ELECTRONIC DISCOVERY RULES AND ELECTRONIC EVIDENCE: A UNITED STATES PERSPECTIVE

Burke T. Ward, Department of Marketing and Business Law, School of Business, Villanova University, USA
burke.ward@villanova.edu

Janice C. Sipior, Department of Accountancy and Information Systems, School of Business, Villanova University, USA
janice.sipior@villanova.edu

Linda Volonino, Information Systems Department, School of Business, Canisius College, USA
volonino@canisius.edu

Carolyn Purwin, Attorney at Law, Philadelphia, Pennsylvania, USA
carolyn.purwin@villanova.edu

Abstract

Electronically stored information (ESI) includes all content an organization stores on electronic media ranging from word processing and spreadsheet files to blog posts and tweets. All forms of ESI may be subject to discovery in a legal dispute, compliance audit, or regulatory investigation. Discovery is the investigative phase of a lawsuit when the parties determine what evidence relevant to the case is, or might be, available. E-discovery amendments to the United States (US) Federal Rules of Civil Procedure became law in December 2006, requiring organizations to respond to e-discovery requests promptly. In order to be able to produce requested data and documents, they must have been saved in such a way that they can be located, accessed, preserved, and searched. With the ever-looming prospect for legal disputes, e.g., employment discrimination, product liability, securities fraud, and theft of intellectual property, organizations doing business in the US are at risk if they are unable to respond. This paper addresses the challenges to organizations in responding to the new e-discovery amendments and concludes with recommendations for the design and development of an electronic records management (ERM) policy that recognizes the duties imposed by the e-discovery amendments.

Keywords: E-Discovery, Electronically Stored Information, Electronic Records Management, Spoliation, Computer Forensics.

1 INTRODUCTION

Electronically stored information (ESI) includes all content an organization stores on electronic media ranging from word processing and spreadsheet files to blog posts and tweets. All forms of ESI may be subject to discovery in a legal dispute, compliance audit, or regulatory investigation. Discovery is the investigative phase of a legal case when the parties determine what evidence relevant to the case is, or might be, available.

In April 2006, the United States (US) Supreme Court approved e-discovery amendments to the Federal Rules of Civil Procedure (FRCP), which became law in December 2006. These amended rules require that organizations respond to electronic discovery (e-discovery) requests promptly and impose sanctions for defaulting parties. As such, e-discovery is an inescapable obligation (like paying...
corporate taxes) to be able to produce all requested ESI. A challenge for organizations is to manage electronic information without exposing the organization to sanctions in a later lawsuit. In order to be able to produce requested data and documents, they must have been saved in such a way that they can be located, accessed, preserved, and searched. With the ever-LOOMING prospect for legal disputes, e.g., employment discrimination, product liability, securities fraud, and theft of intellectual property, organizations in, or doing business within, the US are at risk if they are unable to respond. Failure to comply with e-discovery can result in judicial sanctions. If requested ESI is damaged or destroyed, then additional sanctions can be imposed (Ward et al., 2009). Interestingly, the amendments to the FRCP closely mirror the e-discovery obligation in the United Kingdom, which is defined in Part 31 of the Civil Procedure Rules (CPR) (Room, 2008). The critical necessity to meet e-discovery requirements is thus a common compliance requirement confronting organizations across geographies (Trend Micro, 2009).

This paper examines the legal e-discovery process by addressing the challenges confronting organizations in meeting e-discovery requirements and proposes electronic records management (ERM) policies and practices that recognize the duties imposed by the e-discovery amendments.

2 THE LEGAL DISCOVERY PROCESS

Discovery is the formal pre-trial process whereby litigating parties discover and obtain information. Subject to certain exceptions, such as privileged information, the scope of discovery is relevancy. Admissibility is not an issue in discovery. Rule 26(b)(1) of the FRCP states that:

*Parties may obtain discovery regarding any matter, not privileged, that is relevant to the claim or defense of any party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence.*

Discoverable items include hard-copy documents and any data stored in electronic format. E-discovery is the process of acquiring and presenting electronic information in the discovery phase of litigation. The process of acquiring electronic information includes forensics and retrieval of information. Presenting electronic information includes organization and indexing, presentation in a searchable format, enabling document production with the information, and packaging for presentations (Brown, 2003). Digital information from any source, including primary files, copies, versions, metadata, system data, legacy data, and backup data, is discoverable if relevant and not privileged (Withers, 2000).

