

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

ST. LUKE TECHNOLOGIES, LLC,

Plaintiff,

v.

ORACLE AMERICA, INC.,

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”); 7,587,368 (“the ‘368 patent”); 8,380,630 (“the ‘630 patent”); and 8,600,895 (“the ‘895 patent”) (collectively, the “patents-in-suit”). Defendant Oracle America, Inc. (“Oracle” 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.*

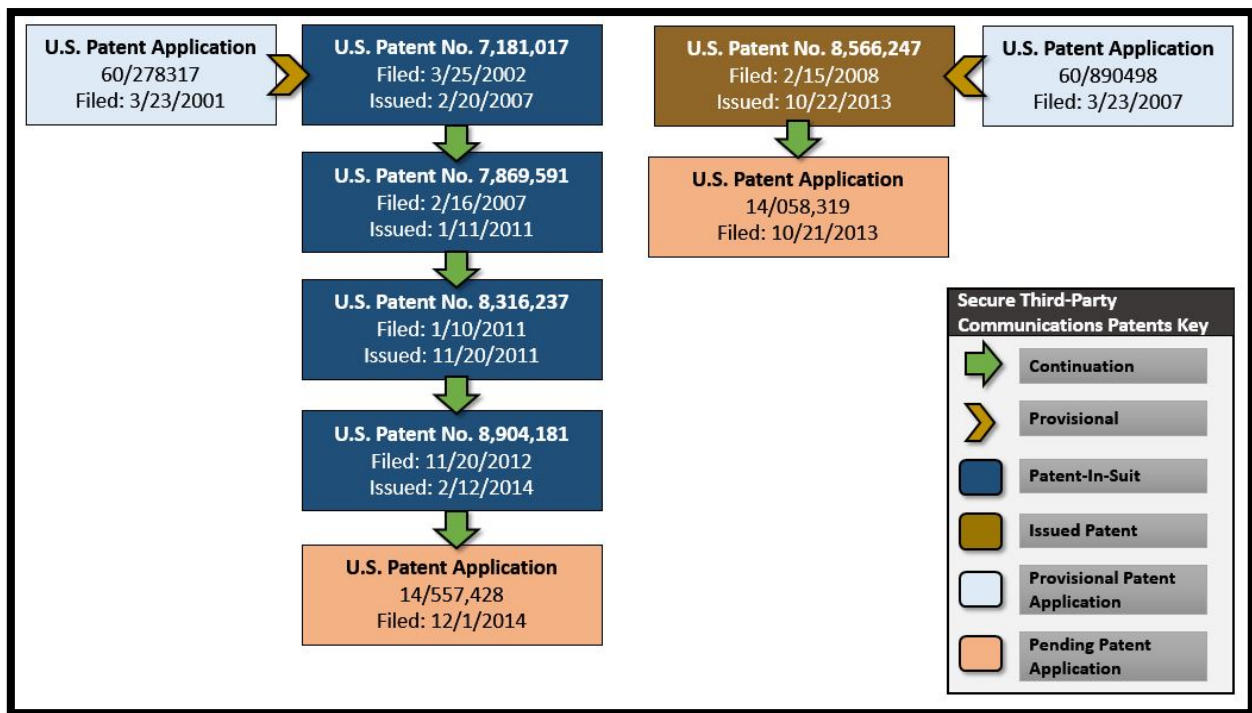
INTRODUCTION

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, Oracle has unlawfully and without permission copied the technologies and inventions of Dr. Robert H. Nagel, David P. Felsher, and Steven M. Hoffberg.

2. Dr. Nagel, Mr. Felsher, and Mr. Hoffberg are the co-inventors of the ‘237 patent, the ‘017 patent, the ‘591 patent, the ‘181 patent, and U.S. Patent No. 8,566,247 (“the ‘247 patent”) (collectively, the “Secure Third-Party Communications Patents” or “STPC patents”). The STPC patents have been cited in over 550 United States patents and patent applications as

prior art before the United States Patent and Trademark Office.¹ 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 Oracle infringes.²



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

¹ The STPC patents have been cited as prior art in three patents and published patent applications assigned to Oracle. See U.S. Patent Nos. 8,064,604; 8,463,624; and U.S. Patent App. No. 2013/0343544.

² St. Luke’s STPC patents are in two patent families claiming priority to U.S. Patent Applications 60/278,317 and 60/890,498.

Felsher, and Mr. Hoffberg's secure third party communications system as the "gold standard for protecting data privacy" *Oracle Customers Secure Critical Encryption Keys with Oracle Key Vault*, ORACLE PRESS RELEASE (August 7, 2014).

5. Oracle executives have repeatedly stated encrypted communication systems such as the inventions disclosed in the STPC patents are essential to successful cloud computing security.³

6. Oracle has recognized that systems such as Dr. Nagel and his co-inventors' secure third party communications system solve critical security issues presented by the increasing use of cloud computing.

One of the *key concerns* for organizations as they move to a shared resource model on the Cloud is insuring the *security of their data*. The Oracle Database Cloud Service, like the Oracle Database that is the foundation of the Database Cloud, has been created from the beginning with the utmost concern for security.

Security and the Oracle Database Cloud Service, ORACLE WHITE PAPER (Sept. 2012) (emphasis added).

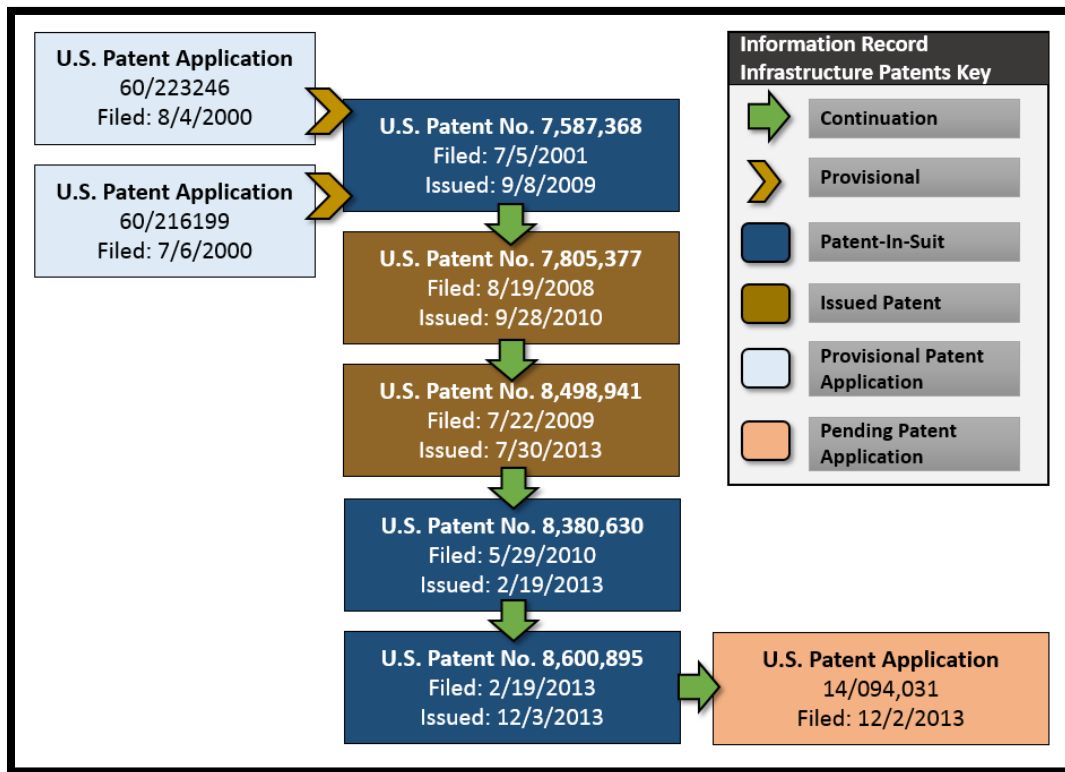
7. Mr. Felsher is the inventor of the '368 patent, the '630 patent, the '895 patent, and U.S. Patent Nos. 8,498,941 ("the '941 patent"), and 7,805,377 ("the '377 patent") (collectively, the "Information Record Infrastructure Patents" or "IRI patents"). The IRI patents have been cited by over 970 United States patents and patent applications as prior art before the United States Patent and Trademark Office.

8. The IRI patents have been cited as prior art in twenty-four patents and published patent applications assigned to Oracle. *See* U.S. Patent Nos. 7,165,246; 7,222,331; 7,272,830; 7,281,244; 7,484,095; 7,593,942; 7,814,075; 7,814,076; 7,831,570; 8,121,955; 8,234,694; 8,463,624; 8,473,417; 8,732,856; 9,049,195; and U.S. Patent App. Nos. 2013/0110923; 2013/0346104; 2014/0067407; 2004/0143551; 2004/0143641; 2004/0143820; 2004/0143827; 2004/0143831; and 2004/0154013.

³ *See e.g., Oracle Customers Secure Critical Encryption Keys with Oracle Key Vault*, ORACLE PRESS RELEASE (Aug. 7, 2014); *Oracle Introduces Key Vault Software Appliance to Manage and Safeguard Encryption Keys*, DATABASE TRENDS AND APPLICATIONS (Aug. 7, 2014).

9. 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 based on the access privileges of the user.

10. The below diagram shows the IRI patent family tree, a pending IRI patent application, and the IRI patents Oracle infringes.



THE INVENTORS' LANDMARK SECURE COMMUNICATION SYSTEMS

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

12. 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

13. 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>.

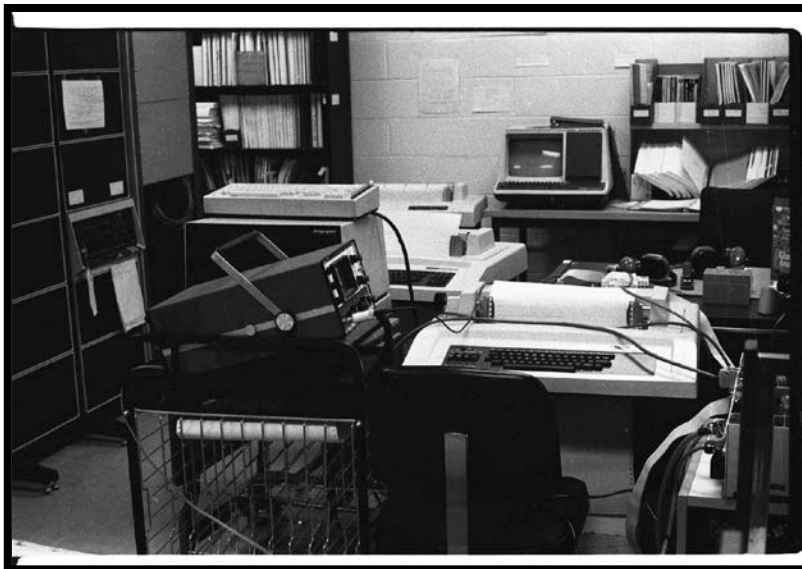


IMAGE OF THE DEC PDP-11/50 SYSTEM, COLUMBIA UNIVERSITY COMPUTING HISTORY ARCHIVE (circa 1976), <http://www.columbia.edu/cu/computinghistory/> (showing an installed PDP-11/50 device that was a component in Dr. Nagel's data distribution system).

14. 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.”).



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

Reuters Announces Retrieval System For Cable TV Subscribers, BROADCAST MANAGEMENT/ENGINEERING MAGAZINE at 9, February 1975.

15. 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).

16. 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 Oracle 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).

17. 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.

18. 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.

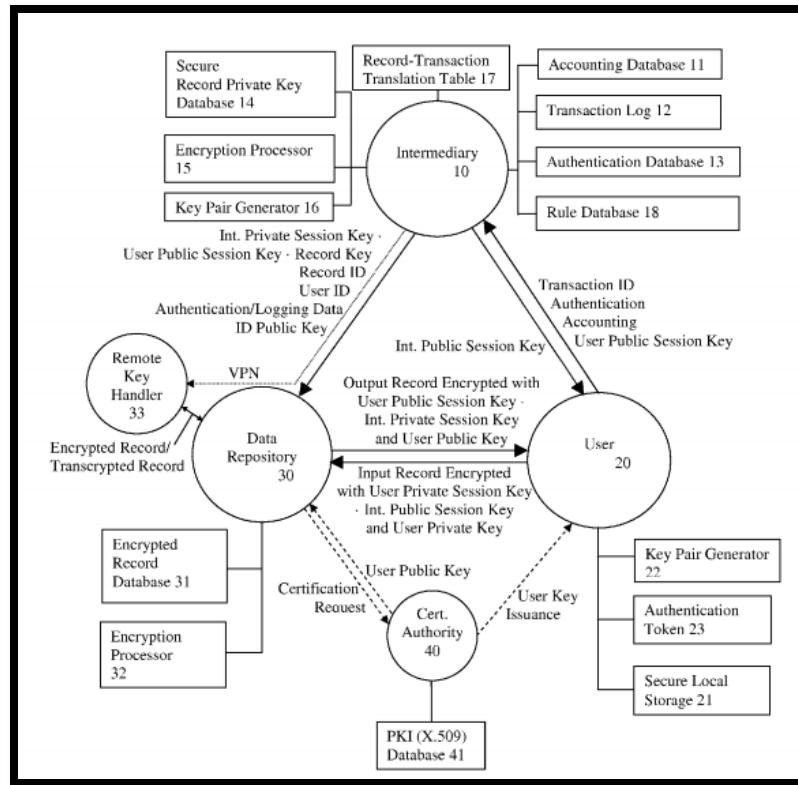
19. The rise of cloud computing (the delivery of on-demand computing resources over a distributed network), has made Dr. Nagel and his co-inventors' insights uniquely valuable. Medical records, financial information, email messages, and other forms of electronic data are now placed on remote servers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

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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**

26. The inventions taught in the STPC patents relate to the encryption of data passed through an intermediary and have been recognized by Oracle as important and valuable. “One of the key concerns for organizations as they move to a shared resource model on the Cloud is insuring the security of their data.”¹³

27. The adoption of secure encryption technologies is critical to the success of Oracle’s products and services, especially in the lucrative cloud computing market.

Gain all of the benefits of the cloud – including lower IT costs, increased business agility, less complexity, and greater flexibility – *without sacrificing security or ceding control of your data.*

Oracle Cloud: The Next-Generation Public Cloud That Adapts to Your Organization, ORACLE DOCUMENTATION (2015) (emphasis in original).

28. 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

¹³ *Security and the Oracle Database Cloud Service*, ORACLE WHITE PAPER (Sept. 2012).

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.

- 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 N.V.
- 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

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



30. 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 Oracle, Fellowship Filtering relies on its intellectual property. Oracle’s Executive Chairperson, Larry Ellison, explained the importance of protecting Oracle’s intellectual property:

SAP pleaded guilty to criminal theft of our software. Let me be clear. I’m not accusing SAP of anything. What did SAP do? ***Did you engage in criminal behavior and steal lots of Oracle software? Yes. That’s SAP.***¹⁵

31. On information and belief, Oracle has asserted its patents in federal courts, including the Eastern District of Texas.¹⁶

32. On information and belief, Oracle is a Delaware corporation with its principal office at 500 Oracle Parkway, Redwood City, California 94065. Oracle can be served through its registered agent, Corporation Service Company d/b/a CSC-Lawyers Inco, 211 E. 7th Street Suite 620, Austin, Texas 78701.

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

- A campus in Austin, Texas that is undergoing a rapid expansion.¹⁷

¹⁵ *D10 Video: Larry Ellison Session Highlights*, WALL ST. J. D: ALL THINGS DIGITAL CONFERENCE, May 30, 2012, <http://www.wsj.com/video/d10-video-larry-ellison-session-highlights/909E5610-BBBC-47F4-A056-D96203CBD038.html> (emphasis added); *see also Oracle America, Inc. v. Google Inc.*, Case No. 10-cv-03561 Dkt. No. 1 ¶ 15 (N.D. Cal. August 12, 2010) (“By purposefully and voluntarily distributing one or more of its infringing products and services, Google has injured Oracle America and is thus liable to Oracle America for infringement of the patents at issue.”),

¹⁶ *i2 Technologies, Inc. et al v. Oracle Corporation et al.*, Case No. 10-cv-00284 Dkt. Nos. 85 & 130 (E.D. Tex.).

