belief, Microsoft HealthVault is available to businesses and individuals located in the Eastern District of Texas.

526. On information and belief, Microsoft has partnered with Texas based companies such as National Health Systems Inc., Vemics, Inc., PDX, Inc., and Rx.com Partners, LP (all of Texas) to promote and market Microsoft HealthVault.¹⁰¹

¹⁰¹ *PDX-Rx.com Works With Microsoft HealthVault to Make Prescription Data Available to Patients*, PR NEWSWIRE (June 9, 2009) ("PDX and Rx.com have entered into a strategic agreement with Microsoft to make prescription data, which Rx.com manages for multiple chain and independent pharmacy clients, available to Microsoft HealthVault users by accessing a single site with aggregated prescription data."); Marianne Kolbasuk McGee, *Microsoft, Athenahealth Collaborate On Amalga, HealthVault*, INFORMATIONWEEK GOVERNMENT (February 22, 2011) ("In addition to developing the new AthenaNet-Amalga connector, [Microsoft and Athenahealth] also announced at the Health Information Management and Systems Society (HIMSS) event in Orlando that they are working on projects with . . . Cook Children's Health Care Systems in Texas -- to push data from Amalga, including Athenahealth data, into Microsoft's HealthVault personal health record platform."); *iMedicor Announces Agreement with Microsoft HealthVault*, BUSINESS WIRE (February 28, 2008) ("Through this agreement, Vemics' iMedicor HIPAA compliant EHRT (Electronic Health Record Transport) portal will give HealthVault subscribers a user-friendly conduit for patient-physician communication as well as expedited access to their medical records and images.").

527. On information and belief, Microsoft HealthVault is a system adapted to control access to a patient medical record hosted by at least one medical record repository comprising a plurality of record portions, each record portion being associated with different patient-controlled access control criteria, the system comprising an automated processor, a database adapted to store information for authenticating requestors, a database adapted to store information for determining patient-controlled access control criteria for respective record portions of a patient medical record, and a computer network interface, said processor being controlled by instructions stored on a computer readable storage medium.

Authorization rules

An *authorization rule* is a collection of permissions for creating, reading, updating or deleting different data types. For example, a fitness application can define an authorization rule that specifies read-only access to demographic information but read/write access to exercise information. Most applications define one default authorization rule but multiple rules can be defined for management purposes.

Technical Overview: Permissions, MICROSOFT HEALTHVAULT DOCUMENTATION (2015), <https://msdn.microsoft.com/en-us/healthvault/healthvault-overview-permissions.aspx> (showing various types of authorization rules in Microsoft HealthVault).

528. On information and belief, Microsoft HealthVault receives a request for a medical record from a requestor, said request comprising a medical record identifier, a requestor identifier, requestor authentication information, and patient-provided access control authorization. For example, HealthVault receives a request for an electronic medical record from a requestor—e.g., a personal health device, a health app, a human (user agent) in a particular role, etc.

Reading and Writing Data

HealthVault provides an XML-based web service API with two methods for reading and writing data: GetThings and PutThings. The GetThings method is used to execute queries and return stored data. The PutThings method is used to create and update data.


Technical Overview: Exchanging Data, MICROSOFT HEALTHVAULT DOCUMENTATION (2015), <https://msdn.microsoft.com/en-us/healthvault/dn800946>.

529. On information and belief, Microsoft HealthVault processes a request for the medical record, to authenticate the requestor and determine sufficiency of the patient-provided

access control authorization to meet the patient-controlled access control criteria for each respective record portion encompassed by the request. For example, the HealthVault access control subsystem automatically processes the requestor's (e.g., personal health device; health app; human in a specific role) request for the electronic medical record by (among other things) evaluating the identification, authentication, and authorization information in the request. This includes, for example, cryptographically evaluating the patient-provided access control authorization (e.g., OAuth access token with user-controlled scope parameter) to determine its sufficiency to meet the patient-controlled access control criteria for each respective record portion encompassed by the request.

HealthVault provides:

- **Authentication:** Users can sign in with Windows Live ID, Facebook, and OpenID credentials.
- **Authorization:** HealthVault obtains user authorization before enabling any data access between an application and a user's HealthVault account data.
- **User control:** Users control how their data is shared by explicitly authorizing people and applications to access their data. Users can also terminate application access at any time, and can change or delete information in their records.
- **Auditing:** Data access auditing is built in and available to users.



HealthVault: A Platform For Connected Health Information And Innovation, MICROSOFT HEALTHVAULT DOCUMENTATION (2015), <https://msdn.microsoft.com/en-US/healthvault/dn798973> (the orange arrow identifies the authentication and authorization processes built into Microsoft HealthVault).

530. On information and belief, Microsoft HealthVault selectively communicates through a computer network interface to at least one medical record repository, an identification of each record portion for which access control criteria are determined to be sufficient for access by the requestor. For example, the Microsoft HealthVault access control subsystem selectively communicates through the computer network interface to at least one medical record repository, an identification of each record for which access control criteria (e.g., OAuth access token scope) are determined to be sufficient for access by the requestor.

531. On information and belief, Microsoft HealthVault generates an electronic payment authorization associated with a request for a medical record, for compensation of at

least one of the system and the at least one medical record repository. Microsoft HealthVault automatically generates an electronic audit message associated with the request. “Data access auditing is built in [to Microsoft HealthVault] and available to users.” *Id.*

532. On information and belief, Microsoft HealthVault receives, by an intermediary, a request for a medical record comprising a plurality of record portions, each record portion having an associated different patient-controlled access control criteria, from a requestor, said request comprising a medical record identifier, a requestor identifier, and requestor authentication information. For example, Microsoft HealthVault comprises an access control subsystem intermediary that receives and automatically processes HealthVault record access requests from a variety of different authenticated requestors (e.g., personal health devices, health apps, humans in various roles) under a variety of different circumstances.

HealthRecordAccessor Class

HealthVault

Represents the API set used to access a health record for an individual.

Namespace: Microsoft.Health
Assembly: Microsoft.Health (in Microsoft.Health.dll) Version: 2.1.0.0 (1.15.1003.9505)

▲ Syntax

C# C++ VB

```
public class HealthRecordAccessor
```

▲ Remarks

A HealthRecordAccessor represents a person's view of a health record. This view can vary based upon the access rights the person has to the record. More than one person might have access to the same record but have different views. For instance, a husband might have a HealthRecordAccessor instance for himself and another for his wife's health record to which she granted him access.

HealthRecordAccessor Class, MICROSOFT HEALTHVAULT .NET SDK REFERENCE (2015), available at: <https://msdn.microsoft.com/en-us/library/microsoft.health.healthrecordaccessor.aspx> (“A HealthRecordAccessor represents a person's view of a health record. This view can vary based upon the access rights the person has to the record.”).

533. On information and belief, Microsoft HealthVault receives, by the intermediary, a patient provided access control authorization associated with a request for a medical record from a requestor. For example, the HealthVault access control intermediary receives a patient-provided access control authorization (e.g., OAuth access token with user consent-based scope parameter) associated with a request for a HealthVault medical record from a requestor (e.g., personal health device; health app; human in an identified role).

534. On information and belief, Microsoft HealthVault access control automated processor cryptographically evaluates the Microsoft HealthVault access authorization information (e.g., OAuth access token with consent-limited scope parameter) to further determine sufficiency of the patient-provided access control authorization (e.g., the scope parameter of the OAuth access token, representing a Microsoft HealthVault custodian's consent to a particular scope (e.g., level, type, length, etc.) of access to his or her Microsoft HealthVault electronic medical record by the requestor) to meet the patient-controlled access control criteria for each respective record portion encompassed by the request.

535. On information and belief, Microsoft has directly infringed and continues to directly infringe the '377 patent by, among other things, making, using, offering for sale, and/or selling products and/or services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to, the Microsoft '377 Products. Such products and/or services include, by way of example and without limitation, Microsoft HealthVault.

536. By making, using, testing, offering for sale, and/or selling products and services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to the Microsoft '377 Products, Microsoft has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '377 patent, including at least claims 7 and 13, pursuant to 35 U.S.C. § 271(a).

537. On information and belief, Microsoft also indirectly infringes the '377 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint. Microsoft has had knowledge of the '377 patent since at least service of this Complaint or shortly thereafter. On information and belief, Microsoft knew of the '377 patent and knew of its infringement, including by way of this lawsuit.

538. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '377 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal

and customary use of the accused products would infringe the '377 patent. Microsoft performed the acts that constitute induced infringement, and would induce actual infringement, with the knowledge of the '377 patent and with the knowledge, that the induced acts would constitute infringement. For example, Microsoft provides the Microsoft '377 Products that have the capability of operating in a manner that infringe one or more of the claims of the '377 patent, including at least claims 7 and 13, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '377 Products to utilize the products in a manner that directly infringe one or more claims of the '377 patent. By providing instruction and training to customers and end-users on how to use the Microsoft '377 Products in a manner that directly infringes one or more claims of the '377 patent, including at least claims 7 and 13, Microsoft specifically intended to induce infringement of the '377 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '377 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '377 patent.¹⁰² Accordingly, Microsoft 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 '377 patent, knowing that such use constitutes infringement of the '377 patent.

539. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '377 patent.

540. As a result of Microsoft's infringement of the '377 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

¹⁰² See *e.g.*, *HealthVault: A Platform for Connected Health Information and Innovation*, MICROSOFT HEALTHVAULT DOCUMENTATION (2015); *Technical Overview: Permissions*, MICROSOFT HEALTHVAULT DOCUMENTATION (2015); *Technical Overview: Exchanging Data*, MICROSOFT HEALTHVAULT DOCUMENTATION (2015); *Microsoft HealthVault Help Guide*, MICROSOFT HEALTHVAULT WEBSITE (2015), available at: <https://account.healthvault.com/help/en-US/default.htm>.

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

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

542. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management (“Microsoft Azure RMS”), Microsoft Azure Media Services (“Microsoft Azure Media Services”); Microsoft Office 365 (“Microsoft Office 365”); and Microsoft Azure RMS Enlightened Client programs and services (“Microsoft Azure RMS Clients”)¹⁰³ (collectively, the “Azure and Office 365 RMS System” or the “Microsoft ‘368 Products”).

