Unit 4: Electronics Discovery: An Introduction

4

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- Legal basis of electronic discovery
- ESI preservations: Obligations and Penalties
- Utilizing criminal procedure to accentuate E-discovery

1.2 INTRODUCTION

Electronic discovery or "e-discovery" is the exchange of data between parties in civil or criminal litigation. The process is largely controlled by attorneys who determine what data should be produced based on relevance or withheld based on claims of privilege. Forensic examiners, however, play crucial roles as technical advisors, hands-on collectors, and analysts.

Some examiners view electronic discovery as a second-class endeavour, void of the investigative excitement of a trade secret case, an employment dispute, or a criminal "whodunit." These examiners, however, overlook the enormous opportunities and challenges presented by electronic discovery.[31]

In technical terms, electronic discovery also poses a variety of daunting questions: Where are all the potentially relevant data stored? What should a company do to recover data from antiquated, legacy systems or to extract data from more modern systems like enterprise portals and cloud storage? Does old data need to be converted? If so, will the conversion process result in errors or changes to important metadata? Is deleted information relevant to the case? What types of false positives are being generated by keyword hits? Did the tools used to process relevant data cause any errors or omissions in the information produced to lawyers? What file server data can be attributed to specific custodians? How can an examiner authenticate database reports? What can an examiner do to fill in the gaps after the e-mail has been erroneously deleted?

Confusion over terminology between lawyers, forensic examiners, and laypeople add to the complexity of e-discovery. For instance, a forensic examiner may use the term "image" to describe a forensic duplicate of a hard drive, whereas an IT manager may call routine backups an "image" of the system, and a lawyer may refer to a graphical rendering of a document (e.g., in TIFF format) as an "image." These differing interpretations can lead to misunderstandings and major problems in the e-discovery process, adding frustration to an already pressured situation. George Socha and Thomas Gelbman have created a widely accepted framework for e-discovery consulting known as the Electronic Discovery Reference Model (EDRM). The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;
b) Associate document collections with particular users (custodians);
c) Capture and preserve the metadata associated with the electronic files within the collections;
d) Establish the parent-child relationship between the various source data files;
e) Automate the identification and elimination of redundant, duplicate data within the given dataset;

[31] Stander, Adrie & Val, Kevin & Hooper, Val (2015). Ediscovery in South Africa and the Challenges it Faces

f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;
g) Unprotect and reveal information within files; and
h) Accomplish all of these goals in a manner that is both defensible with respect to clients' legal obligations and appropriately cost-effective and expedient in the context of the matter.[32]

1.3 LEGAL BASIS FOR ELECTRONIC DISCOVERY

In civil litigation throughout the United States, courts are governed by their respective rules of civil procedure. Each jurisdiction has its own set of rules, but the rules of different courts are very similar as a whole.1 As part of any piece of civil litigation, the parties engage in a process called discovery. In general, discovery allows each party to request and acquire relevant, nonprivileged information in possession of the other parties to the litigation, as well as third parties (F.R.C.P. 26(b)). When that discoverable information is found in some sort of electronic or digital format (i.e., hard disk drive, compact disc, etc.), the process is called electronic discovery or e-discovery for short.

The right to discover ESI is now well established. On December 1, 2006, amended F.R.C.P. went into effect and directly addressed the discovery of ESI. Although states have not directly adopted the principles of these amendments en masse, many states have changed their rules to follow the 2006 F.R.C.P. amendments.

In ***Coleman vs Morgan Stanley***[33]**,** after submitting a certificate to the court stating that all relevant e-mail had been produced, Morgan Stanley found relevant e-mail on 1600 additional backup tapes. The judge decided not to admit the new e-mail messages, and based on the company's failure to comply with e-discovery requirements, the judge issued an "adverse inference" to the jury, namely that they could assume Morgan Stanley had engaged in fraud in the underlying investment case. As a result, Morgan Stanley was ordered to pay $1.5 billion in compensatory and punitive damages. An appeals court later overturned this award, but the e-discovery findings were left standing, and the company still suffered embarrassing press like The

[32] Arkfeld, M R (2005), Electronic Discovery and Evidence, Law Partner Publishing, LLC, Phoenix, AZ
[33] *Coleman v Morgan Stanley* 20 So 3d 952 (Fla Dist Ct App) [2009]

Wall Street Journal article, "How Morgan Stanley botched a big case by fumbling e-mails" (Craig, 2005).