- A 55,000 sq. ft. office and training center in Irving, Texas.¹⁸
- Data centers throughout Texas that offer the infringing Oracle products.¹⁹

34. According to Oracle's website, Oracle offers infringing products for sale throughout the United States and Canada, including in the Eastern District of Texas. Further, Oracle 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 Oracle's engagements with Texas entities;²⁰ (2) ongoing contracts with the state of Texas;²¹ (3) Oracle's agreement to be subject to the laws and jurisdiction of Texas;²² (4) Oracle's certification that it is licensed to conduct business in

¹⁷ *Contacts – State of Texas: State Customers*, ORACLE WEBSITE, May 2015, <http://www.oracle.com/us/corporate/pricing/contracts-texas-2196375.html>; Amy Denney & Audrey Spencer, *Oracle to Add 200 jobs, New Office in Austin*, IMPACT NEWS, November 5, 2013, <http://impactnews.com/austin-metro/northwest-austin/oracle-to-add-200-jobs-new-office-in-austin/>

¹⁸ Katherine Leal Unmuth, *Oracle Moves Location On Irving*, The Dallas Morning News, June 10, 2010, <http://irvingblog.dallasnews.com/2010/06/oracle-moving-to-irving.html/> (“About 500 Oracle workers are located in Irving.”).

¹⁹ *Delivering Cloud Services to the State of Texas*, AN ORACLE ENTERPRISE ARCHITECTURE WHITE PAPER 11 (February 2015) (Oracle offers its infringing products through data centers maintained by its partners Verio Enkitic and SunGard. These data centers are located in or near this district at: (1) Verio, Inc. Oracle 15950 Dallas Parkway, Dallas, Texas; (2) Enkitech 5065 North MacArthur Boulevard, Irving, Texas; and (3) SunGard 1001 East Campbell Road, Richardson, Texas.).

²⁰ *Contacts – State of Texas: State Customers*, ORACLE WEBSITE, May 2015, <http://www.oracle.com/us/corporate/pricing/contracts-texas-2196375.html>; Amy Denney & Audrey Spencer, *Oracle to Add 200 jobs, New Office in Austin*, IMPACT NEWS, November 5, 2013, http://impactnews.com/austin-metro/northwest-austin/oracle-to-add-200-iobs-new-office-in-austin (“Gov. Rick Perry’s office announced Nov. 1 that Oracle would receive \$1 million for its \$5.4 million investment. This amount would come from the state’s Texas Enterprise Fund that creates jobs and helps Texas businesses grow.”).

²¹ *DIR Contract No. DIR-TSO-2539*, STATE OF TEXAS DEPARTMENT OF INFORMATION RESOURCES CONTRACT FOR PRODUCTS AND RELATED SERVICES ORACLE AMERICA, INC. (2014), <http://publishingext.dir.texas.gov/portal/internal/contracts-and-services/Contracts/DIR-TSO-2539%20Oracle%20Contract.pdf>.

²² *Id.* (“The laws of the State shall govern the construction and interpretation of the Contract. Exclusive venue for all actions will be in the courts located in Texas.”).

Texas;²³ (5) Oracle's assent to Texas insurance liability;²⁴ and (6) Oracle's agreement (in prior contracts with the state of Texas) to make documentation available to residents of Texas.²⁵

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 Defendant Oracle in this action because Oracle 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 Oracle would not offend traditional notions of fair play and substantial justice. Defendant Oracle, 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, Oracle is registered to do business in the state of Texas, and has appointed Corporation Service Company d/b/a CSC-Lawyers Inco, 211 E. 7th Street Suite 620, Austin, Texas 78701, as its agent for service of process. This Court also has personal jurisdiction over Oracle because it has a principal place of business in Texas.

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

²³ *Id.* (“Ability to Conduct Business in Texas, is hereby restated in its entirety as follows: Vendor is authorized and validly existing under the laws of its state of organization, and shall be authorized to do business in the State of Texas.”).

²⁴ *Id.* (“licensed in the State of Texas, and authorized to provide the corresponding coverage”).

²⁵ *Id.* (“Pursuant to S.B. 1368 of the 83rd Texas Legislature, Regular Session, upon reasonable written request to Vendor, Vendor shall to make any public information (as defined in Texas Government Code Section 552.002) in Vendor's possession which was created or exchanged with the State pursuant to this Contract, and not otherwise excepted from disclosure under the Texas Public Information Act, available in paper or electronic format that is accessible by the public at no additional charge to the State.”).

infringement in the Eastern District of Texas. Additionally, Oracle has previously availed itself of this Court by filing permissive counterclaims of patent infringement in the Eastern District of Texas.²⁶

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. Oracle prizes systems that provide secure third party communications through an intermediary. An Oracle white paper from 2012 described data security as an “utmost concern.”

One of the key concerns for organizations as they move to a shared resource model on the Cloud is insuring the security of their data. The Oracle Database Cloud Service, like the Oracle Database that is the foundation of the Database Cloud, has been created from the beginning with the utmost concern for security.

Security and the Oracle Database Cloud Service, ORACLE WHITE PAPER (Sept. 2012).

40. Oracle recognized that, until recently, security for distributed systems was not a primary concern.

²⁶ *i2 Technologies, Inc. et al v. Oracle Corporation et al.*, Case No. 10-cv-00284 Dkt. Nos. 85 & 130 (E.D. Tex.).

- 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).

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

and backup mechanisms. As organizations increasingly encrypt data at rest and on the network, securely managing all the encryption keys and credential files in the data center has become a major challenge.

At the same time, organizations also need to comply with stringent regulatory requirements for managing keys and certificates. Many global regulations and industry standards call for audits demonstrating that keys are routinely rotated, properly destroyed, and accessed solely by authorized entities.

Oracle Customers Secure Critical Encryption Keys with Oracle Key Vault, ORACLE PRESS RELEASE (August 7, 2014).

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

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

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

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

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

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

44. 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.

45. 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. Bellovin²⁷ 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 PAPER (Aug. 1998).

46. 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

²⁷ At the time, Professor Bellovin was a Fellow at AT&T research laboratories.

to the realm of computers and specifically network cloud computing. “As we know, public cloud uses virtualization heavily as they share resources between many customers. As a result, this creates security vulnerabilities, both from access levels as well as from exploits in the virtualization software.”²⁸

47. 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.

48. ***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 than 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.²⁹

²⁸ Mohd Ujaley, *Cloud Adoption Requires Thorough Risk Assessment: Dell*, EXPRESS COMPUTER (May 26, 2015) (emphasis added) (the quote comes from an interview with Dell General Manager Murli Mohan).

²⁹ 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*.”).



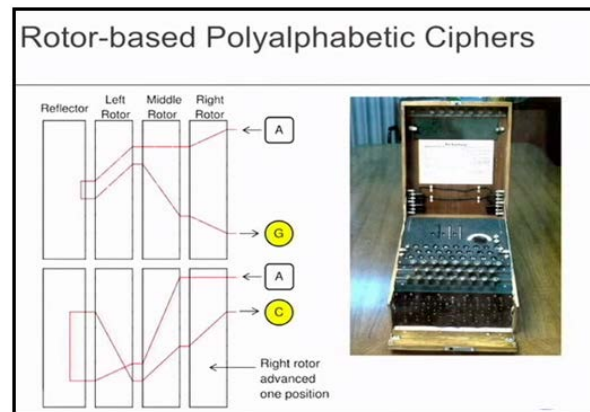
Alexander Stanoyevitch, INTRODUCTION TO CRYPTOGRAPHY WITH MATHEMATICAL FOUNDATIONS AND COMPUTER IMPLEMENTATIONS PRESS (2002).

49. 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.³⁰ 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.

50. ***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

³⁰ 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.³¹ Alan Turing (among others) wanted a technique to break Enigma that did not rely on the key, which could (and frequently did) change.³² 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).

51. ***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

³¹ 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.).

³² 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 deduce a so-called “menu” from a given piece of cipher text and a suspected piece of corresponding plaintext. 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.

52. 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).

53. 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.

54. 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.

55. 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).

56. 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.

57. 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.

58. 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).

59. 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).

60. 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.

61. 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

62. 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."³³ 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).

63. Oracle and its competitor companies, such as 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).

³³ 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).

64. 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).³⁴

³⁴ 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).

65. 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.

66. 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

67. U.S. Patent No. 8,316,237 (the “237 patent”) entitled, System and Method for Secure Three-Party Communications, was filed on January 10, 2011 and claims priority to March 23, 2001. St. Luke is the owner by assignment of the ‘237 patent. A true and correct copy of the ‘237 patent is attached hereto as Exhibit A. The ‘237 patent claims specific methods and systems for securely 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.

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

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

- Certicom Corp.
- Wincor Nixdorf International GmbH
- **Oracle International Corporation**
- Futurewei Technologies, Inc.
- Dell Products, L.P.
- Intuit Inc.

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

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

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

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

71. Although the systems and methods taught in the '237 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the '237 patent claims were innovative and novel. “Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring.” '237 patent, col. 2:56-61. Indeed, Oracle has 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).

72. Further, the '237 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient.³⁵ “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).

³⁵ 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.”); Elena 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.”).

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

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

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

76. Researchers have identified the problems the '237 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).³⁶

77. The '237 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '237 patent require 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.

78. 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

³⁶ 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.

79. 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.

80. 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.

81. 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.

82. 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.

83. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”³⁷ the '237 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

84. 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.

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

86. The '237 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”³⁸

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

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

³⁸ *TQP Dev., LLC v. Intuit Inc.*, Case No. 2:12-CV-180-WCB, 2014 WL 651935, at *4 (E.D. Tex. Feb. 19, 2014) (finding claims directed to encryption to be patent eligible); *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.’”).

88. 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).

89. 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.³⁹

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

91. 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

³⁹ 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."⁴⁰

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).

92. 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."⁴¹

93. 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.

94. '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.


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

⁴⁰ See also *BackupEDGE Encryption Whitepaper*, MICROLITE CORPORATION at 2 (2003) (describing the technology of asymmetric keys as "new"); Roger Clarke, MESSAGE TRANSMISSION SECURITY (May 1998), <http://www.rogerclarke.com/II/CryptoSecy.html> ("Public key cryptography is relatively new and technically complex.").

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

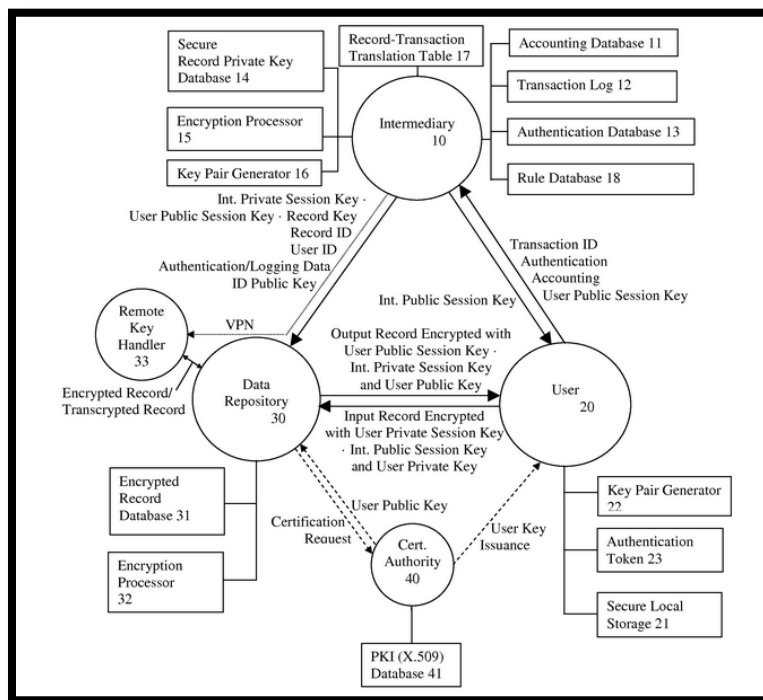
Encryption concepts and terminology

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).

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



'237 patent, Fig. 1.

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

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

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

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

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

- Hitachi-Omron Terminal Solutions, Corporation
- Medapps, Inc.
- Samsung Electronics Co., Ltd.
- NEC Corporation
- Visa International Service Corporation
- Cisco Technology, Inc.
- Yahoo!, Inc.
- Flexera Software LLC
- CompuGroup Medical AG
- Datcard Systems, Inc.
- Futurewei Technologies, Inc.
- 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.

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

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

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

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

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

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

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

102. Further, the '017 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient.⁴² "Third parties, however,

⁴² 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."); Elena 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).

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

104. The ‘017 patent claims are not directed at the broad concept/idea of “encrypting” or “decrypting” information. Instead, they are limited to a concretely circumscribed set of methods and systems for 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.

105. 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.”).

106. Oracle has 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 at 6 (2010).

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

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

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).⁴³

108. The '017 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '017 patent require cryptographically manipulating protected electronic information using

⁴³ 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.

109. The '017 patent is directed to specific problems in the field of cryptography. In the “Background” section of the patent, the '017 patent explains that encryption systems use “keys,” similar to passwords, to control how plaintext is encrypted and decrypted. '017 patent, col. 4:39–4:64. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id.* Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of 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 text. *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.

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

A method for processing information, comprising the steps of:

receiving information to be processed:

defining a cryptographic comprehension function for the information, adapted for making at least a portion of the information incomprehensible;

receiving asymmetric cryptographic key information, comprising at least asymmetric encryption key information and asymmetric decryption key information;

negotiating a new cryptographic comprehension function between two parties to a communication using an intermediary;

processing the information to invert the cryptographic comprehension function and impose the new cryptographic comprehension function in an integral process, in dependence on at least the asymmetric cryptographic key information, without providing the intermediary with sufficient asymmetric cryptographic key information to decrypt the processed information; and

outputting processed information,

wherein the ability of the asymmetric decryption key information to decrypt the processed information changes dynamically.

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

112. The '017 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '017 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

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

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users' private encryption keys into components and for sending those components to trusted agents chosen by the particular users.
- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.

- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls and Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Virtual Private Networks. As described in: U.S. Pat. No. 6,079,020 to Liu and U.S. Pat. No. 6,081,900 and twenty other patented systems involving virtual private networks that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.
- Biometric Authentication. U.S. Pat. No. 5,193,855 to Shamos, disclosing the use of biometrics such as fingerprints to facilitate secure communications and identification of users. Further, the '017 lists numerous patented systems that use biometric authentication that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

114. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁴⁴ the claims in the ‘017 patent do not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

⁴⁴ *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).

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

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

117. The '017 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁴⁵

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

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

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

⁴⁵ *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.’”).

121. The systems and methods claimed in the '017 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 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."⁴⁶

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).

122. The asserted claims do not involve a method of doing business implemented on a computer; instead, it involves a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that the '017 patent is directed at were new and unique to distributed networks as confirmed in a recent paper from Accenture Services Pvt. Ltd. "The unprecedented growth of cloud computing has created new security challenges. The problem is ever more complex as there is a transition from traditional computing to a service-based computing."⁴⁷

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

124. The '017 patent claims cover a systems and methods that transform data from one form into another that will be recognizable by the intended recipient but secure against


⁴⁶ 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.").

⁴⁷ 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).

decryption by unintended recipients. IBM, in its reference guides (“redbooks”), refers to encryption as “transform[ing] data that is unprotected.”

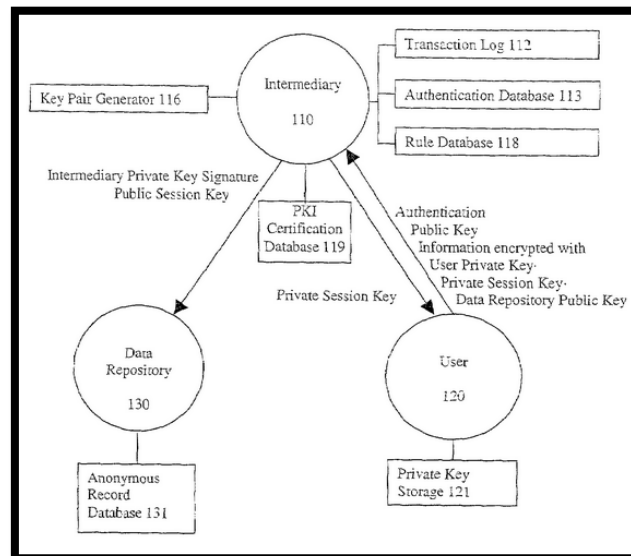
Encryption concepts and terminology

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).

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



‘017 patent, Fig. 2.

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

126. U.S. Patent No. 7,869,591 (the “‘591 patent”) entitled, System and Method for Secure Three-Party Communications, was filed on February 16, 2007, and claims priority to

March 23, 2001. St. Luke is the owner by assignment of the '591 patent. A true and correct copy of the '591 patent is attached hereto as Exhibit C.