543. On information and belief, the Azure and Office 365 RMS System includes encryption technology.

544. On information and belief, the Microsoft ‘368 Products are available to businesses and individuals throughout the United States.

545. On information and belief, the Microsoft ‘368 Products are provided to businesses and individuals located in the Eastern District of Texas.

546. On information and belief, the Azure and Office 365 RMS System stores a plurality of digital records and respective access rules for each digital record in a computer memory associated with a server system. For example, the Microsoft Azure RMS System on a Microsoft server (e.g., an Office 365 app server or an Azure cloud server) stores a plurality of digital records (e.g., Word documents, Excel spreadsheets, PowerPoint presentations, and/or Outlook messages) and respective access rules for each digital record (e.g., respective Microsoft

¹⁰³ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as “enlightened” clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

Azure RMS access rules for each Word document, Excel spreadsheet, PowerPoint presentation, and/or Outlook message) in a computer memory associated with the server.

547. On information and belief, the Azure and Office 365 RMS System running on a Microsoft Server receives a request for access, from a remote computer, to access a digital record stored in the computer memory. For example, the Microsoft Azure RMS receives a request for access, from a remote computer (e.g., a remote computer or mobile device), to access a sensitive digital record (e.g., a rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message) stored in the server memory.

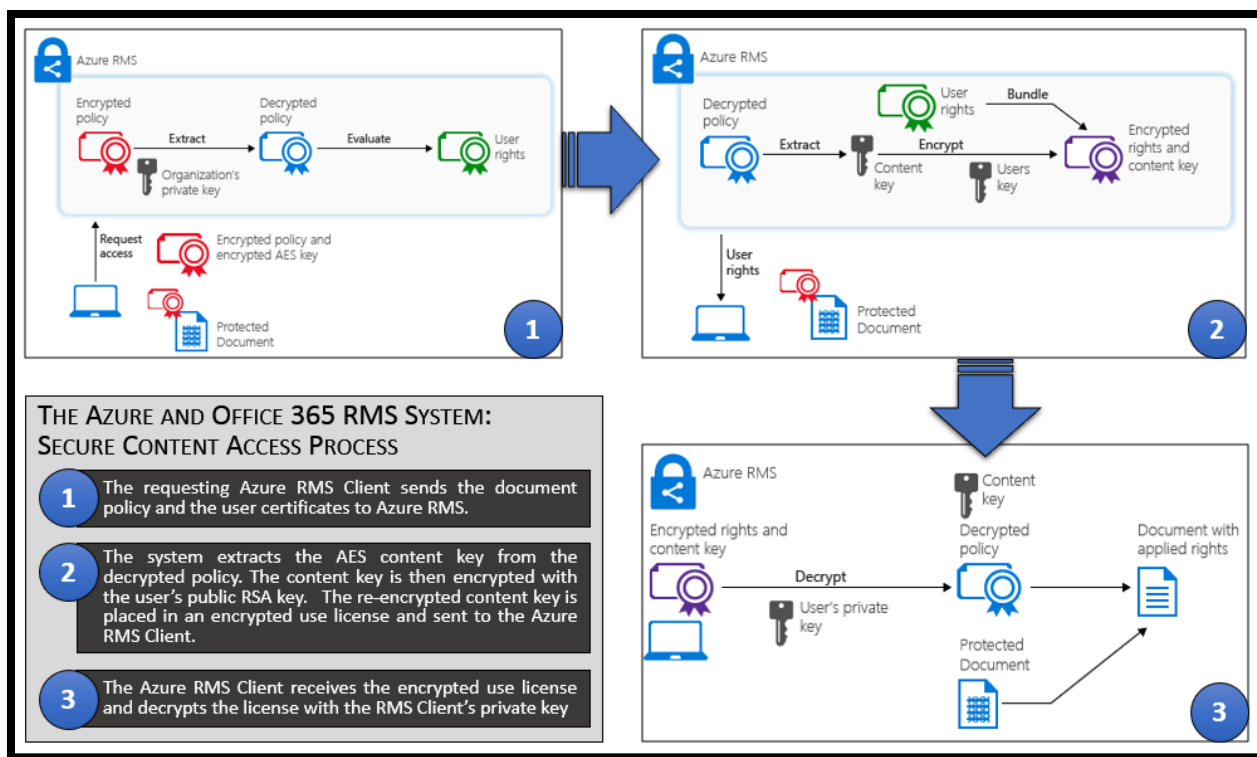
548. On information and belief, the Azure and Office 365 RMS System validates, by the server system, the received request to access the digital record by applying a respective set of access rules for the digital record stored in the computer memory. For example, the Microsoft Azure RMS validates, by the server system, the received request to access the digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message) by applying a respective set of access rules (e.g., Microsoft Azure RMS access rules) for the digital record stored in the server memory based on the authenticated identity, role, and context of the requesting user.

549. On information and belief, the Azure and Office 365 RMS System retrieves, by the server system, a public key having an associated private key, and associates a 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. For example, after validating the received request, Microsoft Azure RMS retrieves, by the server system, a public key having an associated private key (e.g., an RSA public key associated with the authenticated Microsoft Azure RMS user making the request, which has an associated RSA private key).

550. On information and belief, the Azure and Office 365 RMS System after validating the received request, associates a wrapper—a small amount of platform-specific (.NET, iOS, Android, Cordova, etc.) Microsoft Azure RMS code—with the digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message).

The wrapper is designed to invoke local Microsoft Rights Management (MRM) programming on the device to identify and enforce Microsoft Azure RMS rules embedded in the license for the digital record—for example, access log/audit rules requiring notification to a remote server upon certain events.

551. On information and belief, the wrapper used by the Azure and Office 365 RMS System has a respective session key (e.g., an AES content key uniquely generated for the digital record). The session key is required to access the encrypted digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), and the wrapper literally “wraps” it, so that an attempt to decrypt the digital record on a client device will necessarily invoke local MRM programming. The session key is distinct from the public key and the private key.



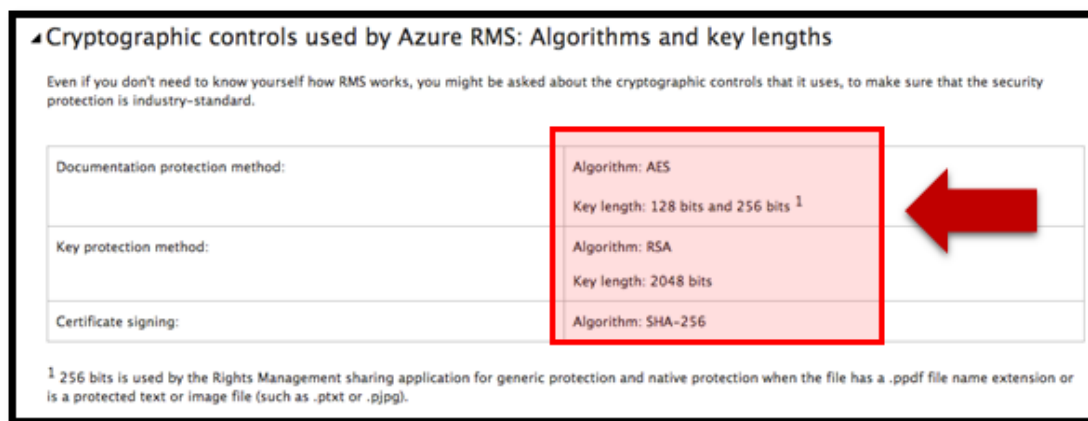
The above figure is based on information contained in *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

552. On information and belief, the logging wrapper generated by the Azure and Office 365 RMS system has a respective session key (e.g., an AES content key uniquely

generated for the digital record). The session key is required to access the encrypted digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), and the logging wrapper literally “wraps” it, so that an attempt to decrypt the digital record on a client device will necessarily invoke local MRM programming. The session key is distinct from the public key and the private key.

553. On information and belief, the Azure and Office 365 RMS System encrypts and sends, by the server system, the requested digital record after validating the received request, using the public key and the session key to encrypt the digital record. For example, Microsoft Azure RMS encrypts and sends, by the server system, the requested digital record after validating the received request (e.g., by determining authorization of the authenticated Microsoft Azure RMS user making the request to access the rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), using the public key (e.g., the RSA public key associated with the authenticated Microsoft Azure RMS user who made the request) and the session key (e.g., the AES content key uniquely generated for the record) to encrypt the digital record).

554. The below excerpt from Microsoft Azure RMS documentation shows the encryption algorithms used by Microsoft Azure RMS to protect secure data.



What is Azure Rights Management?, Microsoft TechNet Article (July 1, 2015) (red arrow indicating the algorithms and key lengths employed by Microsoft Azure RMS).

555. On information and belief, the Azure and Office 365 RMS System receives the encrypted digital record, by the remote computer, and decrypts the encrypted digital record using the private key, and the session key in conjunction with the logging wrapper. For example, tamper-resistant, privileged system-level Microsoft Rights Management code on the remote computer (e.g., the authenticated Microsoft Azure RMS user's computer or mobile device) receives the encrypted digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), and decrypts the encrypted digital record using the private key (e.g., the RSA private key associated with the authenticated Microsoft Azure RMS user requesting the record), and the session key (e.g., the AES content key uniquely generated for the requested record) in conjunction with the logging wrapper.

556. On information and belief, the Azure and Office 365 RMS System generates by the wrapper, at the remote computer, a logging event. For example, tamper-resistant, privileged system-level MRM code on the remote computer (e.g., the requesting Azure RMS user's remote computer or mobile device) generates by the wrapper, at the remote computer, a logging event.