2.1 Amendments to the Federal Rules of Civil Procedure

On December 1, 2006, amendments to the FRCP, relevant to e-discovery, became effective. These amendments to Rules 16, 26, 33, 34, 37, and 45 are intended to bring the discovery rules up-to-date in an information age (Finnegan and Wein, 2006). The amendments to rules 26, 34, and 37 are most relevant to the scope of this paper.

Although extended by case law, amended Rule 34(a) specifically extended the scope of discovery to ESI. Rule 34(a) states:

*Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor’s behalf, to inspect, copy, test, or sample any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained — translated, if necessary, by the respondent into reasonably*
usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served;

Prior to the amendments, all discoverable information was treated the same, whether physical or electronic. The amendment to Rule 26(b) creates a two-tier classification to ESI. Rule 26 (b)(2)(B) states that:

(B) A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Thus, the amendment creates a distinction between ESI that is reasonably accessible, and that which is “not reasonably accessible.” What does this mean? Neither the Rule, nor the Advisory Committee report defines these terms. The Advisory committee gives as examples, of costly or burdensome retrieval, “deleted information, information kept on some backup tape systems for disaster recovery purposes, and legacy remaining from systems no longer in use.” (Beirne et al., 2006).

The Rule’s standard is “not reasonably accessible because of undue burden or cost.” Because of the Rule’s vagueness, guidance will have to come from judicial precedent. The leading case on this issue is *Zubulake v. UBS Warburg* (2003). *Zubulake* was an employment discrimination case. One of the initial issues was the plaintiff’s discovery demands for back emails. The defendant claimed that the requested information was inaccessible, in part because of cost. In deciding this issue, Judge Scheindlin looked to the type of media on which the information is stored, and the cost of its production. She created five categories, presented in Table 1.

<table>
<thead>
<tr>
<th>1.</th>
<th>Active, online data</th>
</tr>
</thead>
<tbody>
<tr>
<td>“On-line storage is generally provided by magnetic disk. It is used in the very active stages of an electronic records [sic] life-when it is being created or received and processed, as well as when the access frequency is high and the required speed of access is very fast, i.e., milliseconds.” Examples include hard drives.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2.</th>
<th>Near-line data</th>
</tr>
</thead>
<tbody>
<tr>
<td>“This typically consists of a robotic storage device (robotic library) that houses removable media, uses robotic arms to access the media, and uses multiple read/write devices to store and retrieve records. Access speeds can range from as low as milliseconds if the media is already in a read device, up to 10-30 seconds for optical disk technology, and between 20-120 seconds for sequentially searched media, such as magnetic tape.” Examples include optical disks.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3.</th>
<th>Offline storage/archives</th>
</tr>
</thead>
<tbody>
<tr>
<td>“This is removable optical disk or magnetic tape media, which can be labeled and stored in a shelf or rack. Off-line storage of electronic records is traditionally used for making disaster copies of records and also for records considered ‘archival’ in that their likelihood of retrieval is minimal. Accessibility to off-line media involves manual intervention and is much slower than on-line or near-line storage. Access speed may be minutes, hours, or even days, depending on the access-effectiveness of the storage facility.” The principled difference between nearline data and offline data is that offline data lacks “the coordinated control of an intelligent disk subsystem,” and is, in the lingo, JBOD (Just a Bunch Of Disks).</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.</th>
<th>Backup tapes</th>
</tr>
</thead>
</table>
| “A device, like a tape recorder, that reads data from and writes it onto a tape. Tape drives have data capacities of anywhere from a few hundred kilobytes to several gigabytes. Their transfer speeds also vary considerably ... The disadvantage of tape drives is that they are sequential-access devices, which means that to read any particular block of data, you need to read all the preceding blocks.” As a result, “[t]he data on a backup tape are not organized for retrieval of individual documents or files [because] ...
the organization of the data mirrors the computer’s structure, not the human records management structure.” Backup tapes also typically employ some sort of data compression, permitting more data to be stored on each tape, but also making restoration more time-consuming and expensive, especially given the lack of uniform standard governing data compression.

5. Erased, fragmented or damaged data

“When a file is first created and saved, it is laid down on the [storage media] in contiguous clusters ... As files are erased; their clusters are made available again as free space. Eventually, some newly created files become larger than the remaining contiguous free space. These files are then broken up and randomly placed throughout the disk.” Such broken-up files are said to be “fragmented,” and along with damaged and erased data can only be accessed after significant processing.