1.4 ESI PRESERVATION: OBLIGATIONS AND PENALTIES

Recent amendments to various rules of civil procedure require attorneys—and therefore digital examiners—to work much earlier, harder, and faster to identify and preserve potential evidence in a lawsuit. Unlike paper documents that can sit undisturbed in a filing cabinet for several years before being collected for litigation, many types of ESI are more fleeting. Drafts of smoking-gun memos can be intentionally or unwittingly deleted or overwritten by individual users, server-based e-mail can disappear automatically following a systematic purge of data in a mailbox that has grown too large, and archived e-mail can disappear from backup tapes that are being overwritten pursuant to a scheduled monthly tape rotation.[34]

The seminal case of ***Zubulake v. UBS Warburg***[35] outlined many ESI preservation duties in its decision. Laura Zubulake was hired as a senior salesperson to UBS Warburg. She eventually brought a lawsuit against the company for gender discrimination, and she requested, "all documents concerning any communication by or between UBS employees concerning Plaintiff." UBS produced about 100 e-mails and claimed that its production was complete, but Ms. Zubulake's counsel learned that UBS had not searched its backup tapes. What began as a fairly mundane employment action turned into a grand e-discovery battle, generating seven different opinions from the bench and resulting in one of the largest jury awards to a single employee in history.[36]

The court stated that "a party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents created thereafter," and outlined three groups of interested parties who should maintain ESI:

---

[34] Carrier, B. 'Open Source Digital Forensics Tools: The Legal Argument', @stake Research Report, October 2002

[35] *Zubulake v UBS Warburg* 217 F R D 309 (S D N Y) [2003]

[36] Federal rules of evidence. Available online at <www.law.cornell.edu/rules/fre/rules.htm>

- **Primary players:** Those who are "likely to have discoverable information that the disclosing party may use to support its claims or defenses" (F.R.C.P. 26(a)(1)(A)).
- **Assistants to primary players:** Those who prepared documents for those individuals that can be readily identified.
- **Witnesses:** The duty also extends to information that is relevant to the claims or defenses of any party, or which is 'relevant to the subject matter involved in the action'" (F.R.C.P. 26(b)(1)).

The Zubulake court realized the particular difficulties associated with retrieving data from backup tapes and noted that they generally do not need to be saved or searched, but the court noted:

"It does make sense to create one exception to this general rule. If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of "key players" to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes".[37]

In addition to clarifying the preservation obligations in e-discovery, the Zubulake case revealed some of the penalties that can befall those who fail to meet these obligations. The court sanctioned UBS Warburg for failing to preserve and produce e-mail backup tapes and important messages, or for producing some evidence late. The court required the company to pay for additional depositions that explored how data had gone missing in the first place. The jury heard testimony about the missing evidence and returned a verdict for $29.3 million, including $20.2 million in punitive damages.

The Zubulake court held the attorneys partially responsible for the lost e-mail in the case and noted, "It is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." (Zubulake v. UBS Warburg, 2004). Increasingly, attorneys have taken this charge to heart and frequently turn to their digital examiners to help assure that their discovery obligations are being met.

[37] Magic Quadrant for E-Discovery Software, Gartner, 2014

1.5 DETERMINING VIOLATIONS OF THE ELECTRONIC DISCOVERY PARADI

As pointed out by the Zubulake decision, the consequences of failing to preserve data early in a case can be severe. Under F.R.C.P. Rule 37, a court has broad latitude to sanction a party in a variety of ways. Of course, courts are most concerned about attorneys or litigation parties that intentionally misrepresent the evidence in their possession, as seen in the Qualcomm case.[38]

The following 10 recommendations are provided for investigators and in-house counsel to avoid the same fate as Qualcomm (Roberts, 2008):

a) Use checklists and develop a standard discovery protocol;
b) Understand how and where your client maintains paper files and electronic information, as well as your client's business structures and practices;
c) Go to the location where information is maintained—do not rely entirely on the client to provide responsive materials to you;
d) Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;
e) Ask all witnesses about other potential witnesses and where and how evidence was maintained;
f) Use the right search terms to discover electronic information;
g) Bring your own IT staff to the client's location and have them work with the client's IT staff, employ e-discovery vendors or both;
h) Consider entering into an agreement with opposing counsel to stipulate the locations to be searched, the individuals whose computers and hard copy records are at issue, and the search terms to be used;
i) Err on the side of production;
j) Document all steps are taken to comply with your discovery protocol.