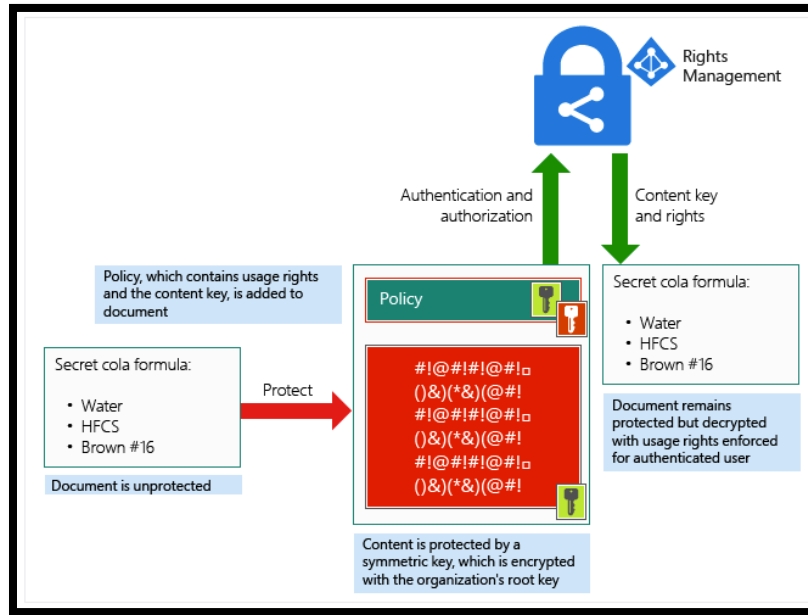
557. On information and belief, the Azure and Office 365 RMS System accounts, at the server, for the decrypting by the remote computer using the wrapper. For example, the Microsoft Azure RMS accounts for the decrypting of the encrypted record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), by the remote computer using the wrapper (e.g., by recording the event in an audit/access log).

558. On information and belief, the Azure and Office 365 RMS System encrypts and sends, 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. For example, Azure RMS encrypts and sends, by the server system, the requested digital record which has been validated (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), using the public key (e.g., the RSA public key associated with the authenticated Microsoft Azure RMS user who made the request) and the session key (e.g., the AES content key uniquely generated for the record) to encrypt the digital record.

559. On information and belief, the Azure and Office 365 RMS System receives a request for access, from a remote computer, to access a digital record stored in the computer memory. For example, the Microsoft Azure RMS receives a request for access, from a remote computer (e.g., a remote computer or mobile device), to access a sensitive digital record (e.g., a rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message) stored in the server memory.

560. On information and belief, the Azure and Office 365 RMS System validates, 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. For example, the Microsoft Azure RMS subsystem on the Microsoft server (e.g., Office 365 app server or Azure cloud server) validates, by the server system, the received request to access the digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message) by applying a respective set of access rules (e.g., Microsoft Azure RMS access rules) for the digital record stored in the server memory based on the authenticated identity, role, and context of the requesting user.

561. The below diagram from Microsoft technical documentation shows the encryption system used by the Azure and Office 365 RMS System.



What is Azure Rights Management?, MICROSOFT TECHNET ARTICLE (July 1, 2015).

562. On information and belief, the Azure and Office 365 System retrieves, by the server system, a public key having an associated private key, and associates 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. For example, after validating the received request, Microsoft Azure RMS retrieves, by the server system, a public key having an associated private key (e.g., an RSA public key associated with the authenticated Azure RMS user making the request, which has an associated RSA private key). After validating the received request, the Azure RMS subsystem of the Microsoft server (e.g., Office 365 app server or Azure cloud server) associates a logging wrapper—a small amount of platform-specific (.NET, iOS, Android, Cordova, etc.) Azure RMS code—with the digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message). The logging wrapper is designed to invoke local Microsoft Rights Management (MRM) programming on the device to identify and enforce Azure RMS rules embedded in the license for the digital record—for example, access log/audit rules requiring notification to a remote server upon certain events.

563. On information and belief, the wrapper used by the Azure and Office 365 RMS System has a respective session key (e.g., an AES content key uniquely generated for the digital record). The session key is required to access the encrypted digital record (e.g., rights-managed Word document, Excel spreadsheet, PowerPoint presentation, or Outlook message), and the logging wrapper literally “wraps” it, so that an attempt to decrypt the digital record on a client device will necessarily invoke local MRM programming. The session key is distinct from the public key and the private key.

564. On information and belief, the Azure and Office 365 RMS System generates by the logging wrapper, at the remote computer, a logging event. For example, tamper-resistant, privileged system-level MRM code on the remote computer (e.g., the requesting Microsoft Azure RMS user’s remote computer or mobile device) generates by the logging wrapper, at the remote computer, a logging event.

565. On information and belief, the Azure and Office 365 RMS System records the logging event in an access log. For example, the Microsoft Azure RMS subsystem on the Microsoft server (e.g., Office 365 web app server or Azure cloud server) records the logging event in an access log.

566. On information and belief, Microsoft Azure RMS documentation on data loss prevention (DLP) discusses an administrative DLP “policy to help keep the organization in compliance with US regulations for protecting personally identifiable information data, but rules can also be configured for other compliance regulations, or custom rules that you define.”

567. On information and belief, Microsoft 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 securely controlling access to a plurality of digital records by a remote computer, including but not limited to, the Microsoft ‘368 Products, which include infringing information records infrastructure technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure RMS, Microsoft Azure

Media Services, Microsoft Office 365, and Microsoft Azure RMS Enlightened Client programs and services.

568. By making, using, testing, offering for sale, and/or selling products and services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to the Microsoft '368 Products, Microsoft 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 1-2, 7-8, 15-16, 18, 20-23, 26, 29-31, 35, 133 and 140, pursuant to 35 U.S.C. § 271(a).

569. On information and belief, Microsoft also indirectly infringes the '368 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of 2010. Microsoft had knowledge of the '368 patent since at least 2010. Microsoft cited the '368 patent in the following issued United States patents and published patent applications:

- U.S. Patent No. 7,792,758 issued on September 7, 2010 entitled "Substitution Groups/Inheritance for Extensibility in Authorization Policy," and assigned to Microsoft Corporation.
- U.S. Patent No. 8,473,612 issued on June 25, 2013 entitled "Trusted Network Transfer of Content Using Off Network Input Code," and assigned to Microsoft Corporation.
- U.S. Patent No. 8,874,930 issued on October 28, 2014 entitled "Graph Encryption," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2004/0098277 published on May 20, 2004 entitled "Licenses That Include Fields Identifying Properties," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2004/0098347 published on May 20, 2004 entitled "Substitution Groups/Inheritance for Extensibility in Authorization Policy," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2010/0125896 published on May 20, 2010 entitled "Trusted Network Transfer of Content Using of Network Input Code," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2011/0138190 published on June 9, 2011 entitled "Graph Encryption," and assigned to Microsoft Corporation.
- U.S. Patent Application No. 2013/0326006 published on December 5, 2013 entitled "Managing Large Data Sets Through Page Based Information Tracking in Multi-Master Environments," and assigned to Microsoft Corporation.

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

571. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '368 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '368 patent. Microsoft 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, Microsoft provides the Microsoft '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 1-2, 7-8, 15-16, 18, 20-23, 26, 29-31, 35, 133 and 140, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '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 Microsoft '368 Products in a manner that directly infringes one or more claims of the '368 patent, including at least claims 1-2, 7-8, 15-16, 18, 20-23, 26, 29-31, 35, 133 and 140, Microsoft specifically intended to induce infringement of the '368 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '368 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '368 patent.¹⁰⁴ Accordingly, Microsoft has induced and continues to induce users of the accused

¹⁰⁴ *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); Jeff Fried, *Information Management Strategy with*

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.

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

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

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

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

575. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Media Services ("Microsoft Azure Media Services"); Microsoft Office 365 ("Microsoft Office 365"); and Microsoft Azure RMS Enlightened Client programs and services ("Microsoft Azure RMS Clients")¹⁰⁵ (collectively, the "Azure and Office 365 RMS System").

576. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Active Directory ("Azure Active Directory").

Microsoft Office 365 in Mind, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPP] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015).

¹⁰⁵ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as "enlightened" clients. Enlightened clients include Windows 8.1, Windows 10, and Windows Phone 8.1. A complete listing of Microsoft Azure RMS "enlightened" client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS "enlightened" applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

577. Microsoft makes, sells, offers to sell, imports, and/or uses products and services that incorporate Azure Active Directory functionality. These products and services include: Microsoft Intune,¹⁰⁶ Microsoft Office 365,¹⁰⁷ Microsoft Dynamics CRM Online,¹⁰⁸ Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple),¹⁰⁹ Microsoft Azure RMS,¹¹⁰ Office 365 SharePoint Online,¹¹¹ and Microsoft OneDrive.¹¹² (collectively, the “Azure Active Directory Applications”).

578. Azure Active Directory and Azure Active Directory Applications (collectively, the “Azure Active Directory System”) is a system for controlling access to a plurality of records stored within a plurality of automated external databases.

579. The Azure Active Directory System and Azure and Office 365 RMS System (collectively, the Microsoft “941 Products”) control access to records in a plurality of databases where each record has an associated set of access rules.

580. On information and belief, the Azure Active Directory System enables receiving a request from a requestor, the requestor having at least one attribute. For example, on information and belief, the Azure Active Directory System receives a request from a requestor (e.g., Azure

¹⁰⁶ *Microsoft Intune*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/microsoftintunemdm/> (“By default, Microsoft Intune works with Azure AD.”).

¹⁰⁷ *Microsoft Office 365*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/office365/> (“By default, Office 365 works with Azure AD.”).

¹⁰⁸ *Microsoft Dynamics CRM*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/crm/> (“By default, Dynamics CRM works with Azure AD.”).

¹⁰⁹ *Protecting Microsoft Azure Blob Storage with Microsoft Azure AD Rights Management in Cloud Services and Web Applications*, MSDN WHITE PAPER (2015).

