E-Discovery: The Intersection of Law, Technology and Business

Dr. Ian J. Redpath, Dr. Linda Volonino

It is estimated that over 95 percent of all business information is electronically stored (referred to as electronically stored information, or ESI). In the “pre-technology” environment, information was prepared on paper and stored in cabinets and boxes. These formats have been replaced with information stored on servers, laptops, flash drives, smartphones, other handheld devices, and numerous other storage media. With the United States one of the most litigious societies, the legal need to obtain ESI as either a defendant or a plaintiff is inevitable. Additionally, there may be a need to produce it by third party vendors such as Verizon, Sprint, Facebook, or Yahoo if they have ESI relevant to a case.

E-discovery (electronic discovery) is the term used to describe the legal process of discovering the ESI that is relevant to a case. The costs of ESI can run in the hundreds of thousands of dollars and there may be hundreds of thousands of documents produced with only a handful actually used in court. Businesses must know what ESI they have, where it is, and how to find it. Being unprepared for e-discovery can result in large monetary penalties or, in the extreme, losing the case. This paper addresses the common issues relevant to e-discovery and what businesses need to do to prepare in anticipation of litigation.

INTRODUCTION

Traditionally, businesses had kept their records on paper with the result being warehouses full of boxes of information. Currently approximately 95 percent of all documents generated by businesses are created electronically (Evangelista, 2004). About one-third of those electronically-created documents are never reduced to paper (Oostenrijk, 2005). This transition from paper to digital records has changed the discovery process.
Discovery is the investigative stage of litigation during which the parties attempt to obtain evidence relevant to their cases. Today, discovery has become e-discovery. Information has become ESI. And evidence is now e-evidence (electronic evidence).

Businesses have been inundated with litigation, both civil and criminal, in which electronic information has been crucial to the outcome. There is a seemingly never ending and ever evolving burden of determining what evidence there is and where it is located. This burden generally falls on the party required to produce the evidence. Documents may be generated and/or stored in multiple locations or forms such as the hard drives of laptops, servers, and e-readers (e.g., iPad); the flash drives of smartphones and personal digital assistants (PDA); and backup tapes. The list continues to expand.

Most cases are settled during discovery without the necessity of a trial. If discovery is conducted properly, a trial attorney will be able to assess the strength and weakness of his/her case and the dangers of proceeding to trial. When all relevant evidence is known before trial, the evaluation of the merits of the case is simplified. Until 2006, the Federal Rules of Civil Procedure (FRCP, 2006) were written based on paper-based discovery. The rules did not address the discovery of electronically stored information, or ESI. In 2006, the rules were amended to specifically address ESI discovery and e-discovery was born.

The cost of finding the “digital smoking gun” can be significant. The 2007 case of Seven Network Ltd v News Ltd. can be viewed as a warning as to what can happen when e-discovery gets out of control. The Judge attempted to limit what he referred to as an “astonishing” discovery process. The matter lasted five years, with costs exceeding $200 million. Judge Ronald Sackville noted:

“The outcome of the process of discovery and production of documents in this case was an electronic database containing 85,653 documents, comprising 589,392 pages. Ultimately, 12,849 documents,
comprising 115,586 pages were admitted into evidence. The exhibit list would have been very much longer had I not rejected the tender of substantial categories of documents that the parties, particularly Seven, wished to have in evidence.” (Seven, 2007)

The Judge ultimately dismissed the claims of the plaintiff.

**Federal Rules of Civil Procedure (FRCP)**

The Federal Rules of Civil Procedure can be looked at as the rulebook for playing the game of e-discovery. In April 2006, the United States Supreme Court approved amendments to the FRCP effective December 2006. E-discovery is now a reality that must be addressed in all litigation, big and small.

**Rule 1**

In all discovery, there is an overriding principle set forth in FRCP Rule 1. It is often overlooked because of its simplicity. However, it sets forth a clear statement of the purpose of the rules, which is: “to secure the just, speedy and inexpensive determination of every action” (FRCP 1). The general rule for discovery is that the party producing the information must bear the costs.

**Rule 26(a)**

Parties to litigation have a positive duty under FRCP Rule 26(a) to either provide a copy or a categorical description and location of any ESI that may be used to support the parties’ claims or defenses. This is a mandate without the need for a request from the other party. It reduces costs and is imposed on all parties to the litigation. The emphasis is on relevance. *Relevance* is defined by the Federal Rules of Evidence (FRE) Rule 401 as evidence having the tendency to make the existence of a fact more or less probable. In other words, that something of consequence to the case did or did not happen.
Rules 34(a) and 34(b)
Rule 34(a) of the FRCP specifically extended the scope of discovery to electronically stored information. 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.

