

Annual ADFSL Conference on Digital Forensics, Security and Law

2009
Proceedings


May 21st, 1:00 PM

Don't Touch That! and Other E-Discovery Issues

Linda Volonino

R. J. Wehle School of Business, Dept. of Information Systems, Canisius College, Buffalo, NY,
volonino@canisius.edu

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Scholarly Commons Citation

Volonino, Linda, "Don't Touch That! and Other E-Discovery Issues" (2009). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 8.

<https://commons.erau.edu/adfsl/2009/thursday/8>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



Don't Touch That! and Other E-Discovery Issues

Linda Volonino

R. J. Wehle School of Business, Dept. of Information Systems
Canisius College, Buffalo, NY
volonino@canisius.edu

ABSTRACT

The ability to preserve and access electronically stored information (ESI) took on greater urgency when amendments to the Federal Rules of Civil Procedure went into effect in December 2006. These amendments, referred to as the *electronic discovery (e-discovery) amendments*, focus on the discovery phase of civil litigation, audits, or investigations. Discovery is the investigative phase of a legal case when opponents learn what evidence is available and how accessible it is. When ESI is the subject of discovery, it is called e-discovery. Recognizing that most business and personal records and communications are electronic, Judge Shira A. Scheindlin stated, "We used to say there's e-discovery as if it was a subset of all discovery. But now there's no other discovery." Computer forensics experts, given their expertise in identifying, acquiring, preserving, and searching ESI, can play a key role throughout the e-discovery process, if they choose to do so. They can also assist in the drafting of the e-discovery request, in preparing the response to such a request, and initiating a legal hold for evidence preservation. The objective of this paper is to provide an overview of the e-discovery amendments and case law, their impact on the duty to preserve and produce ESI, and the computer forensic work that can support the e-discovery process.

Keywords: Electronic discovery, litigation, preservation, Federal Rules of Civil Procedure

1. INTRODUCTION

In April 2006, the U.S. Supreme Court approved changes to the Federal Rules of Civil Procedure (FRCP) to bring the law into alignment with the most common type of evidence—electronic evidence (e-evidence). After Congress approved, the amended FRCP became law on December 1, 2006. These amended rules all aim at one issue—the discovery of *electronically stored information* (ESI). ESI used as evidence is known as electronic evidence, or e-evidence. What this means for companies and individuals is that e-discovery imposes an inescapable obligation to be ready and able produce all relevant ESI on demand.

Litigants and their lawyers can expect to face harsh consequences when requested ESI has been destroyed or made inaccessible. Destruction of evidence, which is called *spoliation*, is arguably the most damaging position a party can be in because a court may find it to be an obstruction of justice. To appreciate the risk, consider that obstruction of justice charges were the reasons for the demise of the major accounting firm Arthur Andersen and jail time for Martha Stewart.

2. MOTIVATION FOR THE E-DISCOVERY AMENDMENTS

The *Judicial Conference Committee on Rules of Practice and Procedure* (2005) identified three reasons for implementing the e-discovery amendments:

1. The volume of ESI created discovery issues that had not existed when legal cases dealt with only paper documents.
2. Unlike information memorialized on paper, ESI can be deleted or overwritten with or without the user's knowledge.

3. Unlike paper documents, ESI sometimes can be unintelligible if separated from the system in which it is created and stored.

Basically, the amendments acknowledge that the law had to change in order to keep up with technology. Few trial or corporate lawyers were prepared for this new job function, which largely remains true. As such, they rely on the expertise of those who understand ESI, search methods, and e-evidence investigation procedure.

3. PRESERVATION: TOUCH OR DON'T TOUCH?

A company's ESI has a dual nature in that it is both fragile and persistent. It is easily altered or destroyed when backup tapes are overwritten or corrupted. Yet it can also persist on employees' hard drives and digital devices. The mistake that many companies and their employees make is believing that they can "game" (e.g., outsmart or play dumb) the e-discovery process. That tactic is equivalent to playing the lethal game of Russian roulette.

Figure 1 contrasts differences in how paper and ESI are destroyed or altered and how they are preserved. Because ESI exists only on storage media that may be overwritten, corrupted, or otherwise be unreadable, proactive procedures are needed to preserve it. Without deliberate action to preserve ESI, the expectation is that it will be destroyed or altered. Courts have recognized the fragility/persistence paradox and the need for companies to take affirmative steps to preserve ESI, as shown in Figure 1. Judges do not tolerate ignorance of computer technology or improper handling of ESI--or attempts to use those excuses to defend the destruction of e-evidence.

| | Affirmative Steps | Passivity |
|--------------|--------------------------|------------------|
| Paper | Destroy, alter | Preserve |
| ESI | Preserve | Destroy, alter |

Figure 1. Differences in the preservation of paper and ESI.