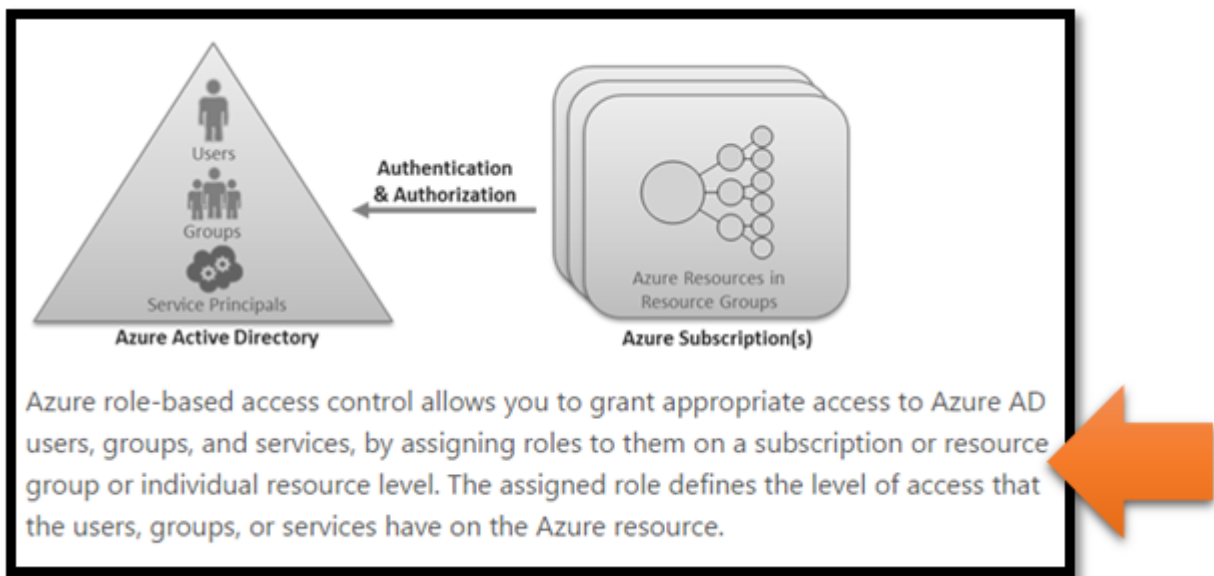
¹¹⁰ *Protecting Data in Microsoft Azure at 32*, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014).

¹¹¹ *Office 365 SharePoint Online*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/sharepoint/> (“By default, Office 365 SharePoint Online works with Azure AD.”).

¹¹² *Microsoft OneDrive*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/skydrive/> (“Use Azure AD to enable user access to Microsoft OneDrive.”).

Active Directory-enrolled end user; Azure Active Directory-enlightened native or web application; Azure Active Directory-enlightened web service), the requestor having at least one attribute (e.g. an identified role; a group, request-specific requestor attributes such as geographic origin, client platform, proffered authentication credentials; etc.).

581. On information and belief, the at least one requestor attribute can be used to implement Azure Active Directory System user-based access policies, Azure Active Directory group-based access policies, and/or service principals based access policies.¹¹³



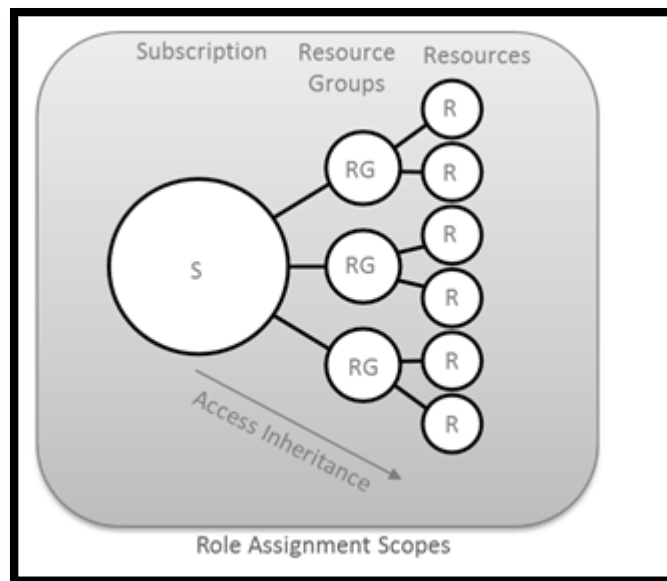
Ingrid Henkel, *Role-based Access Control in the Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015) (the yellow arrow points to the description of Azure Active Directory as enabling role based authentication and authorization).

582. On information and belief, the Azure Active Directory System enables searching the 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. For example, on information and belief, the Azure Active Directory system searches the plurality of

¹¹³ Ingrid Henkel, *Role-based Access Control In The Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015) (“Azure role-based access control allows you to grant appropriate access to Azure AD users, groups, and services, by assigning roles to them on a subscription or resource group or individual resource level.”).

automated electronic databases (e.g., documents and application data stored in and/or hosted by a plurality of structured or unstructured Azure cloud data stores, each external to the centralized Azure Active Directory authentication and access control index) 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.

583. On information and belief, the Azure Active Directory System enables applying a set of access rules (e.g., Active Directory account-specific, user and/or role-specific, and/or resource-specific access policy rules applicable based upon at least the authenticated requestor identity and context; the requested resource; and Azure Active Directory policy decision logic) for each found record by at least one automated processor, to produce a set of accessible records, at a server device. For example, on information and belief, the Azure Active Directory System by at least one automated processor, a set of access rules for each found record in an Azure Active Directory, to produce a set of accessible records at a server device.



Ingrid Henkel, *Role-based Access Control In The Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015) (Text accompanying the above figure states “Access does not need to be granted to the entire subscription. Roles can also be assigned for resource groups as well as for individual resources.”).

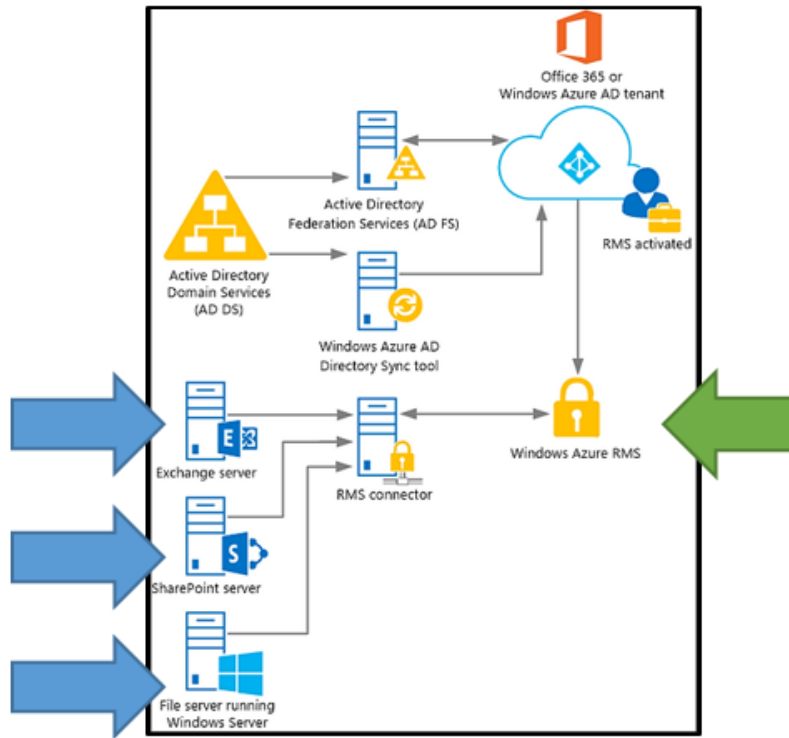
584. On information and belief, the Azure Active Directory System enables applying at least one compensation rule by at least one automated processor, dependent on the at least one attribute of the requestor. For example, on information and belief, Azure Active Directory applies at least one compensation rule by at least one automated processor, dependent on the at least one attribute of the requestor (e.g., by using an attribute of the requestor to determine who and how much to charge for the query).

585. On information and belief, the Azure Active Directory System enables logging at least the request for access by at least one automated processor. For example, on information and belief, Azure Active Directory Reports logs at least the request for access by at least one automated processor.¹¹⁴

586. On information and belief, the Azure Active Directory System enables communicating the set of accessible records. For example, the Azure Active Directory System communicates the linked set of releasable accessible records to the requestor (e.g., Azure Active Directory- enrolled end user; Azure Active Directory – enlightened native or web application; Azure Active Directory - enlightened web service).

587. On information and belief, the Azure and Office 365 RMS System enables controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules. For example, as illustrated in the figure below the Azure and Office 365 RMS System enables access control to a plurality of records stored in automated databases.

¹¹⁴ *Microsoft Azure Security and Audit Log Management* at 29, MICROSOFT AZURE WHITE PAPER (November 2014) (“Azure Active Directory . . . includes a set of security, usage, and audit log reports that provide visibility into the integrity and security of your Azure AD tenant. For example, Azure AD has the capability to automatically analyze user activity and surface anomalous access, and then make it available through customer-visible reports.”).



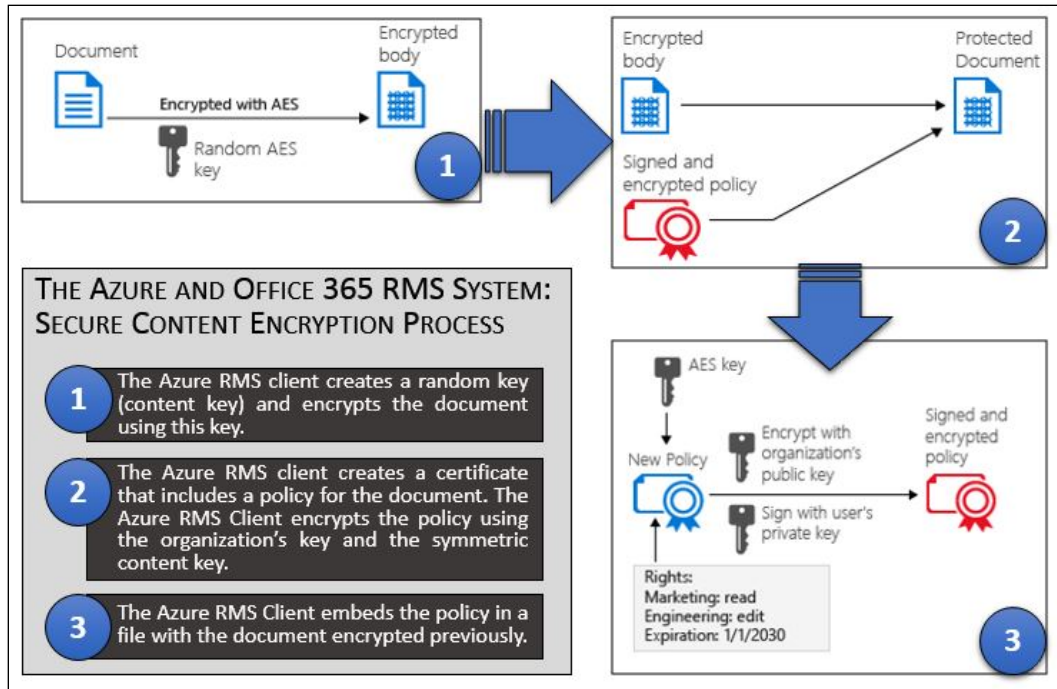
Deploying the Azure Rights Management Connector, MICROSOFT TECHNET ARTICLE (September 1, 2015) (The blue arrows indicate the plurality of extern automated databases holding content such as documents and emails. The green arrow points to Microsoft Azure RMS.).

