

---

# The Business Leader Data Retention and E-Discovery Primer

by *Rebecca Herold, CISSP, CISM, CISA, FLMI*

July 2006


Many organizations are taking advantage of using a wider range of communication systems and technologies than ever before. For example, just to name a few:

Voice over IP (VoIP) is used not only for voice communications but also often integrated with the corporate email system.

Instant messaging (IM) is commonly used to allow real-time interactive business communications.

Blackberry messaging devices are used by a large number of business personnel to send and receive email no matter where they are at, at any time of the day.

These are certainly timesaving and efficient business tools. However, business leaders need to consider the archiving, retention, and discovery requirements that are involved with these technologies to ensure they are not unknowingly putting the business at information security, privacy, and/or legal risk with the ways in which the technologies are implemented.


 What does “discovery” mean? The Encyclopedia Britannica defines legal “discovery” as “In law, pretrial procedures providing for the exchange of information between the parties involved. Discovery may be made through interrogatories, written questions sent from one side to the other in an attempt to secure important facts. It also can be made through depositions, whereby a witness is sworn and, in the presence of attorneys for both sides, is subjected to questions. (The written record of the proceedings also is called a deposition.) Other forms of discovery include an order of production and inspection, which compels the opposing party to produce relevant documents or other evidence, and requests for medical examination in cases in which a party's mental or physical condition is at issue.”

The following discussion is provided to raise awareness of these issues and should not be considered legal advice. Discuss all applicable laws, requirements, and interpretations with your legal counsel to determine how they apply to your particular organization’s unique situation.

---

## Data Retention

Penalties for noncompliance with retention of data in all forms, for a large number of laws and regulations, range all the way from warning letters to multi-million dollar fines, prison time, and business closure.

 In 2003, the U.S. Securities and Exchange Commission (SEC) Final Rule: Retention of Records Relevant to Audits and Reviews went into effect. If you fall under the SEC, you should familiarize yourself with this regulation. Voicemail records generally would not fall within the retention requirements scope of this particular rule “provided they do not contain information or data, relating to a significant matter, that is inconsistent with the auditor’s final conclusions, opinions or analyses on that matter or the audit or review.” However, voicemail would need to be retained “if that item documented a consultation or resolution of differences of professional judgment.” Content and specific types of information are a major consideration for organizations when making retention decisions.

A few of the U.S. laws that have very specific security and retention requirements include:

21 CFR Part 11: Electronic Records, Electronic Signatures

21CFR58.195: FDA Good Laboratory Practice

Age Discrimination in Employment Act

Americans with Disabilities Act

Commodity Futures Trading Commission (CFTC) Rule 1.31

Communications Assistance for Law Enforcement Act (CALEA)

Department of Energy (DOE)10 CFR 600.153 Retention and Access Requirements for Records

Employee Retirement Income Security Act of 1974

FDA Good Manufacturing Standards

Federal Wiretap Act

Gramm-Leach-Bliley Act (GLBA)

Health Insurance Portability and Accountability Act (HIPAA)

Internal Revenue Code Title 26

Mammography Quality Standards Act of 1992 (MQSA)

NASD 3110 and 3111

Occupational Safety and Health Act

Sarbanes-Oxley Act (SOX)

Securities Exchange Act Rules 17a-3 and 17a-4

Social Security Administration (SSA) Records Retention

---

USA PATRIOT Improvement and Reauthorization Act (the reauthorized USA PATRIOT Act)

Toxic Substances Control Act

U.S. Forestry Service

US Code Title 44 (Paperwork Reduction Act)

USA PATRIOT Act

White House's National Strategy to Secure Cyberspace



On June 30, 2006, amendments to CALEA were proposed that, if enacted into law, would greatly impact businesses, particularly ISPs. In particular the amendments would:

- Require routing and addressing hardware manufacturers to offer upgrades or other modifications needed to support Internet wiretapping.
- Authorize the expansion of wiretapping requirements to “public interest” commercial Internet services including instant messaging and VoIP.
- Require ISPs to be able to search customers’ communications to identify VoIP calls, instant messages, and other specific types of communications that could go through the Internet.
- Eliminate the current legal requirement for the Justice Department to publish a yearly public notice of the actual number of communications interceptions.

In addition to the plethora of U.S. laws, there are many more security and retention laws worldwide. For example:

European Union (EU) Data Protection Directive

EU Directive on Telecommunications Privacy

Australia’s Privacy Act of 1988

Canada’s Personal Information Protection and Electronic Data Act (PIPEDA)

Japan’s Personal Information Protection Law



See the March 2006 paper “Data Retention Compliance” for some of the specific requirements of many of these laws (<http://www.realtime-itcompliance.com/LearningCenter/ReadingRoom/tabid/103/Default.aspx>).

---

## Retention Challenges

There are two very basic challenges to meeting all the data retention requirements. Typically, the retention requirements govern the specific types of data that must be retained but not the corresponding forms in which the data is stored. And often the data retention requirements for the same types of data are in conflict throughout multiple applicable laws. Accompanying and complicating these challenges is that many of the laws are vague and open to interpretation, and most governments do not disseminate specific requirements for compliance except for the most high-profile regulations.

