Legal Developments in eDiscovery: Implications for Security Management

Richard S. Swart and Robert F. Erbacher
Utah State University
richard.swart@usu.edu
Robert.Erbacher@usu.edu

Abstract

This paper defines eDiscovery and reviews recent court cases and amendment to Federal Rules of Civil Procedure that are expanding the scope of permissible discovery. The doctrine of spoliation imposes document retention obligations on organizations under the common law, and security managers need to be aware of this doctrine in order to comply with both statutory and common law obligations. Recent cases are discussed that highlight management obligations, and implications for compliance are reviewed. Common employee practices that could impose substantial liability, and which create unnecessary vulnerabilities are reviewed to highlight the tensions between compliance and access to IT resources.

Keywords: *eDiscovery, spoliation, compliance, security management, document retention, risk management*

COMPLIANCE PRESSURES

Corporations are faced with increasing compliance pressures due to the recent passage of numerous pieces of legislation, including HIPAA, Sarbanes-Oxley, Graham-Leach Bliley, the Patriot Act, breach notifications laws, COPPA, FERPA, FISMA and a host of others. IT is in the midst of a "whirlwind of corporate governance reforms" (Smith & McKeen, 2006). Smith and McKeen state that the slate of new laws and regulations are having a huge impact on IT. They conclude that IT in the future will be

increasingly “controlled, standardized and bureaucratized” (Hurley, 2006; Smith & McKeen, 2006). A key question is whether management can use this new paradigm of regulated IT for process and business improvement. Jon Toigo, a leading author in IT, recently stated that in 2005, US companies will spend $80 billion dollars on compliance efforts over the next five years (Toigo, 2006). The Security Compliance Council’s report “The Struggle to Manage Security Compliance for Multiple Regulations” shows that in 2005 organizations spent 34% of their IT resources on compliance initiatives (Hurley, 2006). The 2005 Global Information Security Survey conducted by Ernst & Young showed that for the first time compliance was the primary driver of IT security (LLP, 2005). This report showed that only a 41% of surveyed companies have viewed regulatory compliance as an opportunity to realign there IT security functions or to change their IT architecture. This report showed that most companies are viewing IT security primarily as a vehicle for addressing compliance, and not as part of their overall IT strategy. Thus, while companies are expending tremendous sums on compliance, it is not apparent that these efforts are part of an organized governance structure, or that these efforts are improving security.

RISK MANAGEMENT AND LITIGATION

Risk management is a key component of effective management in any organization. The maintenance of a thorough inventory of information assets into a coherent and well-documented baseline is a key component of any information assurance function. A major new source of risk for corporations stems from the direct costs of compliance with discovery of electronic records (eDiscovery). Organizations are required to maintain very accurate records of all of their data in order to comply with discovery

requests and effective policies must be in place to prevent the destruction of data which might be relevant to possible litigation. Companies that flout the intent of these court rules have faced substantial fines and have had court enter sanction against them in the course of litigation. This paper will review the laws pertaining to eDiscovery, highlight amendments to the Federal Rules of Civil Procedure which went into effect on December 1, 2006, and discuss the implications of recent court cases for security management and compliance programs. In order to effectively manage this risk, senior IT management and legal must be aware of these new requirements and ensure that the organization's IT systems are capable of compliance.

Discovery Law

According to the Wikipedia definition, in law discovery is "the pre-trial phase in a lawsuit in which each party through the law of civil procedure can request documents and other evidence from other parties or can compel the production of evidence by using a subpoena or through other discovery devices, such as requests for production and depositions" (Wikipedia, 2007). While in the majority of the world discovery is a process conducted by the court, or under the close supervision of the courts, in the United States discovery is a process initiated and performed by the litigants. Most states pattern their rules of procedure after the Federal Rules of Civil Procedure. Chapter V of these rules pertains to discovery and depositions and contain rules 26 -37, many of which were recently modified. Failure to follow-these laws, which in part require the preservation and production of "Electronic Stored Information" (ESI) can result in drastic consequences. In a recent case, counsel's failure to accurately inform opposing counsel of the existence

of ESI, and the willful destruction of ESI, contributed to an adverse $1.4 billion damages judgment against Morgan Stanley. ("Coleman v. Morgan Stanley," 2005).