588. On information and belief, the Azure and Office 365 RMS System receives a request from a requestor, the requestor having at least one attribute. For example, on information and belief, Microsoft Azure RMS receives a request from a requestor (e.g., a Microsoft Azure RMS user and/or requestor of the Office 365 information (e.g., Word document or Outlook message)), the requestor having at least one attribute (e.g. key information, an identified role; group, organization, etc.).¹¹⁵

589. On information and belief, the Azure and Office 365 RMS performs controlling access to a plurality of records provided within a plurality of automated electronic databases,

¹¹⁵ Dan Plastina, *Create Custom Templates in Azure RMS with the Azure Management Portal*, THE OFFICIAL RMS TEAM BLOG (April 3, 2014) (“With custom templates you can designate different groups of users that will have access to documents protected with these templates, and you can define an access level or a list of rights for each of these groups.”).

each record having an associated set of access rules. Records stored in automated electronic databases have a “signed and encrypted policy” shown in the figure below.



The above figure is based on information contained in *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

590. On information and belief, the Azure and Office 365 RMS System searches 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.

591. On information and belief, the Azure and Office 365 RMS System applies a set of access rules associated with each found record by at least one automated processor, to produce a set of accessible records, at a server device. “[T]he [Azure] RMS client takes the encrypted use license and decrypts it with its own user private key. This lets the RMS client decrypt the document’s body as it is needed and render it on the screen.”¹¹⁶

¹¹⁶ *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015).

592. On information and belief, the Azure and Office 365 RMS System performs logging at least the request for access by at least one automated processor.¹¹⁷

593. On information and belief, the Microsoft '941 Products are available to businesses and individuals throughout the United States.

594. On information and belief, the Microsoft '941 Products are provided to businesses and individuals located in the Eastern District of Texas.

595. On information and belief, Microsoft 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 securely controlling access to a plurality of digital records by a remote computer, including but not limited to, the Microsoft '941 Products, which include infringing information records infrastructure technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure RMS, Microsoft Azure Media Services, Microsoft Office 365, Microsoft Azure RMS Enlightened Client programs and services, Microsoft Azure Active Directory, and Microsoft products and services that incorporate Microsoft Azure Active Directory functionality.¹¹⁸

596. By making, using, testing, offering for sale, and/or selling products and services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to the Microsoft '941 Products, Microsoft has injured St. Luke and is liable to St.

¹¹⁷ *Logging and Analyzing Azure Rights Management Usage*, MICROSOFT TECHNET ARTICLE (July 1, 2015) (“If you have an information leak, you are likely to be asked who recently accessed specific documents and what information did a suspected person access recently. You can answer these type of questions when you use RMS and logging because people who use protected content must always get an RMS license to open documents and pictures that are protected by RMS, even if these files are moved by email or copied to USB drives or other storage devices. This means that you can use RMS logs as a definitive source of information for forensic analysis when you protect your data by using RMS.”).

¹¹⁸ Products incorporating Microsoft Azure Active Directory functionality include: Microsoft Office 365 products and services; Microsoft OneDrive for Business; Microsoft SharePoint Online; Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple), and Microsoft Azure RMS.

Luke for directly infringing one or more claims of the '941 patent, including at least claims 1, 8, and 16, pursuant to 35 U.S.C. § 271(a).

597. On information and belief, Microsoft also indirectly infringes the '941 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint or shortly thereafter. Microsoft knew of the '941 patent and knew of its infringement, including by way of this lawsuit.

598. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '941 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '941 patent. Microsoft 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, Microsoft provides the Microsoft '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 1, 8, and 16, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '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 Microsoft '941 Products in a manner that directly infringes one or more claims of the '941 patent, including at least claims 1, 8, and 16, Microsoft specifically intended to induce infringement of the '941 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '941 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '941 patent.¹¹⁹ Accordingly, Microsoft has induced and continues to induce users of the

¹¹⁹ *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management at 1*, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Julia

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.

599. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '941 patent.

600. As a result of Microsoft's infringement of the '941 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

COUNT IX
INFRINGEMENT OF U.S. PATENT NO. 8,380,630

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

602. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Rights Management ("Microsoft Azure RMS"), Microsoft Azure Media Services ("Microsoft Azure Media Services"); Microsoft Office 365 ("Microsoft Office 365"); and Microsoft Azure RMS Enlightened Client programs and services ("Microsoft Azure RMS Clients")¹²⁰ (collectively, the "Azure and Office 365 RMS System").

Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015); *See e.g., Protecting Data in Microsoft Azure*, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014); Ingrid Henkel, *Role-based Access Control in the Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015); *Hybrid Identity*, MICROSOFT WHITE PAPER (2015); *Access Control Service 2.0*, MICROSOFT MSDN TECHNICAL LIBRARY (April 14, 2015); *Administering Your Azure AD Directory*, MICROSOFT MSDN TECHNICAL LIBRARY (September 15, 2015); Simon May and Joe Breslin, *Azure AD and Identity Show: Azure AD B2C (Business to Consumer)*, MSDN AZURE AD AND IDENTIFY SHOW (September 16, 2015); Malcolm Jeffrey, *Protecting your data with AD-RMS and Azure RMS*, MICROSOFT IGNITE NEW ZEALAND PRESENTATION (available on MSDN Channel 9) (September 2, 2015).

¹²⁰ Microsoft documentation refers to client devices and applications that support Microsoft Azure RMS as "enlightened" clients. Enlightened clients include Windows 8.1, Windows 10,

603. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Active Directory (“Azure Active Directory”).¹²¹

604. Microsoft makes, sells, offers to sell, imports, and/or uses products and services that incorporate Azure Active Directory functionality. These products and services include: Microsoft Intune,¹²² Microsoft Office 365,¹²³ Microsoft Dynamics CRM Online,¹²⁴ Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple),¹²⁵ Microsoft Azure RMS,¹²⁶ Office 365 SharePoint Online,¹²⁷ and Microsoft OneDrive¹²⁸ (collectively, the “Azure Active Directory Applications”).

and Windows Phone 8.1. A complete listing of Microsoft Azure RMS “enlightened” client devices is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedDevices. Computer applications that natively support Azure RMS include Office 365 ProPlus, Office 365 Enterprise E3, Office Professional 2016, Office Professional 2013, and Office Professional 2010. A complete listing of Microsoft Azure RMS “enlightened” applications is available at: https://technet.microsoft.com/en-us/library/dn655136.aspx#BKMK_SupportedApplications.

¹²¹ Including Azure AD B2C and Azure AD B2B.

¹²² *Microsoft Intune*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/microsoftintunemdm/> (“By default, Microsoft Intune works with Azure AD.”).

¹²³ *Microsoft Office 365*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/office365/> (“By default, Office 365 works with Azure AD.”).

¹²⁴ *Microsoft Dynamics CRM*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/crm/> (“By default, Dynamics CRM works with Azure AD.”).

¹²⁵ *Protecting Microsoft Azure Blob Storage with Microsoft Azure AD Rights Management in Cloud Services and Web Applications*, MSDN WHITE PAPER (2015).

¹²⁶ *Protecting Data in Microsoft Azure* at 32, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014).

¹²⁷ *Office 365 SharePoint Online*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/sharepoint/> (“By default, Office 365 SharePoint Online works with Azure AD.”).

¹²⁸ *Microsoft OneDrive*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/skydrive/> (“Use Azure AD to enable user access to Microsoft OneDrive.”).

605. Azure Active Directory and Azure Active Directory Applications (collectively, the “Azure Active Directory System”) enable controlling access to a plurality of records stored within a plurality of automated external databases.

606. On information and belief, Azure and Office 365 RMS System and the Azure Active Directory System (collectively, the “Microsoft ‘630 Products”) enable receiving an information request from a plurality of external databases.

607. On information and belief, the Azure Active Directory System comprises a security mediator that enables developers to deliver access control to applications and data.

Microsoft Azure Active Directory	Provides a comprehensive and high available IAM cloud solution that combines core directory services, advanced identity governance, and application access management. Also offers a rich standards-based platform that enables developers to deliver access control to their applications, based on centralized policy and rules.	Microsoft Azure Active Directory
----------------------------------	--	----------------------------------

Enabling Enterprise Mobility through People-Centric IT, MICROSOFT WHITE PAPER 32 (October 2014).