This is a useful and thorough set of guidelines for investigators to use for preservation of data issues, and can also serve as a quick factsheet in preparing for depositions or testimony.

[38] Computer Technology Review, Sharon Isaacson, March 2003

1.6 ASSESSING WHAT DATA IS REASONABLY ACCESSIBLE

Electronic discovery involves more than the identification and collection of data because attorneys must also decide whether the data meets three criteria for production. Namely, whether the information is (1) relevant, (2) nonprivileged, and (3) reasonably accessible (F.R.C.P. 26(b)(2)(B)). The first two criteria make sense intuitively. Nonrelevant information is not allowed at trial because it simply bogs downs the proceedings, and withholding privileged information makes sense in order to protect communications within special relationships in our society, for example, between attorneys and clients, doctors and patients, and such. Whether information is "reasonably accessible" is harder to determine, yet this is an important threshold question in any case.[39]

In the Zubulake case described earlier, the employee asked for "all documents concerning any communications by or between UBS employees concerning Plaintiff," which included "without limitation, electronic or computerized data compilations," to which UBS argued the request was overly broad. In that case, Judge Shira A. Scheindlin, United States District Court, Southern District of New York, identified three categories of reasonably accessible data: (1) active, online data such as hard drive information, (2) near-line data to include robotic tape libraries, and (3) offline storage such CDs or DVDs. The judge also identified two categories of data generally not considered to be reasonably accessible: (1) backup tapes and (2) erased, fragmented, and damaged data. Although there remains some debate about the reasonable accessibility of backup tapes used for archival purposes versus disaster recovery, many of Judge Scheindlin's distinctions were repeated in a 2005 Congressional report from the Honorable Lee H. Rosenthal, Chair of the Advisory Committee on the Federal Rules of Civil Procedure (Rosenthal, 2005), and Zubulake's categories of information remain important guideposts (Mazza, 2007).[40]

The courts use two general factors—burden and cost—to determine the accessibility of different types of data. Using these general factors allows the courts to take into account the challenges of

[39] Ward, Burke and Sipior, Janice and Hopkins, Jamie and Purwin, Carolyn and Volonino, Linda, Electronic Discovery: Rules for a Digital Age (February 27, 2011) Boston University Journal of Science and Technology Law, Vol. 18, No. 150, 2012

[40] Friedberg, E, & McGowan, M (2003). Electronic discovery technology. In A Cohen & D. Lender (Eds.), Electronic discovery: Law and practice, Aspen Publishers

new technologies and any disparity in resources among parties (Moore, 2005). If ESI is not readily accessible due to burden or cost, then the party possessing that ESI may not have to produce it (see F.R.C.P. 26(b)). Some parties, however, make the mistake of assessing the burden and cost on their own and unilaterally decide not to preserve or disclose data that is hard to reach or costly to produce. The rules require that a party provide "a description by category and locations, of all documents" with potentially relevant data, both reasonably and not reasonably accessible (F.R.C.P. 26(a)(1)(B)). This allows the opposing side a chance to make a good cause showing to the court why that information should be produced (F.R.C.P. 26(a)(2)(B)).

1.7 UTILIZING CRIMINAL PROCEDURE TO ACCENTUATE E-DISCOVERY

In some cases, such as lawsuits involving fraud allegations or theft of trade secrets, digital examiners may find that the normal e-discovery process has been altered by the existence of a parallel criminal investigation. In those cases, digital examiners may be required to work with the office of a local US Attorney, State Attorney General, or District Attorney, since only these types of public officials, and not private citizens, can bring criminal suits.[41]

A criminal agency can preserve data early in an investigation by issuing a letter under 18 U.S.C. 2703(f) to a person or an entity like an Internet Service Provider (ISP). Based on the statute granting this authority, the notices are often called "f letters" for short. The letter does not force someone to produce evidence but does require they preserve the information for 90 days (with the chance of an additional 90-day extension). This puts the party with potential evidence on notice and buys the agency some time to access that information or negotiate with the party to surrender it.[42]

Another less popular method of obtaining evidence is through a court "d" order, under 18 U.S.C. §2703(d). This rule is not used as often because an official must be able to state with "specific and articulately" facts that there is a reasonable belief that the targeted information is pertinent to

[41] See Jonathan M Redgrave & Kristin M. Nimsger, Electronic Discovery and Inadvertent Productions of Privileged Document, THE FED. LAWYER, July 2002, at 37, available at <http://www.jonesday.com/files/>
[42] Kidwell, B, Neumeier, M, & Hansen, B (2005) Electronic discovery. Law Journal Press

the case. However, this method is still helpful to obtain more than just subscriber information—data such as Internet transactional information or a copy of a suspect's private homepage.