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

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

128. The '591 patent claims specific methods and systems for secure third-party communications—for example, a system and method for communicating information between a first party and a second party that includes identifying desired information; negotiating, through an intermediary, a cryptographic comprehension function for obscuring at least a portion of the information communicated between the first party and the second party; communicating the encrypted information to the second party; and decrypting the encrypted information using the negotiated cryptographic comprehension function. Moreover, in the patented systems and methods, the intermediary does not itself possess sufficient information to decrypt the encrypted information, thus allowing use of an "untrusted" intermediary.

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

130. At the time of the inventions claimed in the '591 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the '591

patent: “Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to additional information, can gain access to private communications or otherwise undermine transactional security or privacy.” ‘591 patent, col. 2:10-15.

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

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

131. Although the systems and methods taught in the ‘591 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the ‘591 patent claims were innovative and novel. “Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring.” ‘591 patent, col. 2:54-69. As described in an article contemporaneous to the ‘591 patent, the rise of cloud computing and distributed networks gave rise to a need to use key encryption to resolve security issues.

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

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

132. Further, the ‘591 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient.⁴⁸ “Third parties, however,

⁴⁸ 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

may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure.” ‘591 patent, col. 2:59-62. Studies have confirmed that the inventions disclosed in the ‘591 patent improve the security of systems.

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

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

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

134. The ‘591 patent claims are not directed at the broad concept/idea of “encrypting” or “decrypting” information. Instead, they are limited to a concretely circumscribed set of methods and systems for 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.

135. 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

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.”); Elena 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.”).

intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

136. Oracle has 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).

137. Researchers have identified the problems the ‘591 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).⁴⁹

⁴⁹ 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.”).

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

139. The '591 patent is directed to specific problems in the field of cryptography. In the “Background” section of the patent, the '591 patent explains that encryption systems use “keys,” similar to passwords, to control how plaintext is encrypted and decrypted. '591 patent, col. 2:16-37. An encryption system thereby encrypts and decrypts information differently depending upon the key input. *Id.* Two common cryptanalytic attacks, linear and differential cryptanalysis, analyze large amounts of 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 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.

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

A method for 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.

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

142. The '591 patent does not preempt the field of secure third-party communications systems, or prevent use of alternative secure third-party communications systems. For example, the '591 patent includes inventive elements—embodied in specific claim limitations—that concretely circumscribe the patented invention and limit its breadth. These inventive elements are not necessary or obvious tools for achieving secure third-party communications, and they ensure that the claims do not preempt other techniques for secure communications.

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

- Key Escrow. U.S. Pat. No. 6,009,177 to Sudia, relates to a cryptographic system and method with a key escrow feature that uses a method for verifiably splitting users'

private encryption keys into components and for sending those components to trusted agents chosen by the particular users.

- Partitioning of Information Storage Systems. U.S. Patent No. 5,956,400 to Chaum, relates to partitioned information storage systems with controlled retrieval.
- Use of a Trusted Intermediary. U.S. Patent No. 6,161,181 to Haynes, describing secure electronic transactions using a trusted Intermediary; U.S. Patent No. 6,145,079 to Misty, describing secure electronic transactions using a trusted intermediary to perform electronic services.
- Split Key Storage. U.S. Patent No. 6,118,874 to Okamoto, teaching encrypted data using split storage key and system.
- Use of a Cryptographic File Labeling System. U.S. Pat. No. 5,953,419 to Lohstroh, disclosing cryptographic file labeling system for supporting secured access by multiple users.
- Computer Security Devices. U.S. Pat. No. 5,982,520 to Weiser, disclosing a personal storage device for receipt, storage, and transfer of digital information to other electronic devices; *see also* U.S. Pat. No. 5,991,519 to Benhammou; U.S. Pat. No. 5,999,629 to Heer; and U.S. Pat. No. 6,034,618 to Tatebayashi.
- Computer Network Firewalls and and Agents. U.S. Pat. No. 6,061,798 to Coley, disclosed the use of an assigned proxy agent to verify the authority of an incoming request to access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

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

144. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁵⁰ the claims in the '591 patent do not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

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

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

147. The '591 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁵¹

148. The claims in the '591 patent require the modifying of data that has concrete and valuable effects in the field of secure third-party communications. By allowing an intermediary to receive secure information but not gain access to the unencrypted form of the information, the '591 patent improves the security of computer systems. Prior art systems that the '591 patent

⁵⁰ *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).

⁵¹ *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.’”).

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).

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

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

151. The systems and methods claimed in the ‘591 patent were not a longstanding or fundamental economic practice at the time of the patented inventions. Nor were they fundamental principles in ubiquitous use on the Internet or computers in general. As just one example, at the time the inventions disclosed in the ‘591 patent were conceived, the use of asymmetric encryption keys was described by Oracle as “relatively new.”⁵²

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/E5364501/tuxedo/docs12cr2/security/publickey.html> (emphasis added).

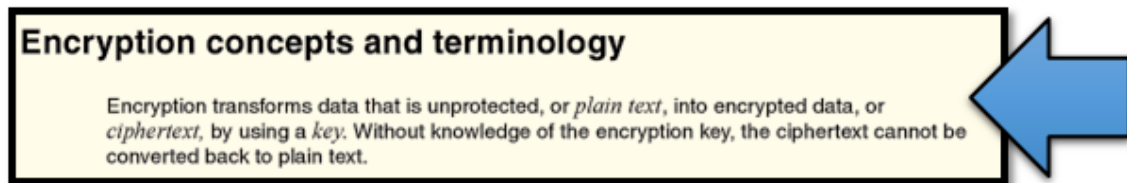
152. The asserted claims do not involve a method of doing business that happens to be implemented on a computer; instead, they involve a method for changing data in a way that will affect the communication system itself, by making it more secure. The security challenges that

⁵² 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 '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."⁵³

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

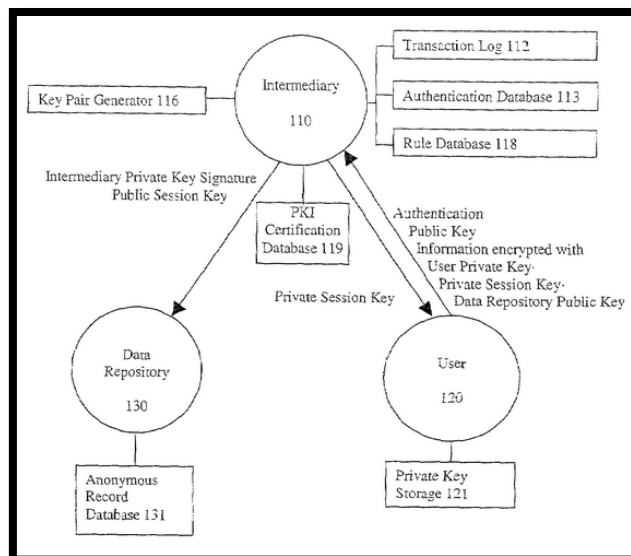
154. '591 patent claims transform data from one form into another that will be recognizable by the intended recipient but secure against decryption by unintended recipients. IBM, in its reference guides ("redbooks"), refers to encryption as "transform[ing] data that is unprotected.



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

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

⁵³ 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).



‘591 patent, Fig. 2.

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

156. U.S. Patent No. 8,904,181 (the “‘181 patent”) entitled, System and Method for Secure Three-Party Communications, was filed on November 20, 2012, and claims priority to March 23, 2001. St. Luke is the owner by assignment of the ‘181 patent. A true and correct copy of the ‘181 patent is attached hereto as Exhibit D. The ‘181 patent claims specific methods and systems for securely 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.

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

158. At the time of the inventions claimed in the ‘181 patent, securely processing, transmitting, and accessing protected electronic data in a massively distributed computing environment presented new and unique issues over the state of the art. As explained in the ‘181 patent: “Often, the nature of these communications protocols places the third party (or group of third parties) in a position of trust, meaning that the third party or parties, without access to

additional information, can gain access to private communications or otherwise undermine transactional security or privacy.” ‘181 patent, col. 2:14-20.

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

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

159. Although the systems and methods taught in the ‘181 patent have been adopted by leading businesses today, at the time of invention, the technologies taught in the ‘181 patent claims were innovative and novel. “Typical public key encryption technologies, however, presume that a pair of communications partners seek to communicate directly between each other, without the optional or mandatory participation of a third party, and, in fact, are designed specifically to exclude third party monitoring.” ‘181 patent, col. 2:59-64. Indeed, Oracle has 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).

160. Further, the ‘181 patent claims improve upon the functioning of a computer system by allowing encrypted electronic data to be securely transmitted through an intermediary without the intermediary gaining substantial access to the unencrypted information. This improves the security of the computer system and allows it to be more efficient.⁵⁴ “Third

⁵⁴ 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.”); Elena Ferrari and Bhavani Thuraisingham, *Security and Privacy for Web*

parties, however, may offer valuable services to the participants in a communication, but existing protocols for involvement of more than two parties are either inefficient or insecure.” ‘181 patent, col. 2:64-67. Studies have confirmed that the inventions disclosed in the ‘181 patent improve the security of systems.

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

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

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

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

163. The inventive concepts claimed in the ‘181 patent are technological, not “entrepreneurial.” For example, transcribing protected electronic information between a first (e.g., server) encrypted form and a second (e.g., network) encrypted form without a substantial

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.”).

intermediate representation of the information in decrypted form is a specific, concrete solution to the technological problem of transferring encrypted information via an intermediary without providing the intermediary substantial access to the information.

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

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

Deepak Panth, Dhananjay Mehta and Rituparna Shelgaonkar, *A Survey on Security Mechanisms of Leading Cloud Service Providers*, in INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS 98(1) at 34 (July 2014) (emphasis added).⁵⁵

165. The '181 patent claims are directed toward a solution rooted in computer technology and use technology unique to computers and computer networking to overcome a problem specifically arising in the realm of secure distributed computing. For example, claims of the '181 patent require 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.

166. The '181 patent is directed to specific problems in the field of cryptography. In the “Background” section of the patent, the '181 patent explains that encryption systems use “keys,” similar to passwords, to control how plaintext is encrypted and decrypted. '181 patent,

⁵⁵ 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.”).

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.

167. 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.

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

A key handler, comprising:

an interface to a memory which stores a plurality of encrypted records, each encrypted record having an associated asymmetric encryption key pair and being encrypted with a first component of the associated asymmetric encryption key pair;

at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to transcrypt the encrypted message to a transcrypted message in an integral process substantially without intermediate decryption, using a transcryption key derived at least in part from the at least one asymmetric session key; and

a communication port configured to conduct the negotiation for the at least one asymmetric session key and to communicate the transcrypted record.

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

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

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

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

access a network element indicated in the request. Once verified, the proxy agent completes the connection to the protected network element on behalf of the source of the incoming request; *see also* U.S. Pat. No. 6,023,762 to Dean, disclosing a data access and retrieval system which comprises a plurality of user data sources each storing electronic data signals describing data specific to a user, or enabling services selected by a user; an agent device which is configurable to select individual ones of the user data sources and present selections of user data and service data to a set of callers who may interrogate the agent device remotely over a communications network; and U.S. Pat. No. 6,029,150 to Kravitz, disclosing a system and method of payment in an electronic payment system wherein a plurality of customers have accounts with an agent. Further, the patent lists thirty-three other patented systems involving Computer Network Firewalls that are not, standing alone, preempted by the inventions claimed in the patents-in-suit.

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

172. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁵⁶ the '181 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

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

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

⁵⁶ *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).

175. The '181 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁵⁷

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

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

178. The '181 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.⁵⁸

⁵⁷ *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.’”).

⁵⁸ 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).

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

180. The systems and methods claimed in the '181 patent were not a longstanding or fundamental economic practice at the time of the 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."⁵⁹

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/E5364501/tuxedo/docs12cr2/security/publickey.html> (emphasis added).

181. 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 '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."⁶⁰

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


⁵⁹ 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.").

⁶⁰ 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).

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

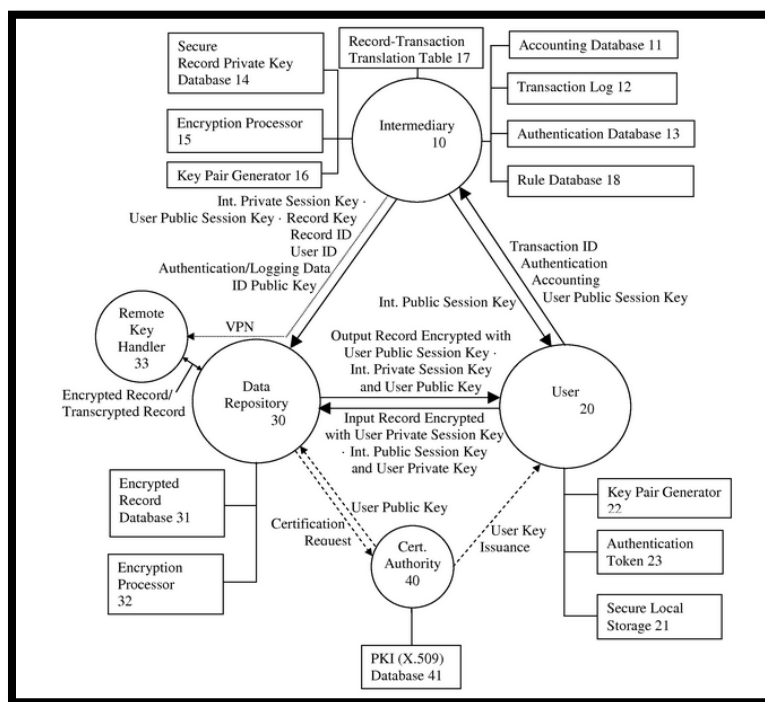
Encryption concepts and terminology

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).

184. One or more claims of the '181 patent require a specific configuration of electronic devices, a network configuration, and the use of encryption systems to secure communications from access by an intermediary. These are meaningful limitations that tie the claimed methods and systems to specific machines. For example, the below diagram from the '181 patent illustrates a specific configuration of hardware disclosed in the patent.



'181 patent, Fig. 1.

C. Information Record Infrastructure Patents

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

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

187. During Mr. Felsher's work in the field of electronic medical records, he witnessed first-hand the drawbacks to existing computer systems and methods for controlling access to protected data. Existing systems failed to efficiently transmit unstructured protected information. '368 patent, col. 3:5-10. Other problems included the inability to secure the protection of data, integrate content management functions, and create a trust infrastructure wherein an independent third party represents and serves as an agent for the content owner. *Id.* at col. 3:4-54:16. The result was an inability to effectively manage access to protective data. The IRI patents disclosed systems and methods that overcome these drawbacks. The inventions disclosed in the IRI patents improved upon the then-available technology, enabled efficient access control of unstructured data, reduced costs, and ultimately resulted in a more secure system.

188. Oracle values systems that provide secure systems and methods for controlling access to protected data such as the system disclosed in the IRI patents and advocates that all businesses to implement such a system as part of its five best practices for protecting regulated data and employee privacy.

Oracle Cloud provides the assurance you need to ensure that your data is safe. Secure data isolation and unified access controls backed by the leader in cloud security mean you can rest easy when your public cloud is Oracle Cloud.

Oracle Cloud: The Next-Generation Public Cloud That Adapts to Your Organization, ORACLE DOCUMENTATION (2015).

189. Oracle's competitors, such as Hewlett-Packard Company and Microsoft Corporation, have confirmed the importance and value of systems and methods that manage access to protected data.

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

HP Information Rights Management Solutions Ensuring Life Cycle Protection Of Digital Information in Microsoft Environments, HP WHITE PAPER (2005).⁶¹

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 UCHHealth, there's ***one fundamental concern that continues to weigh heavily on the minds of providers: Is patient data safe, secure and private in the cloud.***

University of Colorado Health Adopts Microsoft Office 365 for its data privacy and security commitment, MICROSOFT ON THE ISSUES BLOG (December 18, 2013), <http://blogs.microsoft.com/on-the-issues/2013/12/18/university-of-colorado-health-adopts-microsoft-office-365-for-its-data-privacy-and-security-commitment/> (emphasis added).

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

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

Alapan Arnab and Andrew Hutchinson, *Digital Rights Management - An Overview of Current Challenges and Solutions*, in PROCEEDINGS OF INFORMATION SECURITY SOUTH AFRICA CONFERENCE (2004) (emphasis added).⁶²

⁶¹ See also Albert Biketi, *HP Gets Serious About End-To-End Data Protection*, HP SECURITY BLOG (February 19, 2015) (Mr. Biketi, vice president and general manager of data security and encryption at Hewlett-Packard stated "***What our customers need is a data-centric solution that protects sensitive information*** from the moment it's created throughout its entire lifecycle. That means protecting data wherever it moves – from emails to databases and attachments . . . in the cloud, in use, at rest, and in motion.") (emphasis added).