This rule is supplemented by FRCP Rule 34(b), which allows a party to request the form in which ESI is to be produced. A party may also ‘inspect, copy, test or sample the other parties’ ESI. If you are the responding party, you may object to the requested form and tell them the form you intend to use. You must “translate” ESI into a “reasonably useable form.” If no form is requested, then the form defaults to one of the following:

- the form in which the ESI is ordinarily maintained
- a form that is reasonably useable.

Rule 26(b)
Rule 26(b) of the FRCP creates a two-tier classification to electronically stored information. Rule 26(b)(2)(B) states that:

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 amended FRCP creates two categories of ESI: reasonably accessible, and not reasonably accessible. However, neither the Rule nor the FRCP Advisory Committee’s Report defines these terms. The Committee only gives examples of costly or burdensome retrieval, e.g., “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). Similar rules apply to non-parties under FRCP Rule 45.

**Zubulake v. UBS Warburg (2003)**

The Rule’s standard is “not reasonably accessible because of undue burden or cost.” This vague standard without definition requires that guidance come from judicial precedent. The seminal case on this issue is **Zubulake v. UBS Warburg (2003)**. *Zubulake* was an employment discrimination case. In discovery, plaintiff requested older e-mail messages. 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. Scheindlin identified five categories of ESI:

- **Active, online data**: This type of data is in an “active” stage in its life and is available for access as it is created and processed. Storage examples include hard drives or active network servers.
- **Near-line data**: This type of data is typically housed on removable media, with multiple read/write devices used to store and retrieve records. Storage examples include optical discs and magnetic tape.
- **Offline storage and archives**: This represents data on removable media that have been placed in storage. Offline storage of electronic records is traditionally used for disaster recovery or for
records considered “archival” in that their likelihood of retrieval is minimal.

- **Backup tapes:** Data stored on backup tapes isn’t 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. Data stored on backup tapes is also typically compressed, allowing storage of greater volumes of data, but also making restoration more time consuming and expensive.

- **Erased, fragmented, or damaged data:** This type of data has been tagged for deletion by a computer user, but may still exist somewhere on the free space of the computer until it’s overwritten by new data. Significant efforts are required to access this data.

The first three types of ESI are considered to be *accessible*, and the last two types are considered *not reasonably accessible*. For reasonably accessible ESI, the usual rules of discovery apply, namely that the responding party pays for production. When not reasonably accessible ESI is at issue, the judge may still order that it be produced, but may shift costs to the requesting party. If the party wants it, they can pay for its discovery.

**Rule 26(b)(1) and Disclosure**

Disclosure is an on-going requirement. All pre-trial disclosures are due within 30 days of the trial date and the other party has 14 days to object. Failure to object could result in a waiver of objections for trial purposes. Generally under Rule 26(b)(1) you can discover any nonprivileged matter relevant to your claim or defense. However, if you can demonstrate that the ESI is “not reasonably accessible because of undue burden or cost” the ESI may not have to be produced or the court may shift the costs of production.

**Rule 26(f)**

FRCP Rule 26(f) is one of the most important aspects of e-discovery. At the meet-and-confer session, opposing parties are to cooperate to make
e-discovery less costly, fair and expedient. At this session or other sessions, the parties attempt to work out a plan of discovery for both what they want and how it can be produced.
E-DISCOVERY TIMELINE

In paper discovery and prior to December 1, 2006, the time frame for discovery began when the suit was filed. Not so for e-discovery. The time frame for discovery can be looked at as:

- **Time minus zero: Duty to preserve.** You need to take affirmative action—active and timely measures—to prevent the destruction or alteration of what might be relevant e-evidence. This duty generally begins when a legal action is reasonably anticipated. That’s a tough duty to comply with. Clairvoyance would be helpful since the scope of what needs to be preserved and as of when are not clear. Accept the fact that it’s difficult under the best of circumstances to know when a duty to preserve has triggered or what to preserve. Regardless, the courts consistently require counsel to be aware of these issues, and to have guided their clients appropriately in regard to the duty to preserve ESI.

- **Day 1: Complaint served.** You’re on solid ground here since there’s no mistaking that a lawsuit is in play. When the lawsuit is filed and complaint is served on the defendant, it starts a clock that counts off days, although sometimes you need to count backwards.