The Common Law

The common law imposes duties on parties to retain documents. One of the key common law retention doctrines is that of “spoliation” which is the destruction of evidence that is relevant to an existing or pending lawsuit or legal proceeding. These legal proceedings can include agency audits. A company has a duty to preserve any “document” that is related to the issues in a civil or criminal action, audit, or investigation, or when the company is aware that such an action is foreseeable. If a company is found to have negligently or intentionally altered or destroyed evidence that impairs its opponent’s ability prove or defend their claim, a company may be found guilty of spoliation. Opposing counsel and the court may impose sanctions for Spoliation including dismissal of the suit, issue preclusion, adverse inference and even criminal sanctions (Snyder & Isom, 2006).

Electronic Discovery Law

The introduction of evidence from electronic sources is now commonplace in the courts. The Federal Rules of Civil Procedure were written long before this development in evidence, and the courts soon became aware that their rules did not provide adequate guidance to either the lower courts or parties as to their duties to produce electronically stored information. The Advisory Committee on Civil Rules began to tackle the issue of computer-based discovery in 1996. After years of comments and revisions the Judicial Conference and the United States Supreme Court approved the amended rules which

went into effect on December 1, 2006. ("E-Discovery Amendments to the Federal Rules of Civil Procedure Go Into Effect Today," 2006).

The Amended Rules

Key provisions of these new amendments are summarized below.

- Rule 26(b)(2): a party need not provide the discovery or electronically stored information that is not reasonably accessible unless the court orders discovery for good cause
- Rule 26(b)(5)(B): provides a procedure for asserting privilege after production of privileged information— an effort to limit inadvertent waiver
- Rule 33: addresses responding to interrogatories that involve a search of electronically stored information
- Rule 34: Parties must specify whether they seek discovery of documents, electronically stored information, or both; also addresses the objection and dispute resolution procedure
- Rule 37: addresses a party's inability to provide discovery or electronically stored information lost as a result of the routine operation of a party's electronic information system—a sanctions "safe harbor"

Each of these rule changes has direct implications for security and IT management, and these issues are addressed below.

Changing Definitions of Discoverable Material

Under the revised provisions of Rule 16(b), any "electronically stored information" is discoverable. This rule pertains to instant messages, voice over IP, entire databases, or data contained in employees' PDAs or cell phones. No longer can parties limit their eDiscovery planning to formal documents contained within the corporate system. Courts are now aware that evidence may be emailed outside of a company, stored on a laptop, or be contained in instant messages.

Need for Early Attention to ESI Discovery

Rule 26(f) requires an early e-discovery "meet and confer" requirement to address preservation, form of production and protection against privilege waiver. This implies

that as soon as litigation is filed, or reasonably anticipated, counsel and management must move fast to protect corporate ESI and avoid sanctions by the courts.

Management must immediately send a preservation notice to key personnel, which may include business unit managers, DBAs, security administrators, and back-up administrators. This notice informs them to suspend the routine destruction, overwriting, or modification of files, data, or even meta-data pertaining to the issue that may rise to a claim. No paper documents may be destroyed that may pertain to the case. Counsel should also send a preservation notice to their opponent. While many courts have ruled that the routine destruction of documents or data in course of routine work products does not give rise to a claim of spoliation, these new rules have not been subject to testing in the courts and prudence dictates that parties institute preservation practices when any litigation is reasonably foreseeable.

Part of the duty of counsel under the amended rules is to immediately begin due diligence to discover all ESI that may pertain to the case and also to catalog the sources of ESI that may be used. Any disclosure under Rule 26 must explicitly reference the source of ESI that a company may use in its case.

Identification of Data Custodians

Part of the initial disclosure to opposing counsel under Rule 26 must include a list of data custodians. These can be fact witnesses, IT directors, records managers or others who control the ESI access, modification and deletion within the company. This requires that counsel have access to capabilities lists at all times, and that there be an effective operational security management plan in place so that individuals with accountability for the data in question can be immediately identified.