608. On information and belief, the Azure Active Directory System enables authenticating a user. For example, Microsoft Azure Active Directory “is a cloud- based service that provides an easy way of authenticating and authorizing users to gain access to your web applications and services while allowing the features of authentication and authorization to be factored out of your code.”¹²⁹

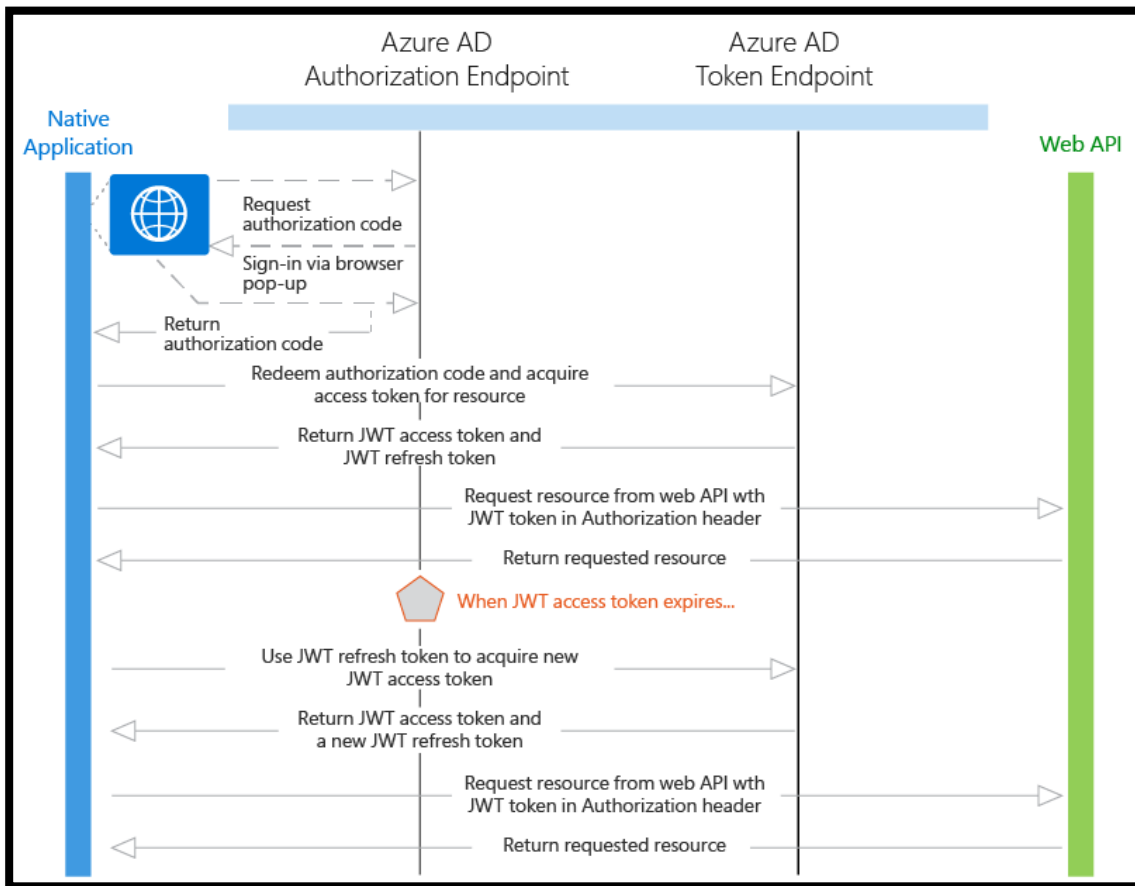
609. On information and belief, the Azure Active Directory System applies access rules associated with located request information. For example, the Microsoft Azure Active Directory describes its functionality as “IT can specify which applications users can see in the company portal based on a variety of criteria, such as a defined user role (for example, finance managers or group managers) or groups within Active Directory.”

610. On information and belief, the Azure Active Directory System includes functionality for automatically communicating through an automated security mediator to a

¹²⁹ Access Control Service 2.0, MSDN Microsoft Azure Library (April 15, 2015).

plurality of external databases. For example, the Azure Active Directory System obtains an access token for the user by using the OAuth 2.0 protocol. The access token is then sent in the request to the Web API (external data source), which authorizes the user and returns the desired resource.

611. On information and belief, the Azure Active Directory System receives a request for authorization to access an external data source. The request received by the Azure Active Directory System includes the Client ID and redirect URL of the application (the Azure Active Directory Application). Azure Active Directory authenticates the user and issues an authorization code response back to the client application's redirect URL. The Azure Active Directory System then issues an authorization code response back to the redirect URI, the client application extracts the authorization code from the response. Using this authorization code, the Azure Active Directory Application sends a request to Azure Active Directory's token endpoint that includes the authorization code. Next, the Azure Active Directory System validates the authorization code and information about the Azure Active Directory Application and web API. Upon successful validation, the Azure Active Directory System returns two tokens: a JWT access token and a JWT refresh token. In the final step, the client application uses the returned JWT access token to add the JWT string with a "Bearer" designation in the Authorization header of the request to the web API. The web API then validates the JWT token, and if validation is successful, returns the external data source. The below diagram shows how the Azure Active Directory System enables access to external data using Azure Active Directory.



M Baldwin, *Authentication Scenarios for Azure AD*, AZURE ACTIVE DIRECTORY DOCUMENTATION (September 17, 2015).

612. On information and belief, the Azure Active Directory System includes functionality for automatically communicating through an automated security mediator to a plurality of external databases.

613. On information and belief, the Azure Active Directory System enables robust logging and audit reporting. The below Microsoft white paper describes Azure Active Directory as enabling user specific reports and activity logs.

4.3.8 Audit access to your Azure RMS tenant

You can use access and usage reports in Azure AD to gain visibility into the integrity and security of your organization's Azure RMS tenant. With this information, a tenant administrator can better determine where possible security risks may lie so that the organization can adequately plan to mitigate those risks.

When you use the Azure Management Portal, reports are categorized in the following ways:

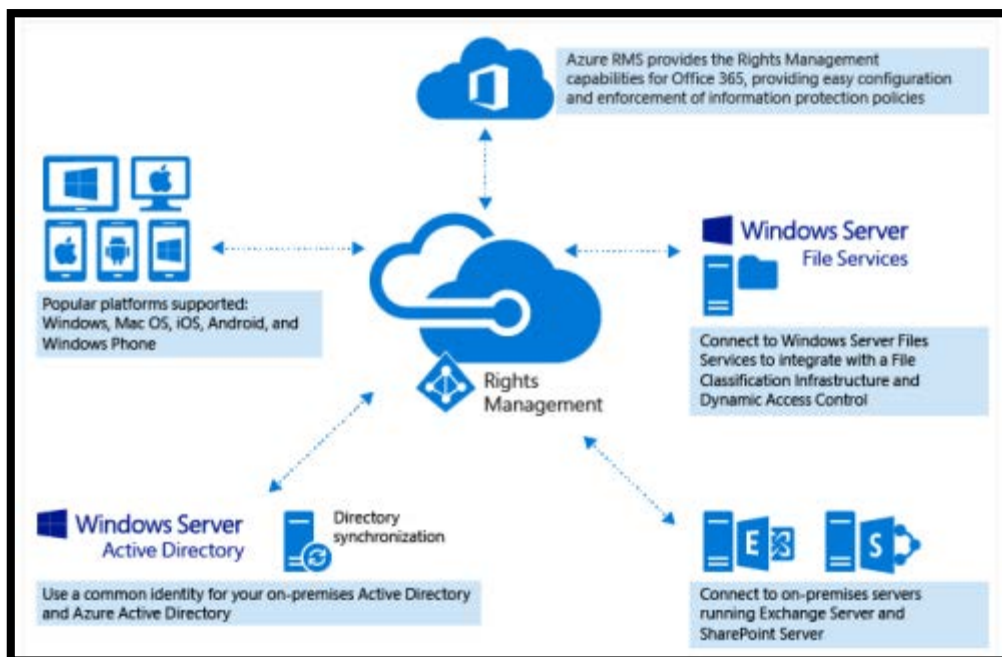
- Anomaly reports - Contain sign in events that Azure RMS/Microsoft found to be anomalous. Our goal is to make you aware of such activity and enable you to be able to make a determination about whether an event is suspicious.
- Integrated Application report - Provides insights into how cloud applications are being used in your organization. AD offers integration with thousands of cloud applications.
- Error reports - Indicate errors that may occur when provisioning accounts to external applications.
- User-specific reports - Display device/sign in activity data for a specific user.
- Activity logs - Contain a record of all audited events within the last 24 hours, last 7 days, or last 30 days, as well as group activity changes, and password reset and registration activity.

Azure RMS Security Evaluation Guide, MICROSOFT RIGHTS MANAGEMENT WHITE PAPER 19 (May 2015).

614. On information and belief, the Azure and Office 365 RMS Solution enables authenticating a user. For example, Microsoft Azure RMS relies on an identity system to authenticate users. And, Microsoft Azure RMS is enabled to request a user's security token via an organizations identity system."¹³⁰

615. On information and belief, the Azure and Office 365 RMS System enables receiving an information request for information stored on a plurality of external databases (e.g., data stored in the cloud). The below diagram shows that Microsoft Azure RMS can access and manage information requests for data stored in both on premise servers (e.g., SharePoint) and in external databases (e.g., the cloud).

¹³⁰ *Azure RMS Security Evaluation Guide*, MICROSOFT RIGHTS MANAGEMENT WHITE PAPER 11 (May 2015).



Azure RMS Security Evaluation Guide, MICROSOFT RIGHTS MANAGEMENT WHITE PAPER 5 (May 2015).

616. On information and belief, the Azure and Office 365 RMS System contains an input port configured to receive a request for information stored in a plurality of external databases from a Microsoft Azure RMS user (e.g., Microsoft Azure RMS Client).

4.3.4 Group membership is defined by the customer organization

Azure RMS allows protecting content for internal users, located in the organization's Active Directory, as well as for external users, located in the Active Directory of a different organization, by using an implicit Azure Active Directory trust. For example, Contoso users may protect some content for an external auditor Jane Doe by referencing her by email address jane.doe@fabrikam.com.

Azure RMS Security Evaluation Guide, MICROSOFT RIGHTS MANAGEMENT WHITE PAPER 13 (May 2015).

617. On information and belief, the Azure and Office 365 RMS System contains an automated centralized index, stored in a memory, configured to store location information and associated access rules for information stored in external databases.

A document containing the secret formula is protected, and then successfully opened by an authorized user or service. The document is protected by a content key. . . . It is unique for each document and is placed in the file header where it is protected by your RMS tenant root key.

What is Azure Rights Management?, MICROSOFT TECHNET ARTICLE (July 1, 2015).

618. On information and belief, the Azure and Office 365 RMS System contains one or more processors, configured to: locate requested information; generate a query corresponding to the request; apply the access rules stored in the automated central index (“ACI”) to restrict access to the located requested information (“LRI”). As explained in a Microsoft TechNet article, access rules such as restricting access to company “executives” are enabled in the Azure and Office 365 RMS system.

For example, for a company- wide strategy paper to be shared with all employees, you could apply a read- only policy to all internal employees. Then, for a more sensitive document, such as a financial report, you could restrict access to executives only.