There are five digital storage locations that are the typical focus of e-discovery projects (Friedberg & McGowan, 2006):

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB "thumb" drives
- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

Although these storage locations are the typical focus of e-discovery projects, especially those where the data are being collected in a corporate environment, examiners should be aware of other types of storage locations that may be relevant such as digital media players and data stored by third parties (for example, Google Docs, Xdrive, Microsoft SkyDrive, blogs, and social networking sites such as MySpace and Facebook).

Informational interviews and documentation requests are the core components of a comprehensive and thorough investigation to identify the potentially relevant ESI in these five locations, followed by review and analysis of the information obtained to identify inconsistencies and gaps in the data collected. In some instances a physical search of the company premises and off-site storage is also necessary.

1.8 LET'S SUM UP

The e-discovery field is complex, and the technical and logistical challenges routinely found in large e-discovery projects can test even the most experienced digital forensic examiner. The high stakes nature of most e-discovery projects leave little room for error at any stage of the process—from initial identification and preservation of evidence sources to the final production and presentation of results—and to be successful, an examiner must understand and be familiar with their role at each stage. The size and scope of e-discovery projects require effective case

management, and essential to effective case management is establishing a strategic plan at the outset, and diligently implementing constructive and documented quality assurance measures throughout each step of the process.

1.9 FURTHER READING

- ACPO. (2008). The Good Practice Guide for Computer-based Electronic evidence. (4th ed.). Available online at www.7safe.com/electronic_evidence/
- Craig, S. (2005). How Morgan Stanley botched a big case by fumbling emails. The Wall Street Journal, A1.
- Mazza, M., Quesada, E., & Sternberg, A. (2007). In pursuit of FRCP1: Creative approaches to cutting and shifting the costs of discovery of electronically stored information, 13 Rich. J.L. & Tech., 11, 101.
- Howell, B. (2009). Lawyers on the Hook: Counsel's professional responsibility to provide quality assurance in electronic discovery. Journal of Securities Law, Regulation & Compliance, 2(3).
- Sedona Conference. (2008). "Jumpstart Outline": Questions to ask your client and your adversary to prepare for preservation, rule 26 obligations, court conferences and requests for production, May 2008. Available online at www.thesedonaconference.org/dltForm?did=Questionnaire.pdf.

1.10 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1) What is the meaning of E-discovery?

Electronic discovery or "e-discovery" is the exchange of data between parties in civil or criminal litigation.

2) What are the objectives of EDRM?

The Electronic Discovery Reference Model outlines the objectives of the processing stage, which include:

a) Capture and preserve the body of electronic documents;

b) Associate document collections with particular users (custodians);
c) Capture and preserve the metadata associated with the electronic files within the collections;
d) Establish the parent-child relationship between the various source data files;
e) Automate the identification and elimination of redundant, duplicate data within the given dataset;
f) Provide a means to programmatically suppress material that is not relevant to the review based on criteria such as keywords, date ranges or other available metadata;
g) Unprotect and reveal information within files; and
h) Accomplish all of these goals in a manner that is both defensible with respect to clients' legal obligations and appropriately cost-effective and expedient in the context of the matter.

3) Write any 3 recommendations that are provided for investigators and in-house counsel to avoid the same fate as Qualcomm?

- Use checklists and develop a standard discovery protocol;
- Go to the location where information is actually maintained—do not rely entirely on the client to provide responsive materials to you;
- Ensure you know what steps your client, colleagues, and staff have actually taken and confirmed that their work has been done right;

4) What are the five digital storage locations?

- Workstation environment, including old, current, and home desktops and laptops
- Personal Digital Assistants (PDAs), such as the BlackBerry® and Treo®
- Removable media, such as CDs, DVDs, removable USB hard drives, and USB "thumb" drives
- Server environment, including file, e-mail, instant messaging, database, application and VOIP servers
- Backup environment, including archival and disaster recovery backups

1.11 ACTIVITY

Explain the meaning of electronic discovery and the violations with respect to it? Also, how it is utilized in the criminal procedure? Briefly explain it with relevant case laws? (800 – 1000 words)