Table 1. Categories of media to determine accessibility of electronically stored information.

<table>
<thead>
<tr>
<th>3 ELECTRONICALLY STORED INFORMATION</th>
</tr>
</thead>
</table>

ESI has become the dominant form of discovery in the litigation process. “We used to say there’s e-discovery as if it was a subset of all discovery. But now there’s no other discovery.” (Losey, 2009). The duty to preserve and produce evidence that is discoverable in pending or anticipated litigation has led to unique problems in e-discovery (Sedona Conference, 2007b). ESI is more voluminous than paper discovery and can be stored or produced in a variety of formats. These issues have contributed to increased litigation costs. Additionally, e-discovery has contributed to an increase in unintentional disclosure of privileged information which can have significant consequences to litigants (Redgrave and Nimsger, 2002).

The US Congress and the Judiciary responded to these issues by making changes to both the FRCP and Federal Rules of Evidence (FRE) (K&L Gates, 2008). With the seemingly unlimited ways to retrieve data, Congress proposed amendments to the FRCP and FRE (Conference of Chief Judges, 2006). These recent changes addressed the prevalence and scope of ESI and its impact on the discovery process. Amendments were designed to control and allocate costs, address issues unique to electronic data, and develop ways to protect attorney-client privilege, and waiver of this privilege in ESI. Attorneys have a duty to advise their clients of their obligation to respond truthfully and completely, to all discovery requests (Wilson, 2006). The ubiquitous nature of ESI has increased the complexity and cost of compliance.

3.1 Challenges in Managing Electronically Stored Information

Previously, non-testimonial evidence primarily consisted of paper documents, photographs and other physical evidence. With the digital age, the format of discovery has changed significantly to include ESI. It is now estimated that 99% of information created and stored is done electronically (Whetstone and Simon, 2006, at p. S1). This has increased the challenges to organizations in managing ESI and meeting e-discovery requirements, including volume of storage, preservation, spoliation, and cost.

3.1.1 Volume of Storage

One of the unique aspects of ESI is the volume stored. Data collections now run into the gigabytes or terabytes for review (Kershaw, 2005). A gigabyte can hold up to 677,693 of plain text documentation or 64,782 pages of Microsoft Word documents (Applied Discovery, 2008). A terabyte can hold up to 75 million pages (Kershaw, 2005). Backup disks alone can hold up to 500 billion pages of plain text (Federal Judiciary Center, 2004). On average employees send or receive about 50 e-mail messages per day, which is an equivalent of more than 1,200,000 messages a year for an organization of 100 employees (Microsoft PressPass, 2005). If a large company has 100,000 employees, the company could be storing up to 1.5 billion emails annually (Moore's Federal Practice, 2009). Many email users send the same email to multiple recipients, who forward it to other recipients. The producing party
“can be required to design a computer program to extract data from its computerized business records, subject to the court’s allocation of costs.” (Anti-Monopoly, Inc. v. Hasbro, Inc., 1995)

E-discovery is therefore more voluminous than paper discovery. Electronic data can be stored in a much greater volume and more places (e.g., on the hard drive of the document’s creator, reviewers, recipients, on the company computer, laptop, home computer, backup tapes) than hard-copy data. Preservation of data has become a complex issue because as time continues new hardware and software is created and as systems become outdated, archives and potentially discoverable data may be destroyed. Metadata, or embedded information that traces the history of a file, exists only for electronic document and historically was excluded from discovery. This information is now discoverable and often a case-changing part of litigation.

Information that is stored is “electronic” if it exists in a medium that can only be read by a computer, including email, web pages, word processing files, audio and video files, images, computer databases, spreadsheets and virtually anything else that is stored on a computing device – including but not limited to servers, desktops, laptops, cell phones, hard drives, flash drives, PDAs and MP3 players. E-discovery also can include metadata, ESI about the characteristics, origins, or the validity of the electronic data. The media that is used to store this information includes cache memory, magnetic disks (such as computer hard drives or floppy disks), optical disks (such as DVDs or CDs), magnetic tapes and flash memory (such as “thumb” or “flash drives”). A single CD-ROM has the ability to store thousands of pages and a hard drive can easily store the equivalent of hundreds of CD-ROMs (Moore's Federal Practice, 2009). Litigants are entitled to emails as long as they are relevant to claims specified in the case (Zubulake v. UBS Warburg, 2003, “Zubulake I”).