- **By Day 99: Meet and Confer conference.** The meet and confer conference is also a duty. Litigants must participate in a meet and confer conference to negotiate an e-discovery plan. The list of topics to negotiate include the following:
  - Any issues relating to preserving discoverable ESI.
  - Any issues relating to search, disclosure, or discovery of ESI.
  - Format in which ESI should be produced.
  - Scope of ESI holdings
  - Estimated ESI production costs in terms of difficulty, risk, time, and money.

The timeframe is established by FRCP 16(b).
Agreements made at the meet and confer and that are listed in Form 35 need to be conducted. Form 35 was amended by the new FRCP to include a report to the court about any agreements that the parties have reached.

- **By Day 120: Scheduling conference.** A scheduling conference is a hearing attended by the prosecuting attorneys, defendants, defendant’s attorneys, and the judge to schedule certain dates and deadlines for the case. This event is generally the first time the litigants and their attorneys come before the Court. (Volonino and Redpath at 19)

The rules are supplemented by other sources such as the Sedona Conference (Sedona) and Electronic Discovery Reference Model (EDRM). While not the law these are good sources in interpreting the rules. The EDRM model is:

**DUTY TO PRESERVE AND SPOLIATION**

The duty to preserve is triggered when litigation can be “reasonably anticipated” (Zubulake and Sedona). It is therefore not triggered by the filing of a lawsuit but by anticipation that there may be litigation. Violating a duty to preserve may result in what is called an adverse inference or even a termination sanction. An adverse inference is an instruction from the judge to the jury that the failure of a party to produce certain ESI was because it would have been adverse to them. A termination sanction can result in losing the case. This would only be done in the most egregious situations.

**Preservation**

The purpose of the preservation duty is clear. Parties that anticipate litigation should not be able to purposely destroy evidence that may be unfavorable to them. This is often referred to as a litigation hold. Clearly the standard should not be a duty to preserve only when the case is actually
filed. It is important that a preservation letter is sent upon anticipation of litigation. This letter must indicate to all parties and non-parties that may have relevant ESI not to destroy it and to preserve it. It may be necessary that a computer be taken out of service until a forensic or preservation image can be created.

**Spoliation, Safe Harbor, and Rule 37**

Spoliation 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,” (Watson, 2004). Spoliation can encompass four distinct torts (O’Hara and Gennaro, 2004):

1. Intentional spoliation by a party to underlying litigation
2. Negligent spoliation by a party to underlying litigation
3. Intentional spoliation by a third party not a party to underlying litigation
4. Negligent spoliation by a third party not a party to underlying litigation

Often common practices can cause spoliation, for example, deleting e-mails and documents from the system. “The fact of deletion can lead
to a court’s imposing serious sanctions for attempting to destroy relevant evidence” (Benson, 2004) if it was after the duty to preserve began. Parties can be sanctioned for spoliation under Rule 37 of the FRCP or through a court’s inherent power to oversee case management.

One problem area is the destruction of ESI through routine operation of the system of a valid document retention policy. FRCP Rule 37(e) provides a safe harbor that the court cannot impose sanctions for failing to produce ESI that you’ve lost from routine, good-faith operation of the system. Rule 37(e) provides:

Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.

**Good Faith**

Good faith is crucial. When litigation is anticipated, you have a duty to hold the ESI and preserve it. Steps must be taken to avoid any destruction of the ESI, even if by routine operation. If the ESI is not available, the courts look to determine whether you’ve destroyed it by routine operation. It is important that a company have a data retention policy in place under its records and information management (RIM) and also that it complies with it. The company should instruct its employees to cease any destruction of documents and take steps to assure that its system will not destroy any relevant ESI. Business must maintain a good RIM program and be able to assess what it has and where it is. A relevant document may be on a laptop of an employee or could be on a cell phone of an employee who has been terminated. That does not change the duty to find it and preserve it.

A LiveOffice survey, conducted by Osterman Research in 2007 (Osterman, 2007), polled more than 400 IT managers and users. According to the results, 63 percent of respondents had faced a legal action requiring them to produce e-mail. Fifty three percent said they weren’t prepared to meet the amended FRCP, while 30 percent weren’t even aware of the FRCP requirements.
A business needs a defensible electronic records management (ERM) as part of its overall RIM program. Records management, either paper or electronic, includes the creation, retention, continued access, and discarding and destruction of business records. The cornerstone of a defensible ESI management system and e-discovery protocol is a well-designed (reasonable, in legalese) ERM policy and program. ERM policies and programs do double-duty in terms of managing the likelihood and the impact of litigation risk. They do the following:

- Minimize or reduce risk associated with the case. You’ve heard the cliché that information is power. Against your opponent in a lawsuit, you don’t have much else. ESI is the negotiating tool or bargaining chip—a situation that moved ERM from a back-office task to a business-critical function for which IT has a major responsibility. ERM helps prevent the risk of not being able to prepare a powerful position for the meet and confer. Or not being able to show your opponent that you’re ready to respond to whatever they throw at you.
- Transfer or offset risk associated with the court. ERM helps minimize the risk associated with not being able to fulfill the duty to preserve when litigation strikes or is reasonably foreseeable. Taking early preventative measures by implementing an ERM designed with e-discovery in mind saves you legal grief down the road. Risk skyrockets for companies with sloppy prelitigation ERM practices. Having a rock solid ERM program is like insurance to offset risk. When challenged, you have the ERM defense to save your hide. (Volonino and Redpath, 2009)

In determining sanctions for spoliation, the courts will take a four-step analysis:

- Was the conduct of discovery acceptable or was it grossly negligent or willful?
- What was the interplay between the duty to preserve and the spoliation?
Which party should bear the burden of proving that the evidence has been lost or destroyed and the consequences of that loss? and
What is the appropriate remedy? (Pension Committee, 2010)

As noted by Judge Scheindlin in Pension Committee, it is a continuum of fault. The further along the continuum the greater the possible sanctions. Termination sanctions should be left to only the most egregious cases. The Qualcomm case (Qualcomm, 2008) is one such case. The court ordered Qualcomm to pay $8.5 million to Broadcom for legal fees incurred as a result of misconduct of Qualcomm in e-discovery.

Rule 30(b) Witness
In order to reduce costs and the need for multiple and probably duplicative witnesses, FRCP Rule 30(b) allows a company to designate a person to serve as a witness on ESI matters. It is imperative that this person be educated on the ESI issues so that her/she may properly be deposed on technology and practice issues. Among other things they should know:

- Which files were searched,
- How the search was conducted,
- Who conducted the search,
- What was told about the ESI being requested and
- The extent and nature of the supervision of those conducting the search.

Protecting Privileged, Protected and Confidential ESI

Certain types of communications/ESI do not have to be produced. The law recognizes both privilege and work product protection. The court may also protect certain confidential information such as trade secrets.

A communications privilege is meant to protect certain relationships as developed under common law. FRE 501 allows the courts to apply
common law and reason in establishing privileges. As a result, courts may differ in what they consider privileged information. Although state rules may differ from federal rules, generally, privileges apply to communications in these types of relationships:

- **Attorney–Client:** If you talk to your attorney about a legal matter, you should be able to expect that the conversation is confidential and not be used against you. If these discussions were allowed to be used in court, it would hinder the ability of attorneys to prepare cases with clients who were afraid or reluctant to be candid. The wheels of justice would get jammed.

- **Physician/Psychotherapist–Client:** Communications with a doctor that relate to diagnosis or treatment of a physical, mental, or emotional condition are covered by the privilege.

- **Husband–Wife:** Communications that were intended to be confidential and made during the marriage are considered part of the sanctity of marriage and have a privilege.

- **Religious Leader–Follower:** If you communicate in confidence to a clergyman, that communication is protected by privilege. Confidence, for this purpose, means that the communication was made privately and was not intended to be told to anyone else.

- **Accountant–Client:** Some states recognize this privilege as similar to the attorney-client privilege. However, the federal government recognizes it only in a very narrow privilege in IRS matters, a situation almost never available in third-party actions.

- **Self-Incrimination:** If a person is under a reasonable apprehension that they may be subjected to a criminal action and that what they are being asked to produce may tend to incriminate them then it need not be produced. It applies only to testimonial evidence and generally doesn’t apply to business entities to the same degree as individuals. (Volonino and Redpath at 168–169)

The United States Supreme Court in *Hickman v. Taylor* (1947), recognized that certain trial preparation materials should be protected under
the work product doctrine. These are materials that reveal your attorney’s strategy and may include evaluations of your case’s strength or weakness, reflections from interviews of witnesses, tactics, or similar information. Work product is not privileged within the meaning of the FRE, but it is safeguarded by FRCP 26(b)(3) and FRCP 45(d)(2), which grants protection to documents and tangible things that meet two criteria:

- They are prepared in anticipation of litigation or for trial.
- They are created by or for a party or its representative. (Volonino and Redpath at 169)

Work product may still be subject to e-discovery if two conditions are met:

- The material is otherwise discoverable under the FRCP or FRE.
- Your opponent shows a substantial need for the materials to prepare his case, and you cannot obtain the material by alternate means without undue hardship. This means that the information sought is essential to your opponent and crucial to the case. (Volonino and Redpath at 169)

The court with an order of protection may protect trade secrets and proprietary information. To invoke protection a business will have to show the economic loss if it is produced and that it is either not relevant or its probative value is outweighed by the potential injury if disclosed.