⁶² See also Murat Kantarcioglu, Wei Jiang, and Bradley Malin, *A Privacy-Preserving Framework for Integrating Person-Specific Databases* at 299, PRIVACY IN STATISTICAL 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.").

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

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

Reid Cushman, *Serious Technology Assessment for Health Care Information Technology*, JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION 4(4) (1997).⁶³

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

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

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).⁶⁴

⁶³ 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”).

⁶⁴ *See also* Aaron Franks, Stephen LaRoy, Miek Wood, and Mike Worth. *Idrm: An Analysis Of Digital Rights Management For The Itunes Music Store*, TECHNICAL REPORT, UNIVERSITY OF BRITISH COLUMBIA (2005) (“The need for secure digital rights management (DRM) is more urgent today than ever before. With the rapid increase in broadband availability, Internet file sharing has become a threat to content providers’ bottom line.”); Mike Godwin, *What Every Citizen Should Know About DRM, A.K.A. ‘Digital Rights Management,’* PUBLIC KNOWLEDGE (2004) (“As circumvention tools evolve, and as new technologies pose new infringement

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/> (emphasis added).

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

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

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

196. Background on the state of the art at the time of the inventions disclosed in the IRI patents confirms that the patented inventions are limited to specific computer systems and methods and address issues specific to accessing protected data using modern computer networks.

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

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, Harikrisha 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.").

The IRI patents address problems specific to and arising from distribution and protected works on the internet.

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

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

Tom Simonite, *Microsoft Thinks DRM Can Solve the Privacy Problem*, MIT TECHNOLOGY REVIEW, October 10, 2013 (emphasis added) (Craig Mundie is Senior Advisor to the CEO at Microsoft and its former Chief Research and Strategy Officer).⁶⁵

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

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

201. *Electronic Medical Records*. The IRI patents disclose systems and methods for controlling access to protected health information where the information is stored in one or more external databases. Systems for controlling access to medical records, contemporaneous to the

⁶⁵ 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.").

IRI patents had significant limitations that the IRI patents address.⁶⁶ These systems included: (1) Anonymizing Records. A method used in contemporaneous systems to the IRI patents is the maintenance of anonymous medical records. However, such techniques did not provide patients and medical professionals the ability to access patient specific records. (2) Indexing. Systems contemporaneous to the IRI patents indexed medical records with anonymous identification codes.⁶⁷ 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.

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

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

⁶⁶ 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. Furthermore, data is no longer only in structured databases. . . . Security for such data has not received much attention.”).

⁶⁷ 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”).

Epic System Corporation's CareWeb⁶⁸ had significant limitations including: inability to effectively control access on a record-by-record basis within respective external databases, as claimed in several IRI patents; inability to distinguish between records within an external or backend database, the databases accessed through CareWeb were basically opaque to the "CareWeb" system; and CareWeb's fixed structure was expressly limited to a particular, monolithic front-end architecture for secure implementation.

204. At the time the inventions disclosed in the IRI patents were conceived, the medical community showed little sign of implementing a system for controlling access to medical records that were stored in 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).

205. 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*, MICROSOFT HEALTH TECHNOLOGY BLOG (December 2013),

⁶⁸ 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.).

<http://www.microsoft.com/en-us/health/blogs/data-privacy-and-compliance-in-the-cloud-is-essential-for-the-healthcare-industry/default.aspx>.

206. 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”).⁶⁹ 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.⁷⁰ In addition, various universities studied and implemented systems for securely managing access to distributed medical records.⁷¹

207. 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. 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.

⁶⁹ Gov. Rick Perry, *State-of-the-State Speech* (February 6, 2007), available at: <http://governor.state.tx.us/news/speech/5567/>.

⁷⁰ 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.).

⁷¹ 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).

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

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

209. 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

210. 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.

211. 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.

212. 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.

213. 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.

214. 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.

215. 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.

216. 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.

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

218. 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.

219. 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.

220. 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.

221. 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.⁷²
- 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.

⁷² 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)”).

- 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).⁷³

222. Although “[e]ncryption, in general, represents a basic building block of human ingenuity that has been used for hundreds, if not thousands, of years,”⁷⁴ the ‘368 patent does not claim, or attempt to preempt, “some process that involves the encryption of data for some purpose” (or similar abstraction).

223. 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.

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

⁷³ 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.”).

⁷⁴ *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).

225. The '368 patent claims systems and methods that “could not conceivably be performed in the human mind or pencil and paper.”⁷⁵

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

227. 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.

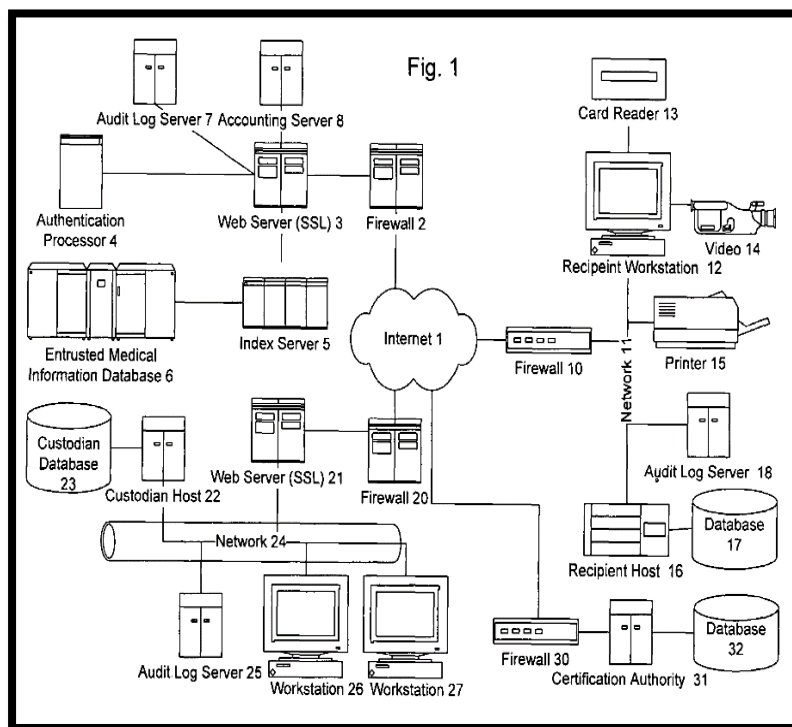
228. The claimed invention in the '368 claims is rooted in computer technology and overcomes problems specifically arising in the realm of computer networks.

229. The systems and methods claimed in the '368 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.

230. 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.

231. 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.

⁷⁵ *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.’”).



'368 patent, Fig. 1.

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

232. 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 F. 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.

233. 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

234. 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.

235. 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.

236. 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.

237. 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.

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

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

240. 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.

241. 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.

242. 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.

243. 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.

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

245. 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.

246. 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.

247. 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.

248. 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).

249. 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.

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

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

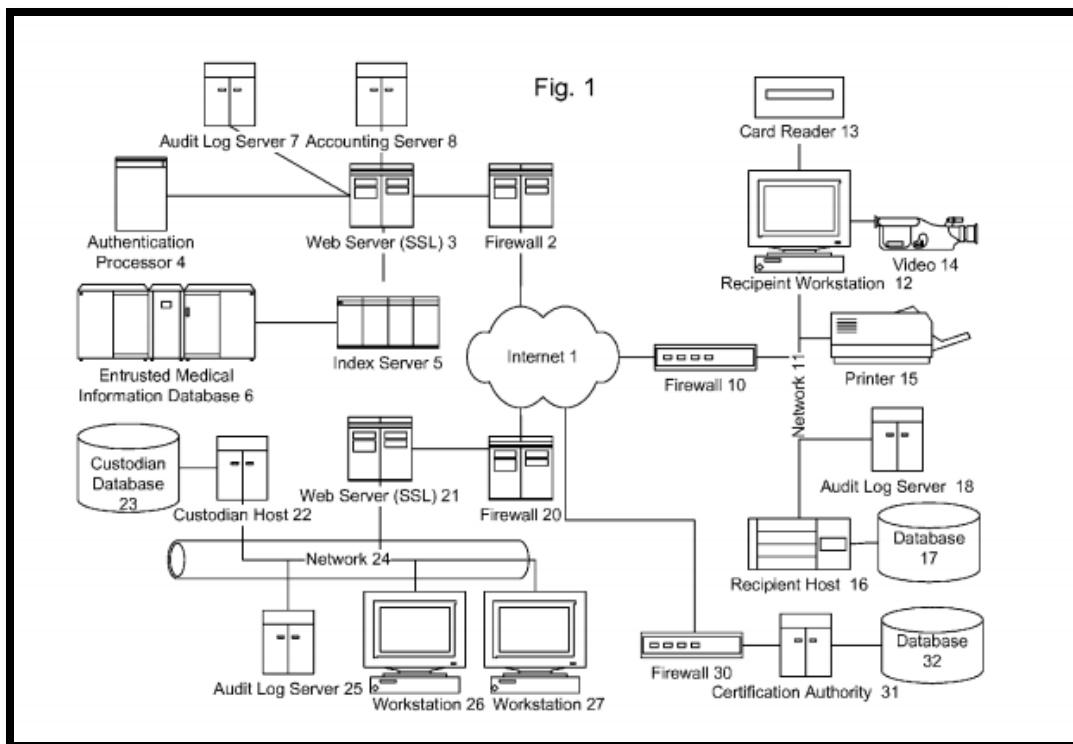
252. The '630 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

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

254. The systems and methods claimed in the '630 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.

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

256. 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.

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

257. 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 G. 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.

258. The '895 patent has been cited by four United States patents and patent applications as relevant prior art.⁷⁶ Specifically, patents issued to the following companies have cited the '895 patent as relevant prior art.

- J.D. Power and Associates

⁷⁶ 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 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.

- Fujitsu Limited
- Extendabrain Corporation

259. 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.

260. 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.

261. 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.

262. 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.

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

264. 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).

265. 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.

266. 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.

267. 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.

268. 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.

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

270. 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.

271. 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.

272. 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.

273. 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).

274. 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.

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

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

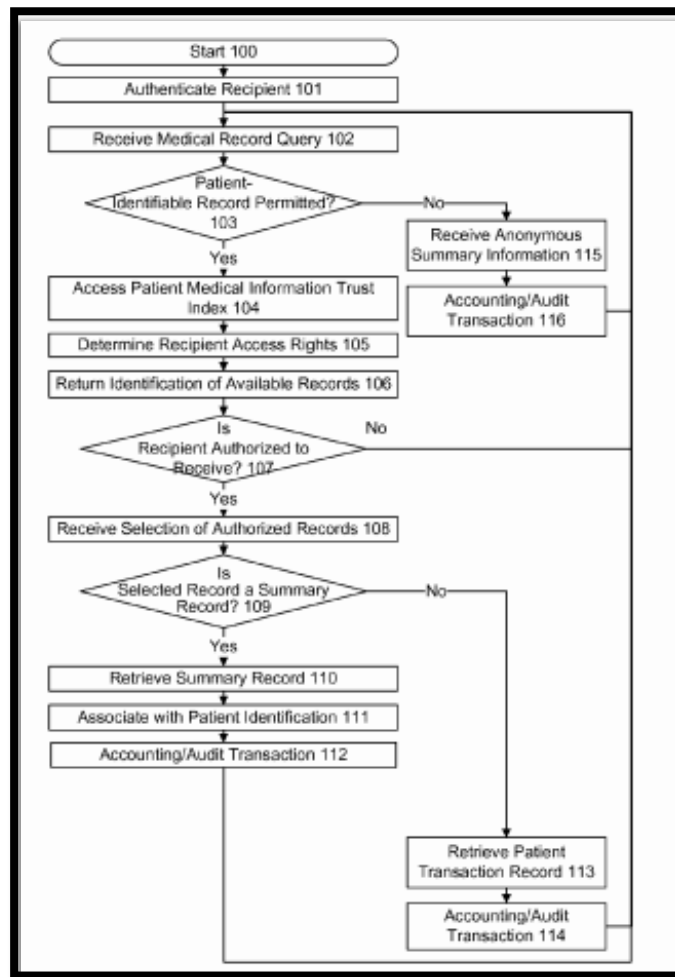
277. The '895 patent claims systems and methods not merely for transferring secure information over a computer network, but for making the computer network itself more secure.

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

279. The systems and methods claimed in the '895 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.

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

281. 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

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

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

284. Oracle designs, makes, sells, offers to sell, imports, and/or uses Oracle Database 12c (“Oracle DB 12c”).

285. Oracle designs, makes, sells, offers to sell, imports, and/or uses Oracle Advanced Security for Oracle DB 12c (“Oracle AS”).⁷⁷

286. Oracle designs, makes, sells, offers to sell, imports, and/or uses Oracle Key Vault (“Oracle KV”).⁷⁸

287. Oracle designs, makes, sells, offers to sell, imports, and/or uses the Oracle DB 12c, Oracle AS, and Oracle KV (collectively, the “Oracle Encryption System” or “Oracle ‘237 Products”).

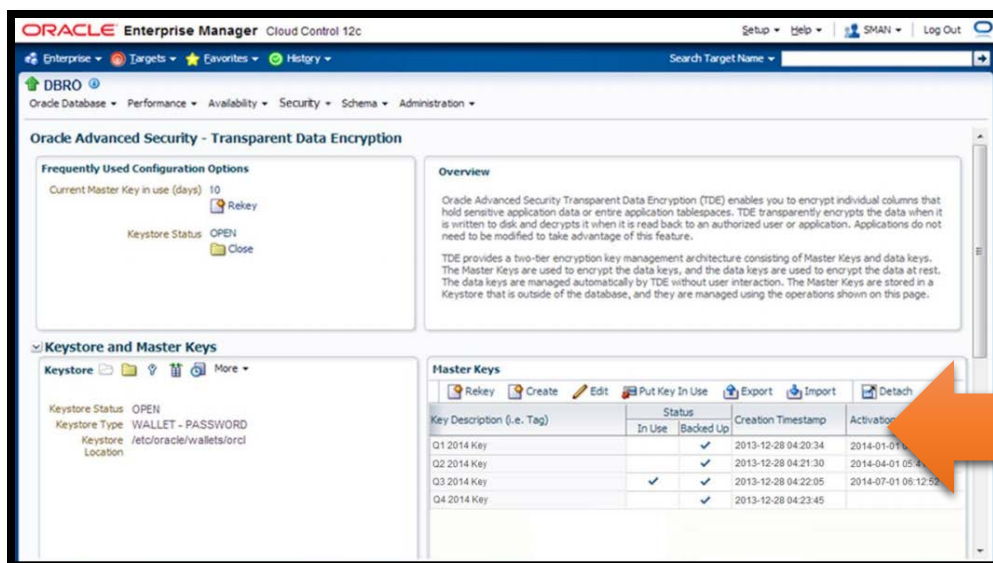
288. On information and belief, one or more Oracle subsidiaries and/or affiliates use the Oracle Encryption System in regular business operations.

289. On information and belief, one or more of the Oracle ‘237 Products include encryption technology.

290. On information and belief, the Oracle ‘237 Products include an interface for managing the master keys that are used to encrypt the data keys (the data keys are used to encrypt data that is at rest). The below screenshot shows an Oracle DB 12 interface for managing master keys.

⁷⁷ See *Oracle Database Advanced Security Data Sheet*, ORACLE DOCUMENTATION (2013), available at: <http://www.oracle.com/technetwork/database/options/advanced-security/advanced-security-ds-12c-1898873.pdf>; see also *Oracle Database Advanced Security Guide 12g Release*, ORACLE DOCUMENTATION (December 2014).

⁷⁸ See *Oracle Key Vault Data Sheet*, ORACLE DOCUMENTATION (2014), available at: <http://www.oracle.com/technetwork/database/options/key-management/overview/ds-security-key-vault-2256707.pdf>.



Todd Bottger, *Oracle Advanced Security Best Practices for Database Encryption and Redaction*, ORACLE OPEN WORLD PRESENTATION at 13 (October 1, 2014) (orange arrow indicating an interface for managing the master keys).

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

292. On information and belief, the Oracle ‘237 Products are available to businesses and individuals throughout the United States.