What is Azure Rights Management?, MICROSOFT TECHNET ARTICLE (July 1, 2015).

619. On information and belief, the Azure and Office 365 RMS System generates instructions to each of the external databases storing the LRI to apply native access rules (“NARs”) of the respective external databases to further restrict access to the LRI and consolidate the requested information retrieved from the external databases storing the LRI.¹³¹

620. On information and belief, the Azure and Office 365 RMS System contains robust logging and audit trail functionality. “IT can track and monitor usage for data that has been protected—for example, who is accessing the data and when.”¹³²

621. On information and belief, the Microsoft ‘630 Products are available to businesses and individuals throughout the United States.

¹³¹ *What is Azure Rights Management?*, MICROSOFT TECHNET ARTICLE (July 1, 2015) (“A document containing the secret formula is protected, and then successfully opened by an authorized user or service. The document is protected by a content key. . . . It is unique for each document and is placed in the file header where it is protected by your RMS tenant root key.”)

¹³² *Enabling Enterprise Mobility through People-Centric IT*, MICROSOFT WHITE PAPER 13 (October 2014).

622. On information and belief, the Microsoft '630 Products are provided to businesses and individuals located in the Eastern District of Texas.

623. On information and belief, Microsoft 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 securely controlling access to a plurality of digital records by a remote computer, including but not limited to, the Microsoft '630 Products, which include infringing information records infrastructure technologies. Such products and/or services include, by way of example and without limitation, Microsoft Azure RMS, Microsoft Azure Media Services, Microsoft Office 365, Microsoft Azure RMS Enlightened Client programs and services, and Microsoft products and services that incorporate Microsoft Azure Active Directory functionality.¹³³

624. By making, using, testing, offering for sale, and/or selling products and services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to the Microsoft '630 Products, Microsoft has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '630 patent, including at least claim 16 pursuant to 35 U.S.C. § 271(a).

625. On information and belief, Microsoft also indirectly infringes the '630 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint.

626. On information and belief, Microsoft has had knowledge of the '630 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '630 patent and knew of its infringement, including by way of this lawsuit.

627. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '630 Products and had knowledge that the

¹³³ Products incorporating Microsoft Azure Active Directory functionality include: Microsoft Office 365 products and services; Microsoft OneDrive for Business; Microsoft SharePoint Online; Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple), and Microsoft Azure RMS.

inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '630 patent. Microsoft 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, Microsoft provides the Microsoft '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 claim 16, and Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '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 Microsoft '630 Products in a manner that directly infringes one or more claims of the '630 patent, including at least claim 16, Microsoft specifically intended to induce infringement of the '630 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '630 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '630 patent.¹³⁴ Accordingly, Microsoft 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.

¹³⁴ See *e.g.*, *What is Azure Rights Management?*, Microsoft TechNet Article (July 1, 2015); Dan Plastina, *Microsoft Rights Management* at 1, MICROSOFT TECHNICAL DOCUMENTATION (July 2013); Julia Kornich, *Use AES-128 Dynamic Encryption and Key Delivery Service*, MICROSOFT AZURE DOCUMENTATION (September 16, 2015); Jeff Fried, *Information Management Strategy with Microsoft Office 365 in Mind*, MICROSOFT IGNITE PRESENTATION (May 4, 2015); *Logging and Analyzing Azure Rights Management Usage*, AZURE RIGHTS MANAGEMENT TECHNET LIBRARY (July 1, 2015); *Enabling Enterprise Mobility Through People-Centric IT*, MICROSOFT WHITE PAPER (October 2014); *[MS-RMPR] Rights Management Services (RMS): Client-to-Server Protocol*, MSDN LIBRARY TECHNICAL DOCUMENTS (June 30, 2015); *Azure RMS Security Evaluation Guide*, MICROSOFT RIGHTS MANAGEMENT WHITE PAPER 13 (May 2015); M. Baldwin, *Authentication Scenarios for Azure AD*, AZURE ACTIVE DIRECTORY DOCUMENTATION (September 17, 2015).

628. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '630 patent.

629. As a result of Microsoft's infringement of the '630 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

COUNT X
INFRINGEMENT OF U.S. PATENT NO. 8,600,895

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

631. Microsoft makes, sells, offers to sell, imports, and/or uses Microsoft Azure Active Directory ("Azure Active Directory").

632. Microsoft makes, sells, offers to sell, imports, and/or uses products and services that incorporate Azure Active Directory functionality. These products and services include: Microsoft Intune,¹³⁵ Microsoft Office 365,¹³⁶ Microsoft Dynamics CRM Online,¹³⁷ Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple),¹³⁸ Microsoft Azure RMS,¹³⁹ Office 365 SharePoint Online,¹⁴⁰ and Microsoft OneDrive.¹⁴¹ ("Azure Active Directory Applications").

¹³⁵ *Microsoft Intune*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/microsoftintunemdm/> ("By default, Microsoft Intune works with Azure AD.").

¹³⁶ *Microsoft Office 365*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/office365/> ("By default, Office 365 works with Azure AD.").

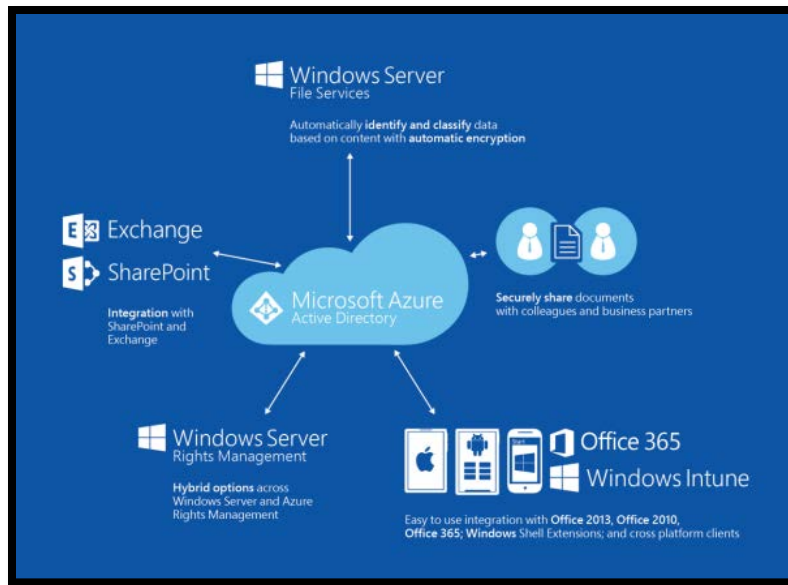
¹³⁷ *Microsoft Dynamics CRM*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/crm/> ("By default, Dynamics CRM works with Azure AD.").

¹³⁸ *Protecting Microsoft Azure Blob Storage with Microsoft Azure AD Rights Management in Cloud Services and Web Applications*, MSDN WHITE PAPER (2015).

¹³⁹ *Protecting Data in Microsoft Azure* at 32, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014).

633. Azure Active Directory and Azure Active Directory Applications (collectively, the “Azure Active Directory System” or “Microsoft ’895 Products”) is a system for controlling access to a plurality of records stored within a plurality of automated external databases.

634. The below image from Microsoft’s Azure Active Directory documentation shows the breadth of products and services that incorporate Azure Active Directory functionality.



Hybrid Identity at 25, MICROSOFT WHITE PAPER (2015) (listing Windows Server, Microsoft Exchange, Microsoft SharePoint, Office 365, Windows Intune and Windows Server as incorporating Azure Active Directory functionality).

635. On information and belief, the Azure Active Directory System—through server-side program code written, maintained, and sold by Microsoft; and stored on and executed by Microsoft cloud servers controls access to a plurality of records within a plurality of automated external databases (e.g., documents and application data stored in and/or hosted by a plurality of structured or unstructured Azure cloud data stores, each external to the centralized Azure Active Directory authentication and access control index), each record having an associated set of

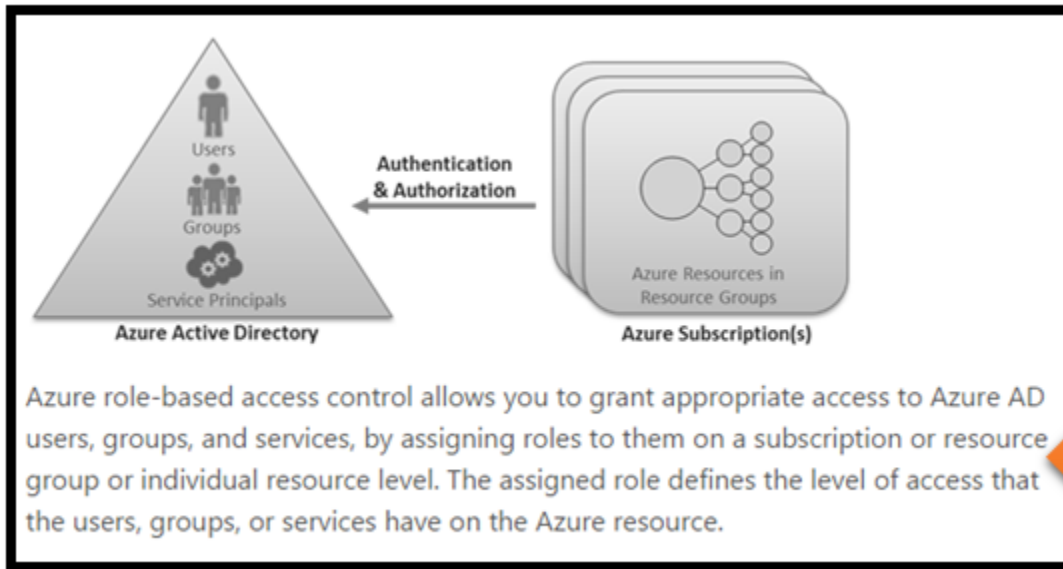
¹⁴⁰ *Office 365 SharePoint Online*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/sharepoint/> (“By default, Office 365 SharePoint Online works with Azure AD.”).