Some business applications use caching to back up data, which refers to the temporary storage of information where it can be readily accessible for future use. Data is retrieved quicker from cache then from the original storage location; cache allows applications to run more quickly (Sedona Conference, 2007a). Web site contents often reside in cached storage locations on a hard drive by “storing of copies of content [that subscribers wish to see most often] at locations in the network closer to subscribers than their original sources ... in order to provide more rapid retrieval of information.” (Inquiry, 2002). Attorneys sometimes use these web caching services to develop the merits of their case.

3.1.2 Preservation

The new Rules require additional preservation and production methods, including parties’ suspension of “routine or intentional purging, overwriting, re-using, deleting, or any other destruction of electronic information relevant to a lawsuit, including electronic information wherever it is stored - at a university workstation, on a laptop or at an employee's home computer.” (Texas A&M University, No Date). Deleted electronic information can be subject to discovery because it is often saved on a backup or emergency system. All of these issues have promulgated what is considered the largest problem in the e-discovery process, which is cost. Discovery is no longer “just about uncovering the truth, but also about how much of the truth the parties can afford to disinter.” (Zubulake v. UBS Warburg, 2003, “Zubulake I”). Some courts have required information in its electronic form even after a responding party has produced the documents in paper form (National Union Electronic Corp. v. Matsushita Electric Industrial Co., 1980).

The preservation of electronic data is an essential tool for litigants to avoid problems in litigation. Litigants and their counsel have a duty to preserve any electronic documents that may be relevant or anticipated for future litigation (Zubulake v. UBS Warburg LLC, 2003 “Zubulake IV”). “While a litigant is under no duty to keep or retain every document in its possession...it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.” (William T. Thompson Co. v. General Nutrition Corp., Inc., 1984). ExxonMobil’s in-house counsel estimated that the company spends $1.9 million
per month creating and preserving electronic information on backup tapes for litigation (Judicial, 2004).

Standards have now been developed to instruct litigants on how to preserve and manage electronic records. FRCP 37(f) acknowledges that if a party does not act in good faith when developing a proposed discovery plan, the court “may, after giving an opportunity to be heard, require that party or attorney to pay to any other party the reasonable expenses, including attorney's fees, caused by the failure.” (Federal Rules of Civil Procedure, 2009). The good faith requirement of Rule 37(f) means that a party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve (Federal Rules of Civil Procedure, 2009).

Clients must be advised that failure to comply with subpoenas can lead to not only civil charges and spoliation sanction but to criminal charges, including obstruction of justice.

3.1.3 Spoliation

As important as the duty to preserve data, litigants also have a duty against the spoliation of electronic data, which is the “destruction or significant alteration of evidence, or the failure to preserve property for another’s use as evidence in pending or reasonably foreseeable litigation.” (Zubulake v. UBS Warburg LLC, 2003 “Zubulake IV”). With respect to paper documents, information could be shredded to avoid discovery by opposing counsel. However, for electronic data a deletion of a document fails to permanently remove the information as it is easily recoverable on a hard drive or back up tape. Some courts have found that intentional spoliation of electronic records is sanctionable where parties have deleted or destroyed evidence that could be found on a computer during or in anticipation of litigation (Bauccio, 2007).

Companies that fail to comply with the new standards or restrictions for destroying or recycling electronic data risk millions of dollars or perhaps more in sanctions during litigation. In some cases, Courts exclude testimony of witnesses based on evidence that was destroyed. If a jury determines that evidence was destroyed while in control of a party, the judge may instruct the jury to use an adverse inference, which allows the jury to infer that the evidence that was destroyed would have an adverse effect on the party that destroyed the evidence and assume the interpretation of what the destroyed document contained by the opposing party is correct (Brown and Weiner, 2003). Many courts require corroborating evidence of spoliation before imposing an adverse inference on negligent spoliators (Turner v. Hudson Transit Lines, Inc., 1991). Courts have argued that it makes little difference whether the party willfully or negligently destroyed evidence, however, a “corroboration requirement is even more necessary where the destruction was merely negligent, since in those cases it cannot be inferred from the conduct of the spoliator that the evidence would even have been harmful to him.” (Turner v. Hudson Transit Lines, Inc., 1991).