### ***Forms of Data Storage Are Constantly Increasing***

Many years ago, when many of the data retention requirements were established, they did not pose as big of a challenge as they now do; data existed primarily on paper and electronically in a centralized database such as on a mainframe. With the blossoming number of ways in which data can now be stored, the challenge that was a short hurdle for most businesses has now increased to become an endless marathon with no finish line in sight.

Just a few of the places where data can be stored beyond on paper and within a centralized structured electronic environment include:

- Email messages


- Voicemail

- IM

- Portable data storage devices, such as USB thumb drives


- Storage-capable printers and fax machines

An additional complicating factor is that technology allows for data created in one form to be automatically transformed to other forms. For example, the capability exists for voicemail to be integrated and saved as email using VoIP technologies. Businesses must determine and document the data retention requirements involved when the data is in both forms. For example, if your organization has a policy to delete email after 2 weeks, any voice messages that were converted to email will also be deleted after 2 weeks. Will this create problems for your company? Do you need to modify email retention based upon your use of VoIP? Would it be best for your organization to automatically purge VoIP files instead of archiving based upon the file type of the attachment, such as it being a WAV or MP3? Or, would just retaining the messages but not the attachment suffice?

 The key to success is first identifying and classifying the data item types, determining the retention requirements for these data types, then determining the storage locations for the data types.

---

To be successful, organizations must consider and decide how to deal with the different retention requirements in each applicable law. For example, should your organization retain all VoIP data to satisfy the regulation with the longest applicable retention time? Or, should you determine which types of VoIP calls are covered under applicable regulations and only retain those calls, purging the rest? One consequence of deciding to archive all calls for a long period of time is that the discovery process will become more difficult, lengthy, and costly because of the huge volume of archived calls.

 Be sure to include data retention within your business continuity and disaster recovery plans.

### ***Conflicting Law Requirements***

Businesses are often faced with trying to decide which law to follow when there are conflicting data retention requirements. For example, with regard to ISP information:


The U.S. has no law currently on the books with specific data retention length requirements for ISP records. There is currently a proposed Child Pornography and Obscenity Prevention Amendments that would require ISPs to retain records for 1 year.

On March 26, 2006, France published new rules that require ISPs, cybercafé operators, and telecommunications firms to retain connection data for 1 year.

On February 19, 2006, the EU Justice and Home Affairs Ministers approved a plan that will require European telephone service providers and ISPs to retain data on all phone calls and emails for 6 months to 2 years.

Ireland, Slovakia, Poland, and Slovenia all have laws requiring data retention for periods longer than 2 years.


Conflicting data retention legal requirements impact all industries and virtually all organizations. Businesses must carefully consider and hold discussions among legal, privacy, and information security leaders about the applicable laws, corresponding data retention requirements, and the best way to resolve conflicts with the requirements.

 Always document your decisions and your basis for them. They will provide evidence that you considered the issues if your organization is ever under investigation for a matter related to data retention.


---

## Electronic Discovery Issues


Electronic discovery (e-discovery) generally involves the activities necessary for organizations to gather and process information contained in electronically stored documents for litigation. As mentioned previously, these documents can include email messages, voicemail, IM files, VoIP files, video files, and individual files stored in multiple formats on many platforms that are geographically scattered across the globe.

 Ensure that information written by old versions of software can be read with current versions to meet data retention requirements and allow for electronic discovery activities.

The data required for a court case might have to be obtained for individuals, departments, teams, project groups, or a combination of these. Finding the requested information is usually a laborious and time-consuming process. Even if the files are found, much of it cannot be quickly or easily searched because of the format in which it is stored.

 According to the October 2005 Fulbright & Jaworski 2005 Litigation Trends Survey, “E-discovery is the number one new litigation-related burden for general counsel at companies with annual revenue exceeding \$100 million.”


Organizations have faced additional hardships and criticisms because of their retention practices, or lack of, and how it impacted litigation. For example, on June 22, 2006, 49 state attorneys general submitted a letter to the U.S. Congress asking them to require a national standard for ISPs to enable enforcement of investigations, in particular those associated with online sexual predators. This request came after an investigation over a 4-month period of the online video of a sexual attack on a 2-year-old girl in Wyoming was traced and determined to have originated through an ISP in Colorado. However, the ISP’s data retention procedures are to delete their logs after 31 days. According to the letter from the attorneys general, without the information, the case was dropped because the perpetrator was not found. Data retention and e-discovery will continue to have more impact on businesses as technology expands and captures information about activities that can be linked to physical as well as cyber crimes.

 Keep in mind that physical information, such as on printed papers, has legal retention requirements as well.

---


## ***New Electronic Discovery Rules***

E-discovery situations have potentially huge legal and financial impact on businesses and must be managed carefully and diligently according to e-discovery rules and orders.