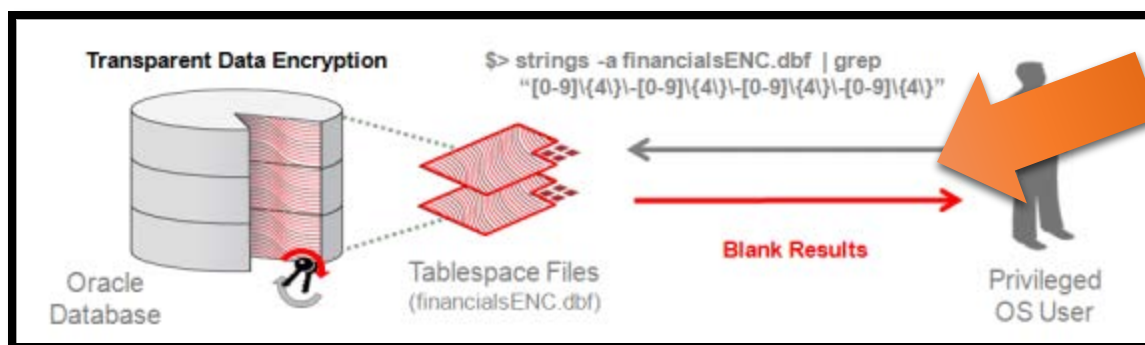
293. On information and belief, the Oracle ‘237 Products are provided to businesses and individuals located in the Eastern District of Texas.

294. On information and belief, the Oracle ‘237 Products are a secure distributed information access control system. For example, Oracle AS is described in Oracle documentation as “an out-of-the-box, two-tier key management architecture consisting of data encryption keys and a master encryption key. The data encryption keys are managed automatically and are encrypted by the master encryption key. The master encryption key is stored and managed outside of the database within an Oracle Wallet.”⁷⁹

⁷⁹ *Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security*, ORACLE WHITE PAPER at 4 (June 2013).

295. On information and belief, the Oracle '237 Products comprise a communication interface device and are configured to communicate with a plurality of independently operating servers. For example, on information and belief, the Oracle Encryption System comprises a communication interface to, and is configured to; communicate with a plurality of independently operating servers used for "cloud storage." For example, includes the Oracle Encryption System includes a key server, such as Oracle KV, that comprises a communication interface configured to communicate with a plurality of independently operating servers (e.g., authenticated cloud consumer virtual machine environments), each communicating server encrypted information, wherein the server encrypted information is in an encrypted form negotiated between a respective server (e.g., respective cloud consumer virtual machine environment) and an intermediary (e.g., the Oracle AS automated key handler).

296. Oracle documentation establishes that the Oracle Encryption System encrypts data and protects data as it moves into and out of a database such as Oracle DB 12c.



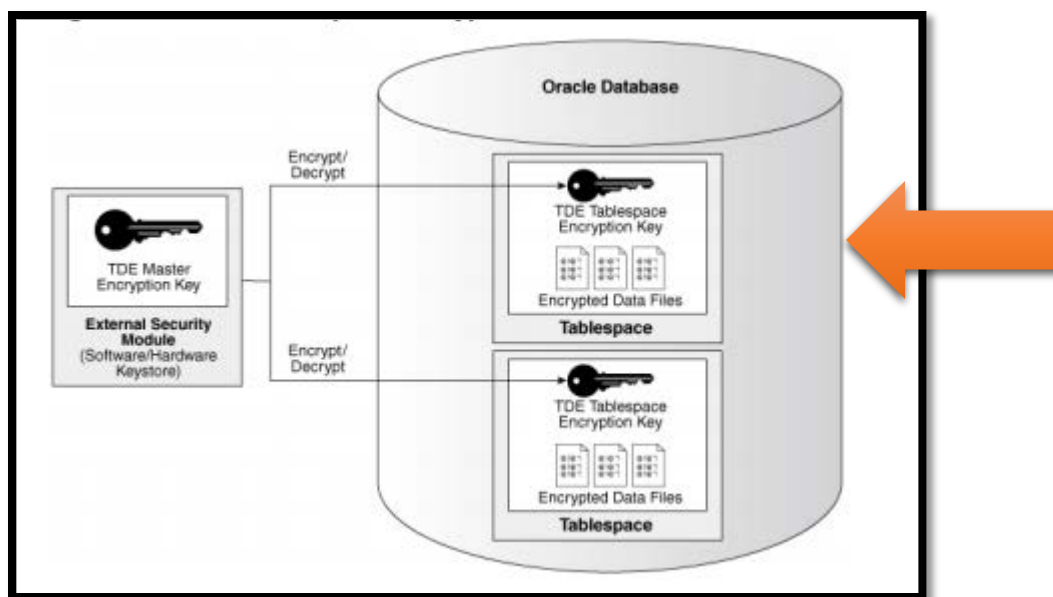
Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security, ORACLE WHITE PAPER at 3 (June 2013) (orange arrow indicating that the encryption is designed to prevent database bypass).

297. On information and belief, Oracle AS provides a two-tiered encryption key management structure that includes master encryption keys and data encryption keys. The master encryption keys are stored out of the database where the encrypted record is stored. For example, master encryption keys can be stored in Oracle KV.

298. On information and belief, the Oracle Encryption System includes an automated processor configured to communicate with a network using network encrypted information,

wherein the network encrypted information is in a form negotiated between a network endpoint and the intermediary, wherein for respective information, the automated processor transcrypts between the server encrypted information and the network encrypted information, substantially without an intermediate representation of the information in a decrypted form. For example, the Oracle AS automated key handler includes an automated processor configured to communicate with a network (e.g., a VPN and/or the Internet) using network encrypted information, wherein the network encrypted information is in a form negotiated between a network endpoint (e.g., an authenticated cloud consumer virtual machine environment) and the intermediary (e.g., the Oracle AS automated key handler).

299. On information and belief, Oracle AS tablespace encryption uses the two-tiered, key based architecture to transparently encrypt and decrypt tablespaces. The master encryption key is stored in an external security module (e.g., Oracle KV) as shown in the below excerpt from Oracle's documentation of Oracle AS.



Oracle Database Advanced Security Guide 12.1, ORACLE DOCUMENTATION at § 2-5 (May 2015) (arrow identifying that the Oracle AS encryption uses the two-tiered, key-based architecture to transparently encrypt (and decrypt) tablespaces).

300. On information and belief, the Oracle '237 Products include an automated processor that transcrypts between the server encrypted information and the network encrypted

information. This transcription is substantially without an intermediate representation of the information in a decrypted form.

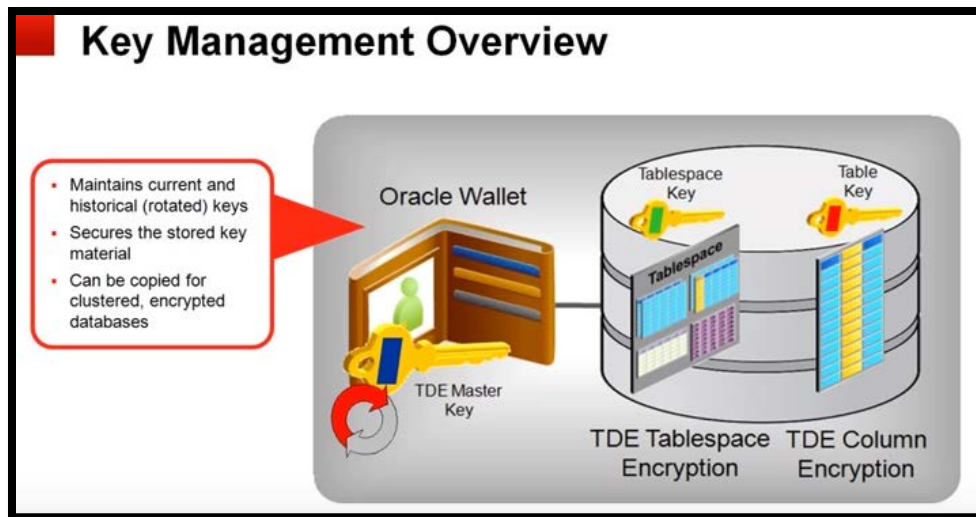
301. On information and belief, the Oracle '237 Products enable encryption of an entire tablespace. "It automatically encrypts data when it is written to disk, and then automatically decrypts the data when your applications access it."⁸⁰

302. On information and belief, the Oracle '237 Products include an audit database configured to log usage of at least one of the plurality of independently operating servers and the activity of the intermediary. For example, the Oracle Encryption System quickly detects devices, enforces encryption, and audits encryption and data use.

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

304. On information and belief, the Oracle '237 Products support encryption algorithms including AES 128, AES 192, AES 256, and DES 168.

305. On information and belief, one implementation of Oracle AS utilizing Transparent Data Encryption is illustrated below:



Todd Bottger, *Oracle Advanced Security Transparent Data Encryption Product Demonstration*, ORACLE LEARNING LIBRARY (February 16, 2014), available at:

⁸⁰ *Oracle Database Advanced Security Guide 12.1*, ORACLE DOCUMENTATION at § 1-1 (May 2015)

<https://www.youtube.com/watch?v=1OGwOeQ6png> (the above image is excerpted from a presentation by Mr. Bottger, a Sr. Principal Product Manager at Oracle).

306. On information and belief, the Oracle ‘237 Products comprise a communications interface configured to communicate with, a plurality of independently operating servers—e.g., a plurality of independently operating servers used for “cloud storage.”

307. On information and belief, Oracle’s documentation states that the Oracle ‘237 Products by “keeping the master key separate from the encrypted data mitigates attacks because both the keys and the encrypted data must be separately compromised to gain access to clear data.”⁸¹

308. On information and belief, the server encrypted storage objects are in an encrypted form negotiated between a respective storage server and an intermediary (e.g., the Oracle server-side encryption resource).

309. On information and belief, Oracle has directly infringed and continues to directly infringe the ‘237 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to the Oracle ‘237 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, the Oracle DB 12, Oracle AS, and Oracle KV.

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

311. On information and belief, Oracle also indirectly infringes the ‘237 patent by actively inducing infringement under 35 USC § 271(b).

⁸¹ *Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security*, ORACLE WHITE PAPER at 4 (June 2013).

312. On information and belief, Oracle had knowledge of the ‘237 patent since at least 2013. Oracle cited the ‘237 patent in U.S. Patent Application No. 13/529,454, which was filed on June 21, 2012.

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

314. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle ‘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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the ‘237 patent. Oracle 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, Oracle provides the Oracle ‘237 Products that have the capability of operating in a manner that infringe one or more of the claims of the ‘237 patent, including at least claim 18, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle ‘237 Products to utilize the products in a manner that directly infringe one or more claims of the ‘237 patent. By providing instruction and training to customers and end-users on how to use the Oracle ‘237 Products in a manner that directly infringes one or more claims of the ‘237 patent, including at least claim 18, Oracle specifically intended to induce infringement of the ‘237 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle ‘237 Products, e.g., through Oracle’s user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the ‘237 patent.⁸² Accordingly, Oracle has induced and continues to induce users of

⁸² See e.g., *Oracle Database Advanced Security Data Sheet*, ORACLE DOCUMENTATION (2013); *Oracle Database Advanced Security Guide 12g Release*, ORACLE DOCUMENTATION (December 2014); *Oracle Key Vault Data Sheet*, ORACLE DOCUMENTATION (2014); Todd Bottger, *Oracle Advanced Security Best Practices for Database Encryption and Redaction*, ORACLE OPEN

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.

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

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

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

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

318. Oracle designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for communication of encrypted information.

319. Oracle designs, makes, uses, sells, and/or offers for sale in the United States Oracle Documents Cloud Service ("Document Cloud").

320. Oracle designs, makes, uses, sells, and/or offers for sale in the United States Oracle WebCenter 11gR1 PS8 (11.1.1.9.0), Oracle WebCenter 11gR1 PS7 (11.1.1.8.0), Oracle WebCenter 11gR1 PS6 (11.1.1.7.0), Oracle WebCenter 11gR1 PS5 (11.1.1.6.0) (collectively, "WebCenter").

321. On information and belief, Document Cloud and WebCenter (collectively, the "Oracle '017 Products") enable securing and tracking of digital information.

WORLD PRESENTATION (October 1, 2014); *Encryption and Redaction in Oracle Database 12c with Oracle Advanced Security*, ORACLE WHITE PAPER (June 2013); *Oracle Database Advanced Security Guide 12.1*, ORACLE DOCUMENTATION (May 2015); Todd Bottger, *Oracle Advanced Security Transparent Data Encryption Product Demonstration*, ORACLE LEARNING LIBRARY (February 16, 2014).

322. On information and belief, Oracle has stated in its documentation that one or more of the Oracle '017 Products use encryption to extend the management of information beyond a data repository "to every copy of an organization's most sensitive information, everywhere it is stored and used - on end user desktops, laptops and in other repositories, inside and outside the firewall."⁸³

323. Oracle designs, makes, uses, sells, and/or offers for sale products and services such as the Oracle '017 Products, that infringe the '017 patent.

324. On information and belief, the Oracle '017 Products include encryption technology.

325. On information and belief, the Oracle '017 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

326. On information and belief, the Oracle '017 Products are available to businesses and individuals throughout the United States.

327. On information and belief, the Oracle '017 Products are available to businesses and individuals located in the Eastern District of Texas.

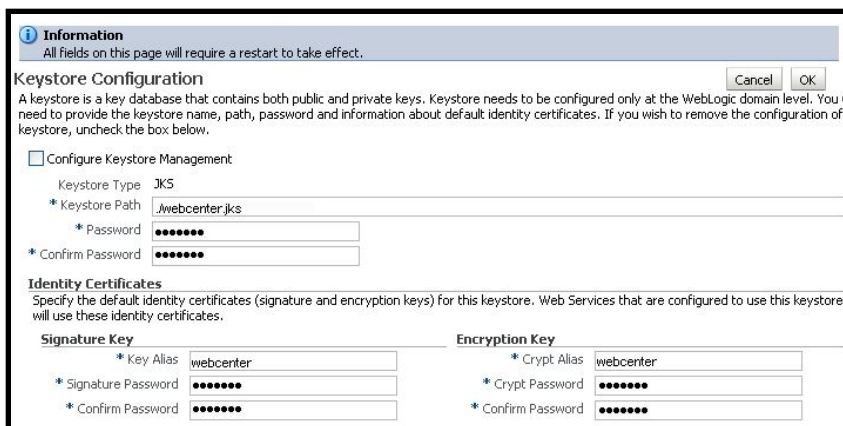
328. On information and belief, the Oracle '017 Products receive information to be processed (e.g., communications that should be encrypted and transmitted to the intended recipient).

329. On information and belief, the Oracle '017 Products enable the utilization of public-private, asymmetric key pairs (e.g., RSA key pairs).

330. On information and belief, the Oracle '017 Products enable encryption of a message using a symmetric key wrap including: AES 256, AES 192, and AES 128 symmetric key wraps.

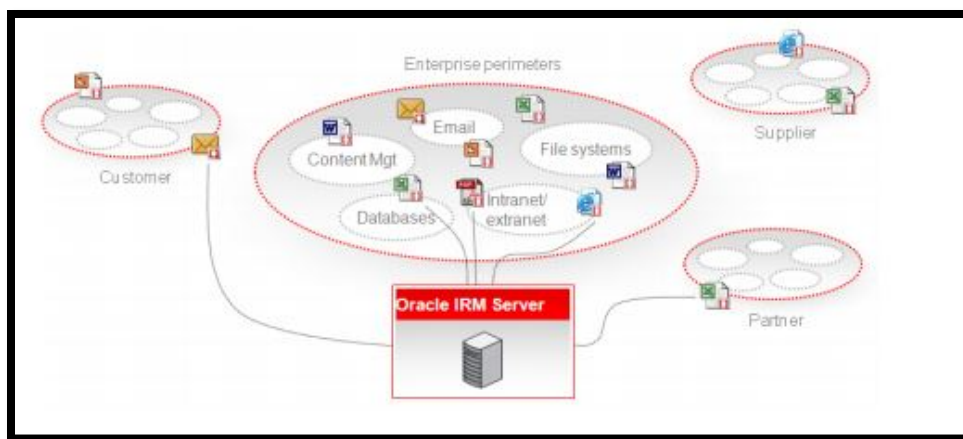
⁸³ *Oracle Information Rights Management*, ORACLE WEBCENTER WEBPAGE, available at: <http://www.oracle.com/technetwork/middleware/webcenter/content/index-094034.html>.

331. On information and belief, the Oracle '017 Products enable asymmetric key wraps including: RSA 256, RSA 192, and RSA 128 asymmetric key wraps.



Fusion Middleware Administrator's Guide for Oracle WebCenter, ORACLE DOCUMENTATION HELP CENTER (2013) (showing the configuration screen for the WebCenter key store).

332. Oracle documentation shows a high-level view of the architecture of Oracle's WebCenter system that "[e]ncrypting the information so that no matter how many copies are made, or where they are stored, they are useless without the relevant decryption keys."



Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used, ORACLE WHITE PAPER at 5 (March 2010).