1. **Verify that the ESI is a trade secret or proprietary research.**
   You do this by:
   - Determining the value of the ESI both to the company and in the market (that is, internally and externally).
   - Evaluating how easy it would be for someone to duplicate your trade secret or proprietary research.
• Estimating the amount of time and effort that you spent in development.
• Identifying the level of disclosure within your business and the measures taken to protect the information.

2. **Assert that the ESI is a trade secret or proprietary research.**
   You do this by proving that:
   • The information has separate economic value.
   • You have made an effort to maintain its secrecy. (Volonino and Redpath at 170).

This protection is not automatic and is at the discretion of the judge. The rules provide protection for ESI that is inadvertently disclosed provided the disclosing party takes appropriate steps. In fact, FRE 502 states that in a federal action, privileged or protected ESI that is inadvertently disclosed may be used for any purpose even in other actions. This same rule may not be available in a state action not covered by the Federal Rules.

**Costs Allocations Associated with e-Discovery**

The court may limit relevant information if what is requested is duplicative or the cost of production is prohibitive. As mentioned earlier, FRCP Rule 26(b) establishes a “not reasonably accessible standard”. The courts may shift the costs of production if the party still wants it. The court may also shift the cost of production as a sanction for e-discovery misconduct. The costs of production may be significant. Just some examples:

• In 2002, in *Murphy Oil v. Fluor Daniel*, Fluor Daniel spent $6.2 million to restore and print e-mail from 93 backup tapes.
• In 2002, in *Rowe Entertainment v. William Morris Agency*, the William Morris Agency spent $9.7 million to restore e-mail from 200 tapes, in addition to hundreds of thousands dollars to retrieve and review 250,000 e-mail messages.
To illustrate the cost of dealing with offline ESI, in *Bank of America Corp. v. SR Int’l Bus. Ins. Co.* (Nov. 1, 2006), the restoration and organization of e-mail data from 400 backup tapes was estimated at $1.4 million.

In *Disability Rights Council of Greater Washington v. Washington Metro Transit Authority* (June 1, 2007), the defendant failed to stop automatic purging of e-mails for three years after the complaint was filed.

It must also be remembered that the party producing may be a third party such as an e-mail provider or cell phone company.

One of the assertions that may be made to avoid production is that it would create an undue burden. Costs are often cited as being the undue burden for not reasonably accessible. This issue may also be raised as a matter of proportionality. The *proportionality issue* allows courts to limit or shift costs when the costs of discovery could exceed the possible verdict. This can help avoid the use of discovery to force settlement by making it too costly for the other side to continue the case or not settle.

The cost of discovery is usually borne by the producing party. 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 parties. Allocating e-discovery costs to the parties requires a weighing and balancing of the facts to determine fairness in the production of evidence.
In *Zubulake*, the plaintiff Zubulake wanted an extensive e-discovery order to be issued for backed up email. The other side cited undue burden as a result of cost. The Court eventually ordered cost-splitting. The Court applied 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 of restoring back-up tapes and the defendant the remaining 75% of the cost associated with restoration, search, and review.

**Conclusion**

It is safe to say that the FRCP places a burden on companies to be sure that their IT experts become legally savvy and their attorneys become IT savvy whenever litigation can be reasonably anticipated. As technology advances, the law must adjust to meet the new environment. The costs associated with the new world of e-discovery can be outrageously high. Often companies hire outside vendors for their e-discovery technology and legal needs because they lack the expertise or ability. This ever-changing area is a hazardous minefield for businesses that are not litigation-ready. All businesses, large and small, need to assess their exposure and develop preemptive plans to address what has become inevitable litigation. There is much to be lost unless parties are prepared for and knowledgeable in e-discovery.
REFERENCES


Federal Rules of Evidence, as in effect 2010.


*Qualcomm v Broadcom*, Slip Copy, 2008 WL 638108 (S.D.Cal.)


The Intersection of Law, Technology and Business

Seven Network Ltd. v News Ltd., FCA 1062 2007.

The Pension Committee of the University of Montreal Pension Plan et al. v Banc of America Securities LLC etc al., No. 05 Civ. 9016 (SAS) (S.D.N.Y. Jan. 15, 2010).