 On October 19, 1999, a federal judge required Philip Morris USA to preserve “all documents and other records containing information which could be potentially relevant to the subject matter of this litigation.” Despite the order, Philip Morris continued to delete electronic mail, according to their procedures, which was over 60-days old, on a monthly system-wide basis for at least 2 years after the judge’s requirement. In February 2002, the defendants became aware of the situation, and that some emails relevant to the lawsuit were, in all likelihood, lost or destroyed. It was not until June 19, 2002, 4 months after learning about this situation, that Philip Morris notified the Court and the Government. Additionally, despite becoming aware of the problem in February 2002, Philip Morris continued the monthly deletions of email in February and March of 2002. Subsequently, on July 21, 2004, a federal judge ordered Philip Morris USA, Inc. to pay \$2.75 million in sanctions for destroying these emails.


On April 21, 2006 the U.S. Supreme Court approved new and amended federal court rules that will take effect December 2006. Among other issues, these include electronic discovery rules covering how electronic information is handled or acquired. Some of the more significant amendments that will impact businesses include the following:

The safe harbor amendment to Fed. R. Civ. P. 37, Rule 37(f) will allow parties to not be subjected to court sanctions if electronically stored information was deleted or lost as a result of the “routine, good faith operation” of their computer systems. Many businesses are concerned that this wording will lead to corporate defendants modifying their computer systems to “routinely” destroy information needed in litigation.


 Clearly document data retention requirements for your organization, for all types of data, to help diffuse such allegations. Make sure these requirements are clearly communicated to all areas responsible for retention.

The amendment to Rule 26(b)(2) requires the responding party to identify the sources of potential information that it has not searched or produced because the costs and burdens of accessing the information would be excessive. If the requesting party still demands the information, the responding party must demonstrate that the information is not reasonably accessible. Even if the responding party demonstrates this, the new rule allows a court to order the organization to produce the data with “appropriate terms and conditions,” which could include requiring the requesting party to pay for the responding party’s costs of producing the data.

 Businesses must consider not only the cost of data retention but also those involved with retrieving and producing data during discovery. Searching all storage locations and collecting electronic files, duplicating hard drives, restoring backup tapes, and sometimes implementing legacy software to read the files can cost hundreds of thousands of dollars.


 According to e-discovery software vendor Attenex, “Lovells, the sixth largest international law firm in the world, was tasked with evaluating potential conspiracy and fraud claims arising out of a complex multi-party transaction. During the investigation stage, the firm set out to review 35GBs (two million pages) of restored email data under tight staffing and cost controls. Using traditional electronic discovery methods, the case was estimated to take one year and cost \$4-5 million.”

An amendment to Fed. R. Civ. P. 26(b)(5) allows parties to retrieve information that was provided to other parties unintentionally during discovery. After being notified by the producing party that it had received privileged information, the receiving party would be required to return it. If the receiving party believed it was entitled to the information, it would have the burden of making its case to the court. Data is often unintentionally provided to litigation parties within metadata.


 Metadata is commonly described as data about data, and is defined as “information describing the history, tracking, or management of an electronic document” within the Federal Rule of Civil Procedure that goes into effect December 2006. Appendix F to The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age defines metadata as “information about a particular data set which describes how, when and by whom it was collected, created, accessed, or modified and how it is formatted (including data demographics such as size, location, storage requirements and media information.)” Metadata created by any software application has the potential for inadvertent and unintentional disclosure of confidential or privileged information in both a litigation and non-litigation setting.

Other amendments to Rule 26 and Rule 16(b) require parties to address disclosure and discovery of electronically stored information issues early in the litigation.

A revision to Civil Rule 33 states that the responding party “may be required to provide some combination of technical support, information on application software, or other assistance” to enable the requesting party to understand the business records produced.

 Organizations should work with the information security and IT areas to create e-discovery procedures and identify the staff that will be involved to provide such assistance.


An amendment to Rule 34(a) would add a specific category of “electronically stored information” that would be included as information expressly subject to production in discovery along with “documents,” which would remain as a separate category.

 Electronically stored information could be anything within electronic storage devices, including such things as logs, audit trails, voicemail, instant messages, streaming video, information from other types of computers—such as digital video recorders, fax, and copy machines memory—and so on.

Another amendment to Rule 34(d) would permit a requesting party to specify the form in which electronic data must be produced. If a party does not specify the form of production, a responding party must produce the information in the form in which it is “ordinarily maintained,” or a form “which is reasonably useful by the requesting party.”




---

 According to the 2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association (AMA) and The ePolicy Institute, 24 percent of organizations have had employee email subpoenaed, and 15 percent of companies have gone to court to battle lawsuits triggered by employee email.

## Keep Data Proliferation to a Minimum

Minimizing the locations in which critical business data is copied and located will reduce the risks of data retention noncompliance, and the exorbitant costs involved with e-discovery. All the more reason for implementing sound policies regarding data classification, defining the appropriate locations to store certain types of data, and ensuring tight controls that limit storage of massive databases on unlimited numbers of end-user storage devices.

 Unless absolutely necessary to support critical business requirements, do not allow entire databases of customer and employee information and associated data to be stored on mobile computing and storage devices under the control of personnel while outside of the enterprise facilities.

Discuss data retention and discovery issues with your legal counsel prior to establishing policies, procedures, and standards for these issues. Planning ahead for addressing data retention and e-discovery issues will save your organization significant time and money, in addition to reducing the risk of associated fines and penalties.