333. On information and belief, the Oracle '017 Products documentation represents that the Oracle '017 Products enable the secure transmission and receipt of messages using server-side security controls, strong encryption, and digital signatures.

Classification-Based Rights Management

A significant challenge created by protecting individual documents, emails, and so on is that this can very easily lead to an unmanageable number of policies and tie business workflows into knots. Potentially, each business user and application could define unique rules for each document, creating great inconsistency and an overwhelming administrative burden. From a governance and compliance standpoint, it can rapidly become difficult to ensure or demonstrate that information really is being protected as required.

Oracle IRM addresses this challenge with a unique classification-based rights model that enables a very large number of documents to be protected by a very small, manageable number of policies. Each policy has clearly defined business ownership and, in most deployments, the solution guards against the creation of ad hoc policy at the whim of individual business users. Indeed, the management of IRM policies may simply be a facet of a broader security infrastructure that manages roles and rights for a range of business data and applications.

Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used, ORACLE WHITE PAPER at 7 (March 2010) (the yellow added highlights the email encryption functionality).

334. On information and belief, the documentation for the Oracle '017 Products represents that Oracle WebCenter and Document Cloud enables the exchange of private data without exposing it to “[u]nauthorized users.”

Oracle IRM distributes rights management between centralized servers and desktop agents. Authors continue to create documents and emails in their existing document and email applications.

Oracle IRM enables documents or emails to be automatically or manually sealed at any stage in their lifecycle, using sealing tools integrated into the Windows desktop, authoring applications, email clients, and content management and collaborative repositories. Sealing wraps documents and emails within a layer of strong encryption and digital signatures, together with indelible links back to network-hosted servers (operated by the organization to which the information belongs) that store the decryption keys and associated access rights.

Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server, Oracle Documentation at § 1-1 (January 2011).

335. On information and belief, the Oracle '017 Products define a cryptographic comprehension function (e.g., session-specific cryptographic key and/or other cryptographic

comprehension information) for the information, adapted for making at least a portion of the information incomprehensible.

336. On information and belief, in an initial provisioning/registration process, Oracle creates an asymmetric key pair for an authenticated user of the Oracle '017 Products. The below table shows the available cryptographic modes for the Oracle WebCenter product.

Oracle IRM Cryptographic modes					
Mode	FIPS 140-2	Content Encryption	Content Signing	Key Encryption	Client Module
AES128		AES 128	HMAC-SHA256 w/ 128-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES256		AES 256	HMAC-SHA256 w/ 256-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES128-FIPS	✓	AES 128	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
AES256-FIPS	✓	AES 256	HMAC-SHA256 w/ 256-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
DES3-FIPS	✓	Triple-DES 168	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API

Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used, ORACLE WHITE PAPER at 13 (March 2010).

337. On information and belief, the Oracle '017 Products receive asymmetric key information (e.g., a public/private key pair), comprising at least asymmetric encryption key information (e.g., private key encryption information) and asymmetric decryption key information (e.g., public key decryption information).

338. On information and belief, the Oracle '017 Products use a cryptographic intermediary (e.g., a key handling/cryptographic intermediary) to negotiate a new cryptographic comprehension function (e.g., new session-specific cryptographic key, initial conditions, and/or other cryptographic comprehension information).

339. On information and belief, the Oracle '017 Products process the information to invert the cryptographic comprehension function (e.g., the initial session-specific cryptographic key, initial conditions, and/or other cryptographic comprehension information) and impose the new cryptographic comprehension function (e.g., the new session-specific cryptographic key, initial conditions, and/or other cryptographic comprehension information) in an integral process, in dependence on at least the asymmetric cryptographic key information (e.g., in an integral wrapping and/or envelope encryption process, in dependence on at least RSA 512, RSA 1024, and RSA 2048, or other types of asymmetric key information), without providing the intermediary (e.g., the Oracle key-handling intermediary) with sufficient asymmetric key information to decrypt the processed information.

340. On information and belief, the oracle '017 Products output the processed information.

341. On information and belief, the ability of the asymmetric decryption key information (e.g., the asymmetric Oracle decryption key information) to decrypt the processed information (e.g., the message information) changes dynamically (e.g., as session and/or wrap cryptographic comprehension function information is [re-] negotiated between the intermediary and the Oracle WebCenter client).

342. On information and belief, Oracle has directly infringed and continues to directly infringe the '017 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, the Oracle '017 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, Document Cloud and WebCenter.

343. By making, using, testing, offering for sale, and/or selling the Oracle '017 Products, Oracle has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '017 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

344. On information and belief, Oracle also indirectly infringes the '017 patent by actively inducing infringement under 35 USC § 271(b).

345. On information and belief, Oracle had knowledge of the '017 patent since at least 2007. Oracle cited the '017 patent in U.S. Patent No. 8,064,604, which was filed on January 9, 2007, and issued on November 22, 2011. Oracle also cited the '017 patent in U.S. Patent No. 8,463,624, which was filed on September 23, 2003, and issued on June 11, 2013.

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

347. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '017 patent. Oracle 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, Oracle provides the Oracle '017 Products, which have the capability of operating in a manner that infringe one or more of the claims of the '017 patent, including at least claim 1, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '017 Products to utilize the products in a manner that directly infringe one or more claims of the '017 patent, including at least claim 1. By providing instruction and training to customers and end-users on how to use the Oracle '017 Products in a manner that directly infringes one or more claims of the '017 patent, including at least claim 1, Oracle specifically intended to induce infringement of the '017 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '017 Products through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '017 patent.⁸⁴ Accordingly, Oracle has induced and

⁸⁴ See e.g., *Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used*, ORACLE WHITE PAPER (March 2010); *Oracle Fusion Middleware*

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.

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

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

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

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

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

352. Oracle designs, makes, uses, sells, and/or offers for sale in the United States Oracle Documents Cloud Service ("Document Cloud").

353. Oracle designs, makes, uses, sells, and/or offers for sale in the United States Oracle WebCenter 11gR1 PS8 (11.1.1.9.0), Oracle WebCenter 11gR1 PS7 (11.1.1.8.0), Oracle WebCenter 11gR1 PS6 (11.1.1.7.0), Oracle WebCenter 11gR1 PS5 (11.1.1.6.0) (collectively "WebCenter").

354. On information and belief, Document Cloud and WebCenter (collectively, the "Oracle '591 Products") enable securing and tracking of digital information.

Administrator's Guide for Oracle IRM Server, ORACLE DOCUMENTATION (January 2011); *Oracle Information Rights Management*, ORACLE WEBCENTER WEBPAGE, available at: <http://www.oracle.com/technetwork/middleware/webcenter/content/index-094034.html>.

355. On information and belief, the Oracle '591 Products include encryption technology.

356. On information and belief, the Oracle '591 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

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

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

359. On information and belief, the Oracle '591 Products enable the utilization of public-private, asymmetric key pairs (e.g., RSA key pairs).

360. On information and belief, the Oracle '591 Products documentation represents that the Oracle '591 Products enable the secure transmission and receipt of messages using server-side security controls, strong encryption, and digital signatures.

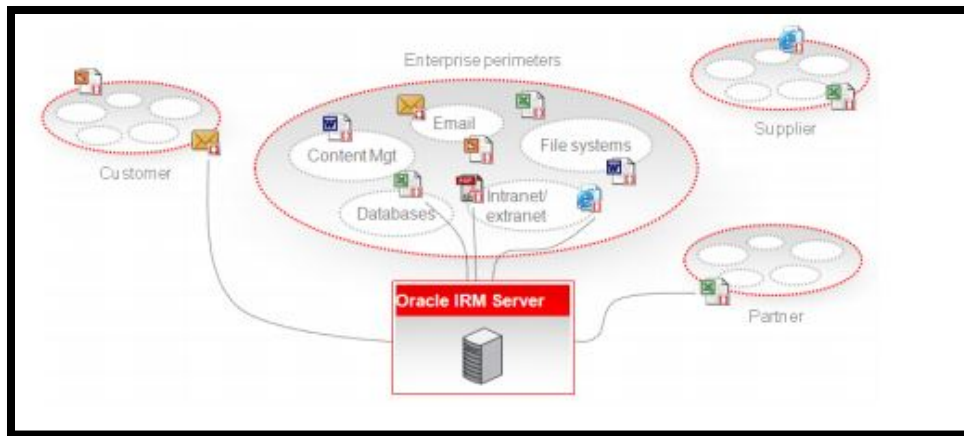
Oracle IRM distributes rights management between centralized servers and desktop agents. Authors continue to create documents and emails in their existing document and email applications.

Oracle IRM enables documents or emails to be automatically or manually sealed at any stage in their lifecycle, using sealing tools integrated into the Windows desktop, authoring applications, email clients, and content management and collaborative repositories. Sealing wraps documents and emails within a layer of strong encryption and digital signatures, together with indelible links back to network-hosted servers (operated by the organization to which the information belongs) that store the decryption keys and associated access rights.

Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server, ORACLE DOCUMENTATION AT § 1-1 (JANUARY 2011).

361. On information and belief, the documentation for the Oracle '591 Products represents that the Document Cloud and WebCenter products enable the exchange of private data without exposing it to hackers or anyone other than the intended recipient.

362. Oracle documentation shows a high-level view of the architecture of Oracle's WebCenter system that "[e]ncrypting the information so that no matter how many copies are made, or where they are stored, they are useless without the relevant decryption keys."



Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used, ORACLE WHITE PAPER at 5 (March 2010).

363. On information and belief, the Oracle '591 Products receive and store in a first memory information encrypted based on a first set of cryptographic keys (e.g., a first set of 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.

364. On information and belief, the oracle '591 Products receive and store in a second memory (e.g., privileged memory dedicated to cryptographic key storage and/or manipulation) a first portion (e.g., a public key portion) of a second set of cryptographic keys (e.g., a second set of asymmetric keys), having a corresponding second portion (e.g., a private key portion) being required for decryption of a message encrypted using the first portion of the second set of cryptographic keys (e.g., the public key portion of the second set of asymmetric keys).

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

366. On information and belief, the Oracle '591 Products, without requiring or employing sufficient information either to decrypt the encrypted information or to comprehend the transcribed information, generate a transcription key for transforming the received encrypted information to transcribed information.

367. On information and belief, the Oracle '591 Products generate 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 (e.g., information representing the public key portion of the first set of asymmetric cryptographic keys), information representing the first portion of the second set of cryptographic keys (e.g., information representing the public key portion of the second set of asymmetric cryptographic keys), and a first portion of the set of session keys (e.g., a first portion of the set of RSA and/or AES session keys).

368. On information and belief, Oracle creates an asymmetric key pair for an authenticated user of the Oracle '591 Products. The below table shows the available cryptographic modes for the Oracle WebCenter product.

Oracle IRM Cryptographic modes					
Mode	FIPS 140-2	Content Encryption	Content Signing	Key Encryption	Client Module
AES128		AES 128	HMAC-SHA256 w/ 128-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES256		AES 256	HMAC-SHA256 w/ 256-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES128-FIPS	✓	AES 128	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
AES256-FIPS	✓	AES 256	HMAC-SHA256 w/ 256-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
DES3-FIPS	✓	Triple-DES 168	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API

Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used, ORACLE WHITE PAPER at 13 (March 2010).

369. On information and belief, Oracle has directly infringed and continues to directly infringe the ‘591 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to the Oracle ‘591 Products.

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

371. On information and belief, Oracle also indirectly infringes the ‘591 patent by actively inducing infringement under 35 USC § 271(b).

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

373. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '591 patent. Oracle 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, Oracle provides the Oracle '591 Products that have the capability of operating in a manner that infringe one or more of the claims of the '591 patent, including at least claim 13, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '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 Oracle '591 Products in a manner that directly infringes one or more claims of the '591 patent, including at least claim 13, Oracle specifically intended to induce infringement of the '591 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '591 Products, e.g., through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '591 patent.⁸⁵ Accordingly, Oracle 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.

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

⁸⁵ See e.g., *Oracle Information Rights Management 11g – Managing Information Everywhere It Is Stored and Used*, ORACLE WHITE PAPER (March 2010); *Oracle Fusion Middleware Administrator's Guide for Oracle IRM Server*, ORACLE DOCUMENTATION (January 2011); *Oracle Information Rights Management*, ORACLE WEBCENTER WEBPAGE, available at: <http://www.oracle.com/technetwork/middleware/webcenter/content/index-094034.html>.

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

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

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

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

378. Oracle designs, makes, sells, offers to sell, imports, and/or uses Oracle Key Vault ("Oracle Key Vault").

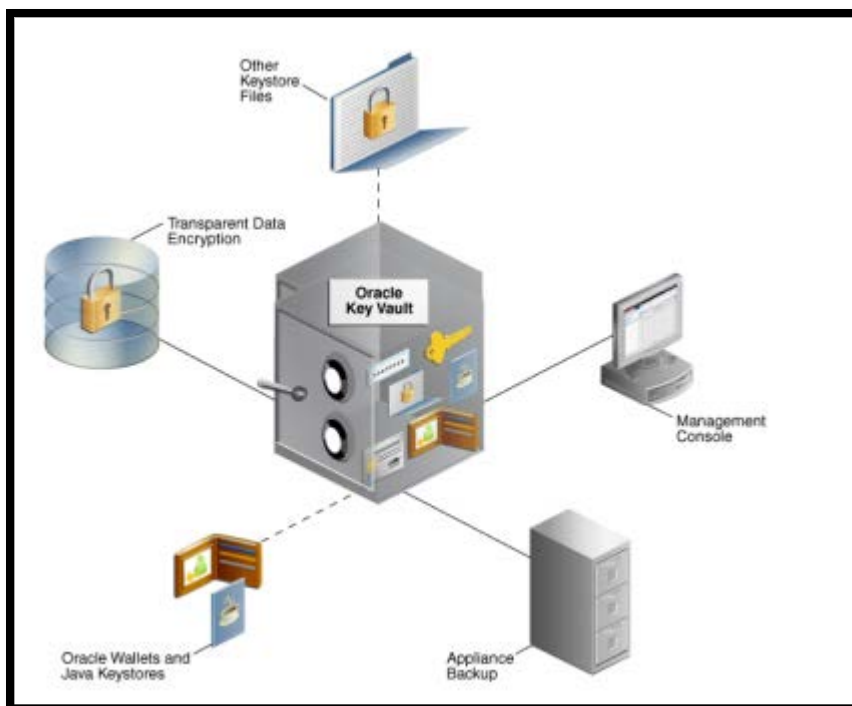
379. Oracle designs, makes, sells, offers to sell, imports, and/or uses Oracle Wallet Centralized Encryption Key Management ("Oracle Wallet").

380. On information and belief, the Oracle Key Vault and/or the Oracle Wallet (collectively, the "Oracle KV System" or "Oracle '181 Products"), comprise a key handler.

381. On information and belief, the Oracle KV System includes logic and hardware for securely handling cryptographic keys in the cloud.

382. On information and belief, the Oracle KV system 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 Oracle KV system comprises an interface to a memory (e.g., an encrypted data store on an Oracle KV keystore server) that stores a plurality of encrypted cryptographic key records.

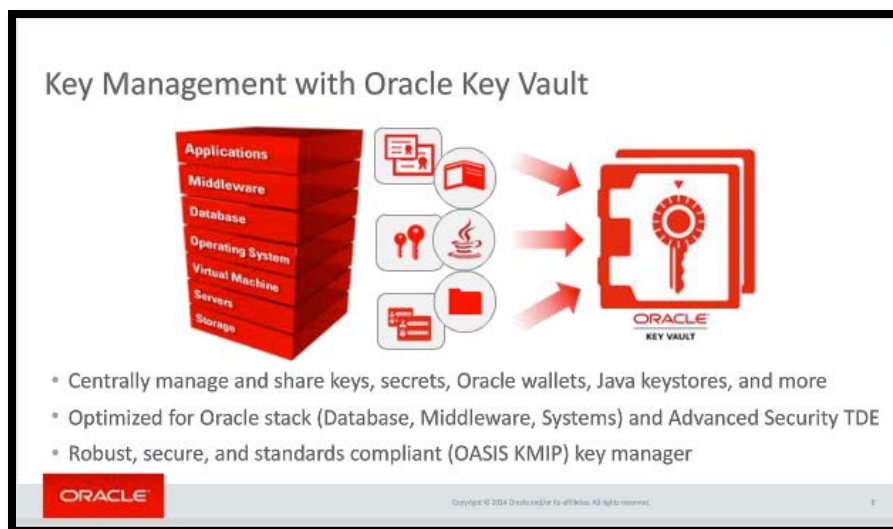
383. The below diagram from Oracle's documentation illustrates the Oracle Key Vault environment.