Format of Data or Records Being Produced

Courts have ruled that all data, including meta data should be preserved. Williams v. Sprint/United Mgmt. Co., 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005)("[W]hen a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their meta data intact, unless that party timely objects to production of meta data, the parties agree that the meta data should not be produced, or the producing party requests a protective order.") This case also highlights that litigants are only required to produce the data in the format as maintained for the ordinary course of business. Parties are not required to change the format of the data, or provide any other services to opposing parties. Conversely, parties may not sanitize or scrub their records in order to only reveal portions of the records for discovery purposes. Data must be presented as used in business, which may require the production of entire databases.

ESI contained on Sources That Are Not Reasonably Accessible

While courts may require a company to produce all ESI, Rule 26(b)(2) makes a distinction between ESI that is "reasonably accessible" and that whose production would cause undue hardship or burden. A party may fail to produce requested data if it the cost or hardship is unreasonable. The opposing party may them file a Motion to Compel Discovery and the courts will only grant such a motion for good cause – essentially that the party requesting the data cannot prosecute his claims without it. This limits the ability of counsel to engage in what might be described as "fishing trips" through the records of an opposing company. Due diligence would suggest that estimates of cost be maintained for producing certain types of data. For example, if a company has a distributed

workforce that tele-commutes, the cost of creating forensic copies of all hard-drives of all employees and searching through these images for ESI would clearly be prohibitive. However, accessing a handful of employee computers would be unlikely to result in a defense under Rule 26(b)(2).

"Safe Harbor" Provisions

One of the most debated provisions of the amended rules is the "safe harbor" provision in Rule 37(f). This rule states that absent exceptional circumstances a court may not impose penalties on a party for failing to produce ESI that was lost as a result of the good faith, routine operation of an ESI system. This rule accounts for the routine modification and overwriting of data that are normal in the use of information systems. However, parties must be careful when litigation is reasonably anticipated. In Rambus, Inc. v. Infineon Techs. AG, 220 F.R.D. 264 (E.D.Va. 2004) the plaintiff knew the that the defendant might be bringing patent infringement lawsuits when documents were purged. The Court concluded that even if the plaintiff "did not institute its document retention policy in bad faith, if it reasonably anticipated litigation when it did so, it is guilty of spoliation."

Employee Behaviors that Introduce Risk in eDiscovery

This section of the paper discusses common employee behaviors that introduce significant risk to organizations through possible eDiscovery violations. Two often overlooked sources of vulnerability include instant messaging and e-mail.

Unchecked Instant Messaging Risk

David R. Cohen, Esquire, a partner with Kirkpatrick & Lockhart Nicholson Graham LLP identified the following facts about instant messaging and its implications for discovery (Cohen, 2006).

- 31% of employees use IM at office
- 78% of them downloaded from the internet using IM
- Only 20% of employers have an IM policy
- Only 11% of organizations use IM gateway/management software to monitor/purge/retain or otherwise control IM risks
- 21% of employers have had IM's subpoenaed

Courts have ruled that IMs and email are within the scope of discovery. Many employees do not realize that IM conversations can be stored, logged and discovered. There is little incentive for employees to monitor their own conduct when using IM. It is frequently perceived to be akin to a phone conversation. Employees may inadvertently disclose information that could harm the company in the course of litigation, or even use racist, derogatory, or obscene language that could give rise to other claims.

Another key risk comes from the difficult to purge IMs. It is usually unknown whether copies have been made of IM conversations and there is no central server that can be searched to determine whether the data has been forwarded.

Email Forwarding

Many companies have email scanning software that monitors incoming email, or which archives email within the company. However, the ability of users to forward their emails to other email services such as Yahoo or Gmail imposes serious security concerns (Stone, 2007).