3.1.4 The Cost of Complying with E-Discovery Requirements

The cost of discovery is usually borne by the producing party (Sedona Guidelines, 2005). However, Rule 26(b)(2)(C) states that “[T]he frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.” Courts have used this provision to order a cost shifting, or cost sharing between the requesting and producing parties. This approach is essentially one of weighing and balancing.

The leading case on this issue is, again, Zubulake v. UBS Warburg. Zubulake wanted an extensive e-discovery order to be issued for backed up email. UBS Warburg argued that the expense was an undue burden, in part, because of cost. The Court eventually ordered cost-splitting. The Court
evaluated the cost-splitting based upon a seven-factor test, developed by Judge Scheindlin. Each of the factors is weighed dependent upon its importance. The seven factors are:

1. The extent to which the request is specifically tailored to discover relevant information
2. The availability of such information from other sources
3. The total cost of production, compared to the amount in controversy
4. The total cost of production, compared to the resources available to each party
5. The relative ability of each party to control cost and its incentive to do so
6. The importance of the issues at stake in the litigation
7. The relative benefits to the parties of obtaining the information

Ultimately, the plaintiff was required to bear 25% of the cost associated with the restoration of backup tapes; the defendant would bear the remaining 75% of restoration cost, plus all other costs relating to searching and reviewing the restored emails (Jones, 2003).

4 RECOMMENDATIONS FOR AN ELECTRONIC RECORDS MANAGEMENT POLICY

The challenges confronting organizations in meeting e-discovery requirements underscores the necessity for proper ERM to reduce the complexity, time-consuming nature, and expense of the e-discovery process. Organizations need to address ERM for both every day operational purposes, and for compliance. Electronic data is often recycled or overwritten as part of routine business practices (Scheindlin and Wangkeo, 2004) because businesses simply cannot retain volumes of outdated information due to finite physical space and budgets. Moreover, records that have ceased to have operational or legal value, and that are retained unnecessarily, are subject to potential discovery (Launchbaugh, 2004). Therefore, it is important for organizations to have a comprehensive ERM policy. This policy should be enacted in good faith before there is a pending litigation. Built into the policy should also be a discovery response plan that contains policies and procedures for responding to discovery in a timely, responsible manner (Launchbaugh, 2004).

According to Kahn (2005), 80% of organizations have recently made or are planning to make changes in the way they manage information. A thorough ERM policy should meet the following criteria (Kiel et al., 2005):

1. Comply with statutory or regulatory obligations that govern different types of documents retained.
2. Specify the length of time that each type of document is retained.
3. Establish a method of destruction and a destruction schedule.
4. Provide a detailed protocol for halting routine destruction in the event of anticipated or actual litigation.

In an age where email is often a primary source of legal discovery, a survey found that 59% of organizations do not have a formal email retention policy (Winkler, 2005). It is imperative that email usage and content rules be established. The organization’s ERM policy should encompass email as well.

The ERM policy should address people, procedures, and technology solutions (Trend Micro, 2009). Employees and other individuals authorized to use organizational information, such as business partners and suppliers, should be educated and trained. Proper procedures must be put in place to enable employees to adhere to established policies in a workable manner that is integrated with their responsibilities. Technological solutions should be implemented to automate processes when possible. Further, technological solutions can be employed to support policies and facilitate training.
5 CONCLUSION

A challenge for organizations is to manage electronic information without exposing the organization to sanctions in a later lawsuit. Courts have struggled with the demands of e-discovery, and the issue of sanctions for intentional or unintentional failure to comply. The amendments to the FRCP are an attempt by the US legal system to address the issues of electronic records management as information technology continues to advance. Organizations must respond to the necessity to address ERM by developing and implementing a comprehensive policy, for compliance and litigation purposes. The policy is not absolute protection from sanctions, but at a minimum creates a credible defense. Further, if such a policy is automated, the recent amendments to the FRCP afford a higher level of protection from sanctions.

References


Texas A&M University. No Date. 'Electronic Discovery and Data Preservation Frequently Asked Questions.' available at http://security.tamu.edu/Information_Security/Security_for_Students/Know_the_Rules/Electronic_Disclosure_and_Data_Preservation.php?q1


Winkler D. 2005. 'E-mail Management: Compliance, control, consolidation.' Computer Technology Review (25:2), pp. 11-12.