Oracle Key Vault Administrators Guide 12c Release 1, ORACLE DOCUMENTATION at § 1-2 (June 2015) (Oracle Key Vault, in the center, stores and manages the security objects and backup devices. It works with components including: (1) Transparent Data Encryption refers to Oracle databases that have tables and tablespaces configured to use TDE. (2) Other Keystore Files can be JCEKS keystores that you upload to Oracle Key Vault from endpoints or download from Key Vault to endpoints.).

384. On information and belief, upon information and belief, 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, Oracle KV 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 Oracle KV 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). The below diagram is

excerpted from Oracle's documentation and shows at a high level key management with Oracle KV.

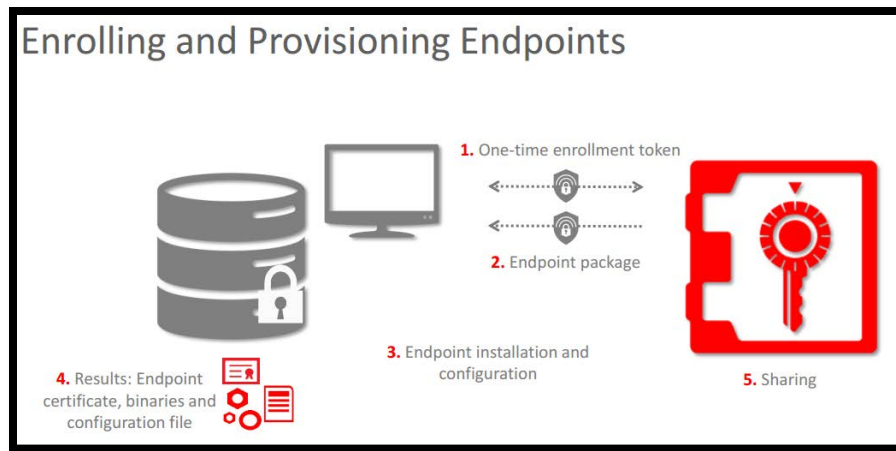


Saikat Saha, *Introducing Oracle Key Vault: Centralizing Keys, Wallets, and Java Keystores*, ORACLE OPEN WORLD PRESENTATION at 8 (September 29, 2014) (Mr. Saha is a Sr. Principal Product Manager for Oracle Database Security).

385. On information and belief, the Oracle KV System comprises at least one automated processor operating in a privileged processing environment, configured to receive a selected encrypted record from the memory through the interface, to negotiate at least one asymmetric session key, and to 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. For example, the Oracle KV system 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 Oracle KV system includes at least one privileged-mode automated processor in the Oracle KV key server that is configured to retrieve a selected encrypted key record from the memory (e.g., the encrypted data store on an Oracle KV keystore server).

386. On information and belief, the Oracle KV System comprises a key server that transcribes 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, on information and belief, the Oracle KV key server uses a transcription key derived at least in part from the at least one asymmetric session key to securely transcribe the encrypted key record from server-encrypted (e.g., “wrapped”) form into session-encrypted form. The below slide from a presentation at Oracle Open World 2014 shows the enrollment process for the Oracle KV System.



Saikat Saha, *Introducing Oracle Key Vault: Centralizing Keys, Wallets, and Java Keystores*, ORACLE OPEN WORLD PRESENTATION at 12 (September 29, 2014).

387. On information and belief, the Oracle KV System 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, the Oracle KV System comprises at least one communication port configured to conduct the negotiation between the Oracle KV key server and the authenticated cloud consumer VM environment for the at least one asymmetric session key.

388. On information and belief, the Oracle KV System 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 Oracle KV key server to a remote stream processor for transparent encryption/decryption of cloud data.

389. On information and belief, the Oracle KV key server is configured to communicate with the Oracle KV keystore server through one of at least two types of virtual private networks, SSL VPN and IPSec VPN.

390. On information and belief, one or more Oracle subsidiaries and/or affiliates use the Oracle '181 Products in regular business operations.

391. On information and belief, the Oracle '181 Products include encryption technology.

392. On information and belief, the Oracle '181 Products enable sending encrypted information through an intermediary where the intermediary is not able to view the unencrypted message.

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

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

395. On information and belief, Oracle has directly infringed and continues to directly infringe the '181 patent by, among other things, making, using, offering for sale, and/or selling secure three-party communications products and/or services, including but not limited to, the Oracle '181 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, the Oracle Key Vault and Oracle Wallet.

396. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Oracle '181 Products, Oracle 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 and 11, pursuant to 35 U.S.C. § 271(a).

397. On information and belief, Oracle also indirectly infringes the '181 patent by actively inducing infringement under 35 USC § 271(b).

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

399. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '181 patent. Oracle 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, Oracle provides the Oracle '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 and 6, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '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 Oracle '181 Products in a manner that directly infringes one or more claims of the '181 patent, including at least claims 1 and 6, Oracle specifically intended to induce infringement of the '181 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '181 Products, e.g., through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '181 patent.⁸⁶ Accordingly, Oracle has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '181 patent, knowing that such use constitutes infringement of the '181 patent.

⁸⁶ See e.g., Saikat Saha, *Introducing Oracle Key Vault: Centralizing Keys, Wallets, and Java Keystores*, ORACLE OPEN WORLD PRESENTATION (September 29, 2014); *Oracle Key Vault Administrators Guide 12c Release 1*, ORACLE DOCUMENTATION (June 2015).

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

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

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

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

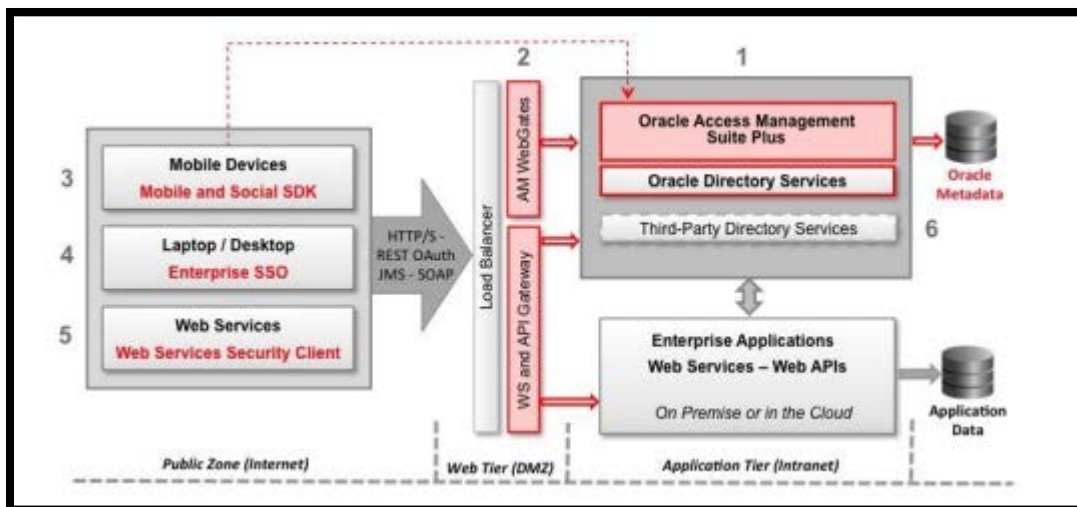
403. Oracle designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling access to digital records stored in one or more databases.

404. Oracle designs, makes, uses, sells and/or offers for sale in the United States products and/or services comprising the Oracle Identity Management Platform Version 11gR2 ("Oracle Access System" or "Oracle '368 Products"). The Oracle Access System includes products and services such as: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.⁸⁷

405. On information and belief, the Oracle '368 Products are Information Rights Management products for information stored in the cloud and/or external databases.

406. On information and belief, the Oracle '368 Products comprise a database system with a plurality of digital records, each having an associated set of access rules, stored in a computer memory associated with a server system.

⁸⁷ See The Oracle Identity Management Platform: Identity Services at Internet Scale, Oracle White Paper (2012) (describing the various products and services that make up the Oracle Identity Management Platform).



Oracle Access Management: Complete, Integrated, Scalable Access Management Solution, ORACLE WHITE PAPER at 4 (2015) (showing the components of Oracle Access Management).

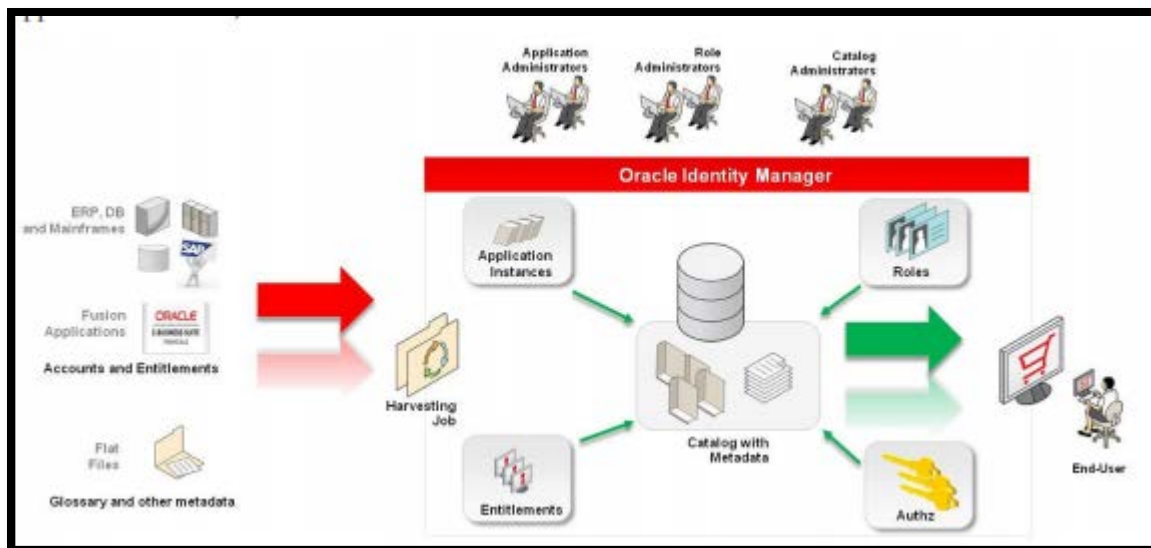
407. On information and belief, the Oracle '368 Products comprise at least one interface computer (e.g., an identity and access management server) in communication with at least one remote computer (e.g., a remote computer requesting to access files in the cloud storage server system) receiving a request to access a digital record stored in the cloud storage server system.

408. On information and belief, the Oracle '368 Products include an automated processor, associated with the server system.

409. On information and belief, the Oracle '368 Products validate the received request to access the digital record by applying a set of access rules (e.g., a role-specific, time-specific, and/or location-specific set of access rules) for the digital record stored in the computer memory. Oracle documentation states “Identity Context secures access to resources using traditional security controls (roles and groups) as well as dynamic data established during authentication and authorization (authentication strength, risk levels, device trust).”⁸⁸

⁸⁸ *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER at 8 (2015)

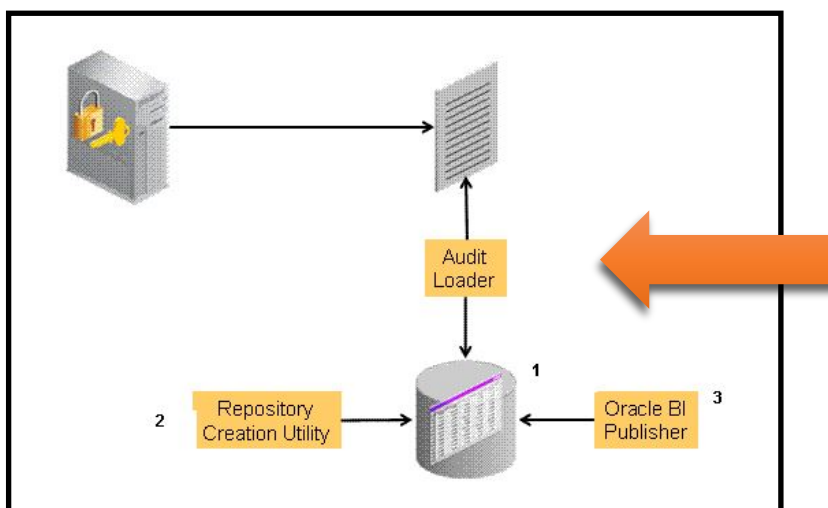
410. On information and belief, the figure below demonstrates the Oracle '368 Products use of a set of role-based access controls, where certain users are only allowed to access certain systems and/or perform certain actions within a given system.



Oracle Identity Manager – Business Overview, ORACLE WHITE PAPER at 8 (January 2014) (showing that the Oracle Identity Manager provides a centralized catalog of access rights, including enterprise and application roles, application accounts, and entitlements).

411. On information and belief, the Oracle '368 Products retrieve a public key having an associated private key in order to implement a first layer of cryptographic protection using an asymmetrical algorithm.

412. On information and belief, after validating the received request, the Oracle '368 Products comprise use X.509 digital certificates in Privacy Enhanced Mail format. Specifically, Oracle Access Manager server stores a per agent (e.g., client accessing the server) key and server key in a credential store on the Oracle Access Manager server side. The X.509 certificate is a signed data structure designed to send a public key to a receiving party. The X.509 certificate includes standard fields such as certificate ID, issuer's Distinguished Name (DN), validity period, owner's DN, owner's public key, etc.



Oracle Fusion Middleware Administrator's Guide for Oracle Access Management, ORACLE HELP CENTER at 18 (2015) (arrow showing the ability of Oracle Access Management to audit to a database).

413. On information and belief, the Oracle '368 Products encrypt and send the requested digital record using the public key and the session key to encrypt the digital record.

414. On information and belief, Oracle 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 managing access to secure records, including but not limited to, the Oracle '368 Products, which include infringing encryption technologies. Such products and/or services include, by way of example and without limitation, the Oracle Identity Management Platform Version 11gR2 which includes: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.

415. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Oracle '368 Products, Oracle 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 and 78, pursuant to 35 U.S.C. § 271(a).

416. On information and belief, Oracle also indirectly infringes the '368 patent by actively inducing infringement under 35 USC § 271(b).

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

418. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '368 patent. Oracle 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, Oracle provides the Oracle '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 and 78, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '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 Oracle '368 Products in a manner that directly infringes one or more claims of the '368 patent, including at least claims 1 and 78, Oracle specifically intended to induce infringement of the '368 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '368 Products, e.g., through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '368 patent.⁸⁹ Accordingly, Oracle has induced and continues to induce users of the accused products to use the accused products in their ordinary

⁸⁹ See e.g., *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*, ORACLE HELP CENTER (2015); *Oracle Identity Manager – Business Overview*, ORACLE WHITE PAPER (January 2014); *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER (2015).

and customary way to infringe the '368 patent, knowing that such use constitutes infringement of the '368 patent.

419. Accordingly, Oracle has induced and continues to induce users of the accused products to use the accused products in their ordinary and customary way to infringe the '368 patent, knowing that such use constitutes infringement of the '368 patent.

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

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

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

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

423. Oracle designs, makes, uses, sells, and/or offers for sale in the United States products and/or services for managing access to protected data.

424. Oracle designs, makes, uses, sells and/or offers for sale in the United States products and/or services comprising the Oracle Identity Management Platform Version 11gR2 ("Oracle Access System" or "Oracle '630 Products"). The Oracle Access System includes products and services such as: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.⁹⁰

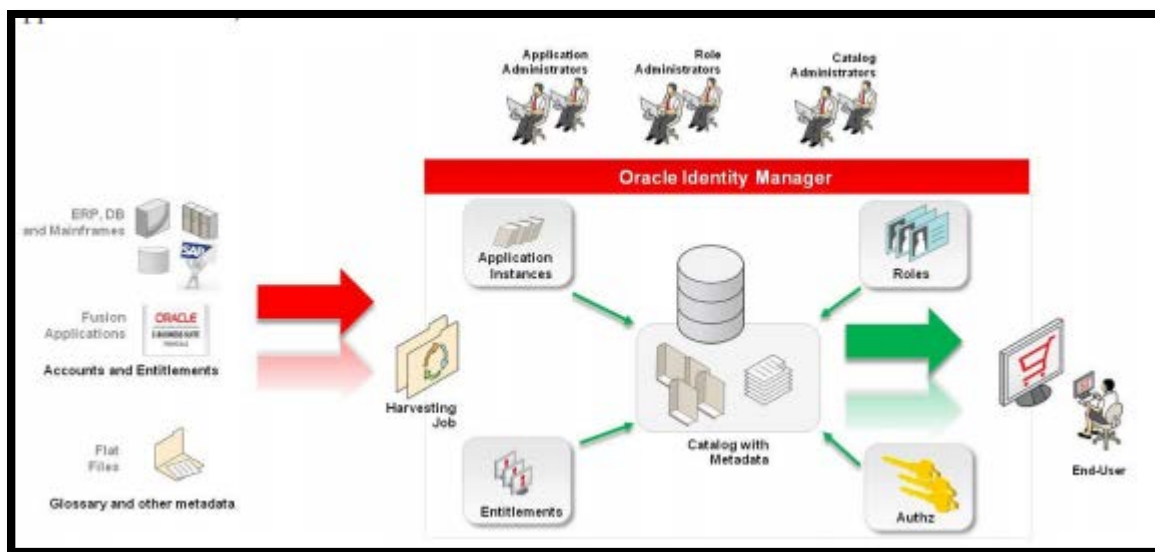
⁹⁰ See *The Oracle Identity Management Platform: Identity Services at Internet Scale*, ORACLE WHITE PAPER (2012) (describing the various products and services that make up the Oracle Identity Management Platform).