The company loses the ability to purge these emails or to control their distribution once they are forwarded. This has serious implications for the scope of discovery. Counsel cannot certify to their management, or to the court that a record has been

destroyed if it possible that an employee has forwarded a message containing potential ESI. Counsel must be concerned that even if data was deleted during the normal course of business from an email server or storage device, that employees may have forwarded emails to unknown third parties whose existence might become known to opposing counsel. Thus, monitoring of outgoing emails is crucial to ensure that employees are not subverting security policy and creating risk. In certain cases, forwarding of email messages may be a statutory violation. In the article by Stone (2007) it was reported that doctors were forwarding patient records to their personal email accounts to work on them from home. If the doctor were to inadvertently disclose this information to a third party by forwarding it to the wrong individual, or if their personal computer was compromised and the data somehow disclosed the doctor and the hospital would be in violation of 1177(a)(3)(b)(1) of PL 104-191 (HIPAA). This law carries a possible penalty of $50,000 per wrongful disclosure and up to one year of federal imprisonment

Implications for practice

Risks from eDiscovery are so great that IT and legal departments must cooperate and create effective policies and procedures to ensure compliance with the revised Federal Rules of Civil Procedure. Management must also ensure that IT managers are trained on their duty to preserve evidence and that the preservation notice provisions are sufficient to ensure that potential ESI is preserved.

These goals can be accomplished via an effective eDiscovery planning process. This must be a strategic consideration for companies. Controlling costs related to compliance and EDiscovery can be a significant competitive advantage. eDiscovery is a corporate governance level issue requiring the input of a cross-functional executive team

that will govern and monitor the enterprises content management system. Preparing for eDiscovery requires that a company create the following:

1. Email and file server backup tape inventory and catalogue
2. Records management policy that standardizes backup tape
3. Rotation and related preservation rules
4. Litigation readiness protocols, including matter management systems, hold management and electronic information requests
5. Procedures for accessing email and file servers
6. Determine who is the custodian of all records

The objectives of this process include establishing a policy to classify, manage ane dispose of records generated in the business. The company must also establish a file plan based on file contents and ensure that records are disposed of in a timely fashion. Sorting through the mass of electronic and paper records and destroying all but necessary records also can reduce the companies risk exposure. No court has ever sanctioned a company for following its own document retention and destruction policy.

Conclusion

This paper has reviewed recent changes to the Federal Rules of Civil Procedure that pertain to eDiscovery. While these rules provide some protection to companies that are following document retention and destruction policies in good faith, recent cases were presented that highlight the possibility of significant damages from failing to comply with eDiscovery requirements. eDiscovery is a new significant source of risk for organizations, and managing this risk requires that companies create detailed inventories of their paper and electronic documents, maintain up-to-date records of the custodians of those records, and ensure that the records will not be destroyed if litigation is anticipated. Security managers must be aware of these issues to ensure that the corporate policies and controls are adequate to protect against these risks.

References

Discovery (law). (2007, January 12). In *Wikipedia, The Free Encyclopedia*. Retrieved 05:08, January 12, 2007, from http://en.wikipedia.org/w/index.php?title=Discovery_%28law%29&oldid=100333753

Cohen, D. R. (2006). Scene From an E-Discovery Case: What to Do and What Not to Do to Avoid E-Discovery Disasters. Retrieved December 20,, 2006, from http://directorsroundtable.com/pdf/Materials%20NY%20E-Dis%2011-3.pdf

Coleman v. Morgan Stanley (Fla. Cir. Ct. 2005).

E-Discovery Amendments to the Federal Rules of Civil Procedure Go Into Effect Today [Electronic (2006). Version]. *Electronic Discovery Law*. Retrieved January 14, 2007 from http://www.ediscoverylaw.com/2006/12/articles/news-updates/ediscovery-amendments-to-the-federal-rules-of-civil-procedure-go-into-effect-today/print.html.

Hurley, J. (2006). *The struggle to manage security compliance for multiple regulations*. Houston, TX: Security Complaince Council.

LLP, E. Y. (2005). *Global Information Security Survey 2005*. Chicago, IL.

Smith, H. A., & McKeen, J. D. (2006). Developments in practice XXI: IT in the new world of corporate governace reforms. *Communications of the Association for Information Systems, 17*(32).

Snyder, K., & Isom, D. (2006). A 30(b)(6) Can Sink Your Ship. *Information Management Journal*(January/February), 52-55.

Stone, B. (2007). Firms Fret as Office E-Mail Jumps Security Walls. *New York Times*.