¹⁴¹ *Microsoft OneDrive*, MICROSOFT AZURE DOCUMENTATION (2015), <https://azure.microsoft.com/en-us/marketplace/partners/microsoft-corporation/skydrive/> (“Use Azure AD to enable user access to Microsoft OneDrive.”).

access rules (e.g., an associated set of Azure Active Directory Access Control 2.0 access rules and/or data store specific native access rules), a location identifier (e.g., an Azure Active Directory URI for the record and/or its data store), and a content identifier (e.g., Azure Active Directory and/or other content metadata for a respective record) maintained in an automated centralized index (e.g., an automated, centralized Azure Active Directory authentication and access control index).

636. On information and belief, the Azure Active Directory System performs a method of controlling access to a plurality of records stored within a plurality of automated external databases, each record having an associated set of access rules (“ASAR”), a location identifier (“LI”), and a content identifier (“CI”) maintained in an automated centralized index (“ACI”).

637. On information and belief, the Azure Active Directory System receives a request (e.g., REST html request) for specified information content (e.g., Office 365 documents and/or Azure-hosted application data relating to a specified user, group, organization, and/or subject). The request is communicated from a requestor (e.g., Azure AD-enrolled end user; Azure AD-enlightened native or web application; Azure AD-enlightened web service) and contains a specific content identifier (“SCI”) (e.g., human-readable and/or machine-encoded content identification metadata relating to the specified information content).

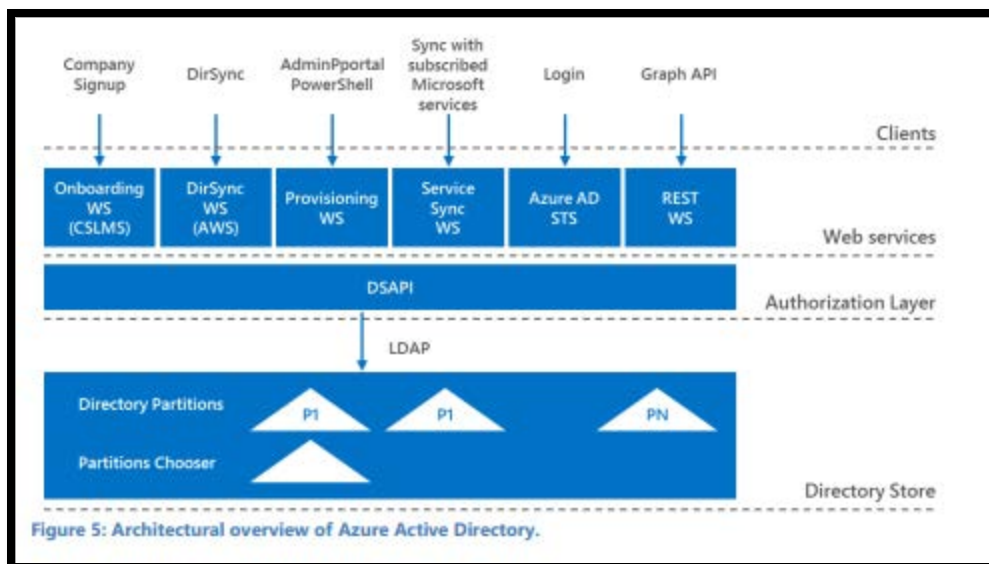


Ingrid Henkel, *Role-based Access Control in the Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015) (the yellow arrow points to the description of Azure Active Directory as enabling role based authentication and authorization).

638. On information and belief, the Azure Active Directory System authenticates a requestor (e.g., Azure Active Directory-enrolled end user; Azure Active Directory-enlightened native or web application; Azure Active Directory-enlightened web service) by cryptographically verifying authentication credentials received in and/or with the request (e.g., authentication header credentials in a REST html request).

639. On information and belief, the Azure Active Directory System queries the centralized Azure Active Directory authentication and access control index to find entries corresponding to the specified content identifier (e.g., the human-readable and/or machine-encoded content identification metadata relating to the specified information content (e.g., user, group, organization, and/or subject)).

640. The below diagram shows the architecture of the Azure Active Directory System.



Protecting Data in Microsoft Azure at 10, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014).

641. On information and belief, for each found query the Azure Active Directory System applies an associated set of access rules ("ASAR") corresponding to the LI to determine if the record stored in a respective automated external database ("AXD") of the plurality of automated external databases corresponding to the LI is accessible. For example, for each found query (e.g., entry in the centralized Azure Active Directory authentication and authorization index corresponding to the request SCI), the Azure Active Directory web service applies the ASAR (e.g., Active Directory Access 2.0 authorization rules) corresponding to the LI (e.g., Azure Active Directory URI for the ACI entry and/or its data store) to determine if the record (e.g., Office 365 document and/or Azure-hosted application data file) stored in a respective automated external database (e.g., individual Azure-stored and/or hosted structured or unstructured data store) of the plurality of automated external databases corresponding to the LI is accessible given the authenticated request context (e.g., user id, role, time, client hardware and/or software, etc.).

642. On information and belief, for each accessible record ("AR"), the Azure Active Directory System automatically communicates from the centralized automated security processor to the AXD storing the AR information sufficient to determine whether the AR is releasable by

the AXD storing the AR by applying a set of native access rules maintained by the AXD storing the AR. For example, for each record (e.g., Office 365 document and/or Azure-hosted application data file) determined to be accessible, the Azure Active Directory System automatically communicates to the automated external database (e.g., individual Azure-stored and/or hosted structured or unstructured data store) information (content and/or access metadata (e.g., OAUTH 2.0 authorization scope information) in a format compatible with the respective AXD) sufficient to determine whether the record determined to be accessible is releasable by the AXD storing the record by applying a set of native access rules maintained by the AXD storing the record (e.g., record-specific access rules local to the respective Azure-stored and/or –hosted structured or unstructured data store, which may be in a standards-compliant or proprietary format).

643. On information and belief, the Azure Active Directory System logically associates the releasable ARs (e.g., the Office 365 documents and/or Azure-hosted application data files determined to be releasable to the requestor in view of the authenticated request context) into a linked set of releasable ARs (e.g., one or more data objects logically associated with the releasable Office 365 documents and/or Azure-hosted application data files and/or with references to the releasable Office 365 documents and/or Azure-hosted application data files).

644. On information and belief, the Azure Active Directory System communicates the linked set of releasable ARs to the requestor (e.g., Azure Active Directory- enrolled end user; Azure Active Directory - enlightened native or web application; Azure Active Directory - enlightened web service).

645. On information and belief, Microsoft 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 securely controlling access to a plurality of digital records by a remote computer, including but not limited to, the Microsoft '895 Products, which include infringing information records infrastructure technologies. Such products and/or services

include, by way of example and without limitation, Microsoft products and services that incorporate Microsoft Azure Active Directory functionality.¹⁴²

646. By making, using, testing, offering for sale, and/or selling products and services for securely controlling access to a plurality of digital records by a remote computer, including but not limited to the Microsoft '895 Products, Microsoft 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).

647. On information and belief, Microsoft also indirectly infringes the '895 patent by actively inducing infringement under 35 U.S.C. § 271(b), at least as of the date of service of this Complaint.

648. On information and belief, Microsoft has had knowledge of the '895 patent since at least service of this Complaint or shortly thereafter, and on information and belief, Microsoft knew of the '895 patent and knew of its infringement, including by way of this lawsuit.

649. On information and belief, Microsoft intended to induce patent infringement by third-party customers and users of the Microsoft '895 Products and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement. Microsoft specifically intended and was aware that the normal and customary use of the accused products would infringe the '895 patent. Microsoft 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, Microsoft provides the Microsoft '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 Microsoft further provides documentation and training materials that cause customers and end users of the Microsoft '895 Products to utilize the

¹⁴² Products incorporating Microsoft Azure Active Directory functionality include: Microsoft Office 365 products and services; Microsoft OneDrive for Business; Microsoft SharePoint Online; Microsoft Azure storage services (e.g., Azure Blob Storage, Azure Table Storage, Azure SQL, and Azure StorSimple), and Microsoft Azure RMS.

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 Microsoft '895 Products in a manner that directly infringes one or more claims of the '895 patent, including at least claims 1, 8, and 16, Microsoft specifically intended to induce infringement of the '895 patent. On information and belief, Microsoft engaged in such inducement to promote the sales of the Microsoft '895 Products, *e.g.*, through Microsoft's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '895 patent.¹⁴³ Accordingly, Microsoft 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.

650. To the extent applicable, the requirements of 35 U.S.C. § 287(a) have been met with respect to the '895 patent.

651. As a result of Microsoft's infringement of the '895 patent, St. Luke has suffered monetary damages, and seeks recovery in an amount adequate to compensate for Microsoft's infringement, but in no event less than a reasonable royalty for the use made of the invention by Microsoft together with interest and costs as fixed by the Court.

¹⁴³ See *e.g.*, *Protecting Data in Microsoft Azure*, MICROSOFT AZURE PLATFORM WHITE PAPER (August 2014); Ingrid Henkel, *Role-based Access Control in the Microsoft Azure Portal*, MICROSOFT AZURE ACTIVE DIRECTORY DOCUMENTATION (August 14, 2015); *Hybrid Identity*, MICROSOFT WHITE PAPER (2015); *Access Control Service 2.0*, MICROSOFT MSDN TECHNICAL LIBRARY (April 14, 2015); *Administering Your Azure AD Directory*, MICROSOFT MSDN TECHNICAL LIBRARY (September 15, 2015); Simon May and Joe Breslin, *Azure AD and Identity Show: Azure AD B2C (Business to Consumer)*, MSDN AZURE AD AND IDENTIFY SHOW (September 16, 2015); Malcolm Jeffrey, *Protecting your data with AD-RMS and Azure RMS*, MICROSOFT IGNITE NEW ZEALAND PRESENTATION (available on MSDN Channel 9) (September 2, 2015).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff St. Luke respectfully requests that this Court enter:

- A. A judgment in favor of Plaintiff St. Luke that Microsoft has infringed, either literally and/or under the doctrine of equivalents, the '237 patent, the '017 patent, the '591 patent, the '181 patent, the '247 patent, the '377 patent, the '368 patent, the '941 patent, the '630 patent, and/or the '895 patent.
- B. An award of damages resulting from Microsoft's acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order requiring Microsoft 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: October 1, 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