425. On information and belief, the Oracle ‘630 Products are Information Rights Management products for information stored in the cloud.

426. On information and belief, the Oracle ‘630 Products enable receiving an information request from a user for information stored in a plurality of external databases.

427. On information and belief, the Oracle ‘630 Products enable authenticating a user. For example, on information and belief, the Oracle Access System “secures access to resources using traditional security controls (roles and groups) as well as dynamic data established during authentication and authorization (authentication strength, risk levels, device trust).”⁹¹

428. On information and belief, the Oracle ‘630 Products apply access rules associated with located requested information. For example, on information and belief, the Oracle Access System incorporates role-based access controls, where certain users are allowed to access certain systems and/or perform certain actions within a given system.

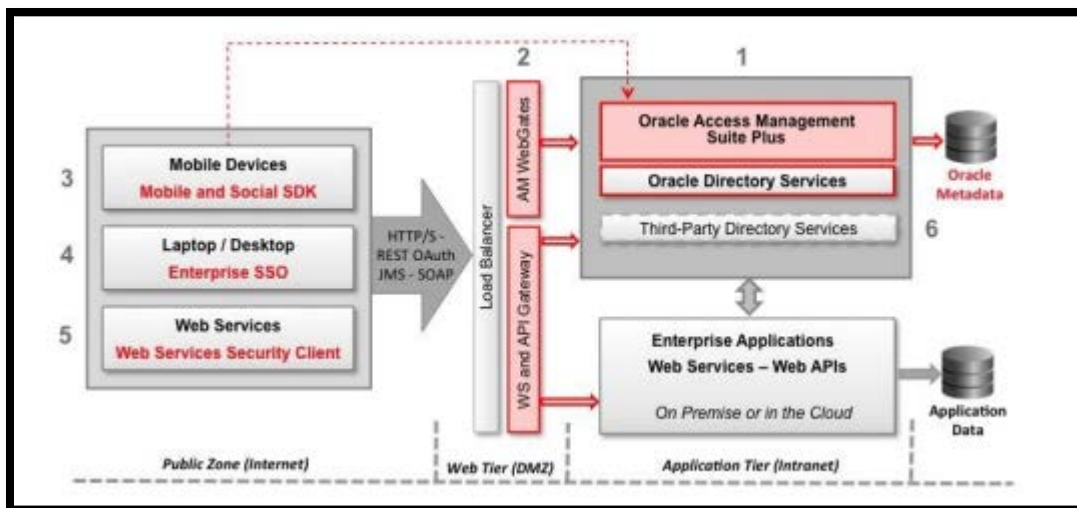


Oracle Identity Manager – Business Overview, ORACLE WHITE PAPER at 8 (January 2014) (showing that the Oracle Identity Manager provides a centralized catalog of access rights, including enterprise and application roles, application accounts, and entitlements).

429. On information and belief, the Oracle ‘630 Products include functionality for automatically communicating through an automated security mediator to a plurality of external

⁹¹ *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER at 8 (2015)

databases. For example, on information and belief, the Oracle Access System obtains an access token for the user. The access token is then sent in the request to the web-hosted client resource (external data source), which authorizes the user and returns the desired resource.



Oracle Access Management: Complete, Integrated, Scalable Access Management Solution, ORACLE WHITE PAPER at 4 (2015) (showing the components of Oracle Access Management).

430. On information and belief, the Oracle ‘630 Products receive a request for authorization to access an external data source. The request received by the Oracle ‘630 Products includes the Client ID and redirect URL of the client. The Oracle ‘630 Products authenticate the user and issue an authorization code response back to the client application’s redirect URL. The Oracle ‘630 Products then issue an authorization code response back to the redirect URL, where the client application extracts the authorization code from the response. Using this authorization code, the client sends a request to the Oracle ‘630 Products’ token endpoint that includes the authorization code. Next, the Oracle ‘630 Products validate the authorization code and information about the client and the web-hosted client resource. Upon successful validation, the Oracle ‘630 Products return an access token. The web-hosted client resource then validates the access token, and if validation is successful, returns the external data source.⁹²

⁹² See *Oracle® Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service 11g Release 1 (11.1.1)*, ORACLE HELP CENTER at § E-2 (July 2011) (“The system for using public keys is called a public key infrastructure (PKI). As part of a

431. On information and belief, the Oracle '630 Products automatically communicate to each of the external databases storing located requested information: a query corresponding to the information request, and information sufficient to apply a set of native access rules of the respective external databases storing the located request information. For example, as explained in Oracle's documentation, the Oracle Access System includes granular, access security rules based on IT-defined user roles.⁹³

432. On information and belief, the Oracle '630 Products contain robust logging and audit trail functionality.⁹⁴

433. On information and belief, Oracle 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 managing access to secure records, including but not limited to, the Oracle '630 Products, which include infringing access management technologies. Such products and/or services include, by way of example and without limitation, the Oracle Identity Management Platform Version 11gR2 which includes: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.

434. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Oracle '630 Products, Oracle has injured St. Luke

public key infrastructure, a certificate authority checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. When the RA verifies the requestor's information, the CA can issue a certificate. Private keys can be derived from a public key. Combining public and private keys is known as asymmetric cryptography, which can be used to effectively encrypt messages and digital signatures.”).

⁹³ *Oracle Identity Manager – Business Overview*, ORACLE WHITE PAPER at 8 (January 2014).

⁹⁴ *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*, ORACLE HELP CENTER at 18 (2015).

and is liable to St. Luke for directly infringing one or more claims of the '630 patent, including at least claims 1 and 9, pursuant to 35 U.S.C. § 271(a).

435. On information and belief, Oracle also indirectly infringes the '630 patent by actively inducing infringement under 35 USC § 271(b).

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

437. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '630 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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '630 patent. Oracle 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, Oracle provides the Oracle '630 Products that have the capability of operating in a manner that infringe one or more of the claims of the '630 patent, including at least claims 1 and 9, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '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 Oracle '630 Products in a manner that directly infringes one or more claims of the '630 patent, including at least claims 1 and 9, Oracle specifically intended to induce infringement of the '630 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '630 Products, *e.g.*, through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '630 patent.⁹⁵ Accordingly, Oracle has induced and continues to induce

⁹⁵ See *e.g.*, *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*, ORACLE HELP CENTER (2015); *Oracle Identity Manager – Business Overview*, ORACLE WHITE

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.

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

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

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

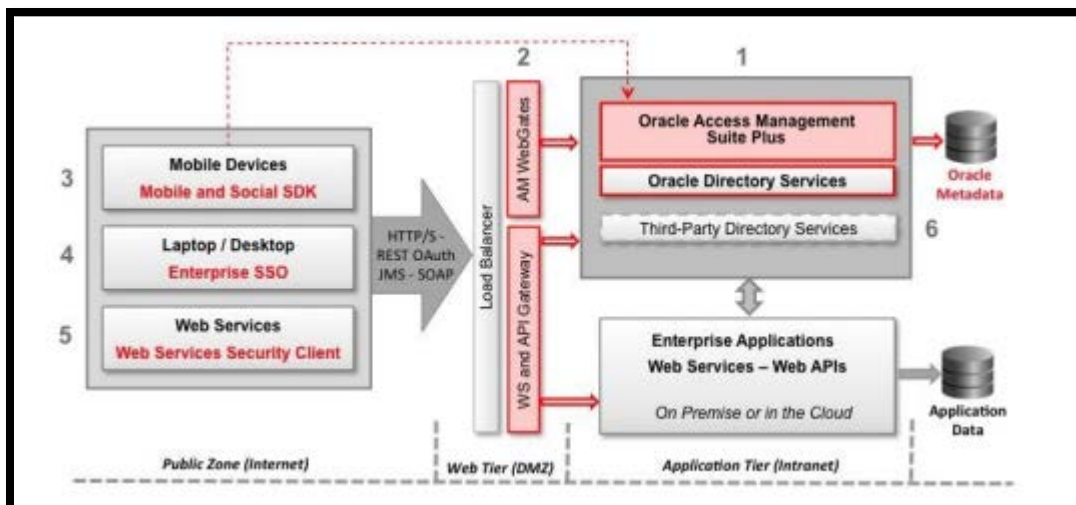
440. St. Luke references and incorporates by reference the preceding paragraphs of this Complaint as if fully set forth herein.

441. Oracle makes, uses, sells, and/or offers for sale in the United States products and/or services for controlling access to protected data.

442. Oracle designs, makes, uses, sells and/or offers for sale in the United States products and/or services comprising the Oracle Identity Management Platform Version 11gR2 ("Oracle Access System" or "Oracle '895 Products"). The Oracle Access System includes products and services such as: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.⁹⁶

PAPER (January 2014); *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER (2015).

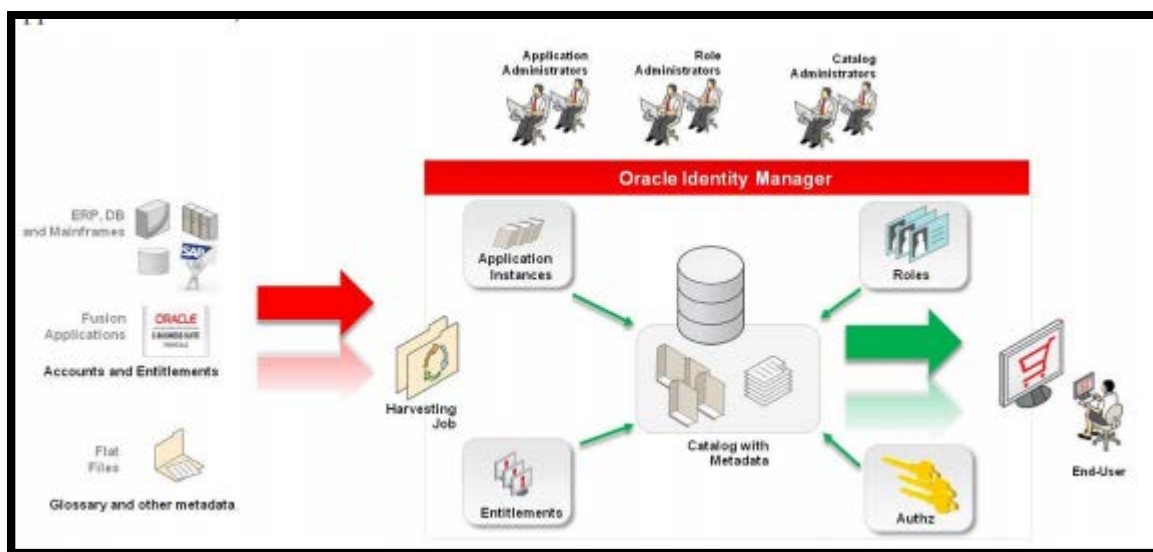
⁹⁶ See *The Oracle Identity Management Platform: Identity Services at Internet Scale*, Oracle White Paper (2012) (describing the various products and services that make up the Oracle Identity Management Platform).



Oracle Access Management: Complete, Integrated, Scalable Access Management Solution, ORACLE WHITE PAPER at 4 (2015) (showing the components of Oracle Access Management).

443. On information and belief, the Oracle ‘895 Products are Information Rights Management products for information stored in the cloud and/or external databases.

444. On information and belief, the Oracle ‘895 Products comprise a database system with a plurality of digital records, each having an associated set of access rules, stored in a computer memory associated with a server system.



Oracle Identity Manager – Business Overview, ORACLE WHITE PAPER at 8 (January 2014) (showing that the Oracle Identity Manager provides a centralized catalog of access rights, including enterprise and application roles, application accounts, and entitlements).

445. On information and belief, the Oracle '895 Products perform a method for controlling access to a plurality of records provided within a plurality of automated electronic databases, each record having an associated set of access rules.

446. On information and belief, the Oracle '895 Products receive a request containing a specified content identifier at a centralized automated security processor.

447. On information and belief, the Oracle '895 Products authenticate the requestor. For example, on information and belief, Oracle Access System “secures access to resources using traditional security controls (roles and groups) as well as dynamic data established during authentication and authorization (authentication strength, risk levels, device trust).”⁹⁷

448. On information and belief, the Oracle '895 Products query an automated central index to find entries corresponding to specified content identifier. For example, on information and belief, the oracle '895 Products—through server-side program code written, maintained, and sold by Oracle; and stored on and executed by Oracle 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 public and/or private cloud data stores, each external to the centralized Oracle '895 Products authentication and access control index), each record having an associated set of access rules (e.g., an associated set of Oracle Access System granular access rules and/or data store specific native access rules), a location identifier (e.g., an URL for the record and/or its data store), and a content identifier (e.g., content metadata for a respective record) maintained in an automated centralized index (e.g., an automated, centralized Oracle '895 Product authentication and access control index).

449. On information and belief, the Oracle '895 Products logically associate the accessible, releasable records into a linked set of releasable records and communicate the linked set of records to the requestor.

⁹⁷ *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER at 8 (2015)

450. On information and belief, Oracle 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 managing access to secure records, including but not limited to, the Oracle '895 Products, which include infringing document infrastructure technologies. Such products and/or services include, by way of example and without limitation, the Oracle Identity Management Platform Version 11gR2 which includes: Oracle Access Management Identity Federation, Oracle Access Management Cloud Federation, Oracle Identity Manager, Oracle Identity Analytics, Oracle Privileged Account Manager, Oracle Access Manager, Oracle Adaptive Access Manager, Oracle Enterprise Gateway, Oracle Identity Federation, Oracle Security Token Service, Oracle Entitlements Server, and Oracle Enterprise Single Sign-On.

451. By making, using, testing, offering for sale, and/or selling encryption products and services, including but not limited to the Oracle '895 Products, Oracle has injured St. Luke and is liable to St. Luke for directly infringing one or more claims of the '895 patent, including at least claim 1, pursuant to 35 U.S.C. § 271(a).

452. On information and belief, Oracle also indirectly infringes the '895 patent by actively inducing infringement under 35 USC § 271(b).

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

454. On information and belief, Oracle intended to induce patent infringement by third-party customers and users of the Oracle '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. Oracle specifically intended and was aware that the normal and customary use of the accused products would infringe the '895 patent. Oracle 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, Oracle provides the Oracle '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 claim 1, and Oracle further provides documentation and training materials that cause customers and end users of the Oracle '895 Products to utilize the products in a manner that directly infringe one or more claims of the '895 patent. By providing instruction and training to customers and end-users on how to use the Oracle '895 Products in a manner that directly infringes one or more claims of the '895 patent, including at least claim 1, Oracle specifically intended to induce infringement of the '895 patent. On information and belief, Oracle engaged in such inducement to promote the sales of the Oracle '895 Products, *e.g.*, through Oracle's user manuals, product support, marketing materials, and training materials to actively induce the users of the accused products to infringe the '895 patent.⁹⁸ Accordingly, Oracle 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.

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

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

⁹⁸ See *e.g.*, *Oracle Fusion Middleware Administrator's Guide for Oracle Access Management*, ORACLE HELP CENTER (2015); *Oracle Identity Manager – Business Overview*, ORACLE WHITE PAPER (January 2014); *Oracle Access Management: Complete, Integrated, Scalable Access Management Solution*, ORACLE WHITE PAPER (2015).

PRAYER FOR RELIEF

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

- A. A judgment in favor of Plaintiff St. Luke that Oracle has infringed, either literally and/or under the doctrine of equivalents, the '237 patent, the '017 patent, the '591 patent, the '181 patent, the '368 patent, the '630 patent, and/or the '895 patent;
- B. An award of damages resulting from Oracle's acts of infringement in accordance with 35 U.S.C. § 284;
- C. A judgment and order requiring Oracle 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 21, 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