Jeff Rothenberg, a senior computer scientist at RAND, captured the paradox by pointing out humorously that "digital information lasts forever, or five years – whichever comes first." What is not humorous is how employees' react when they are informed of the need to preserve their e-mail, documents, or memos related to anticipated or current litigation. Their immediate reaction is to delete such ESI despite the futility of those efforts and the risk of spoliation sanctions they create. Too many companies have relied, in effect, on directives such as "don't touch" to the employees or other data custodians. Computer forensics experts are often needed to help companies preserve ESI in a legally defensive manner.

4. E-DISCOVERY STEAMROLLS THE LITIGATION LANDSCAPE

The United States' FRCP govern the conduct of all lawsuits and other civil actions brought in Federal district courts (LII, 2006). Their e-discovery amendments dramatically increased the number of cases that involve ESI and its preservation. In effect, e-discovery rules have steamrolled the litigation landscape. Typically, lawyers and litigants are unprepared to comply with this type and volume of discovery and all its complexities. Two reasons account for most of this lack of preparedness.

1. Lawyers are not IT people. The huge majority of lawyers never had a course in IT or e-discovery in their law schools. E-evidence lives on in many places and forms that are tough to find, collect, store, and interpret without tech skills.
2. E-discovery must be addressed when a lawsuit is filed. That is, when litigation initiates so does e-discovery.

Comparing Figure 2 to Figure 3 shows how the discovery phase of litigation has changed. Prior to December 2006, discovery was an afterthought because most cases did not get to trial. As a result, cases were ending before discovery got started.

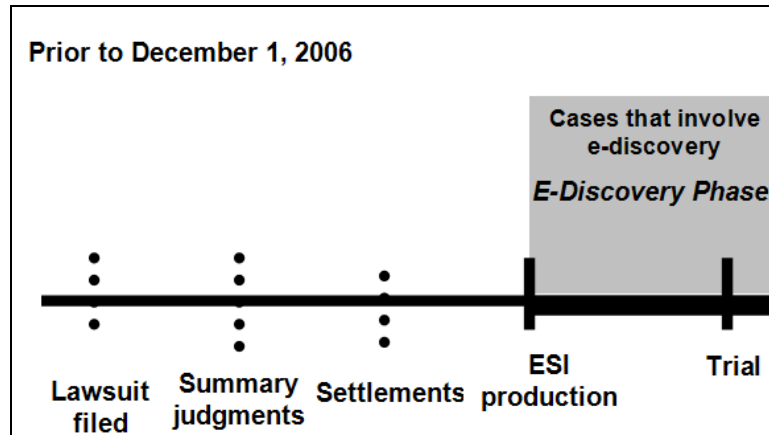


Figure 2. Cases involving e-discovery and ESI production prior to amended FRCP

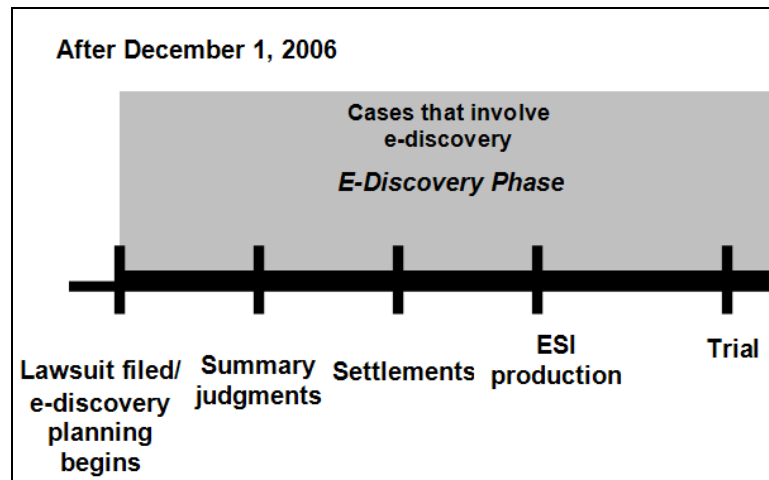


Figure 3. Cases involving e-discovery and ESI production prior to amended FRCP

Three other factors add to the magnitude of e-discovery and the increasing volume of potentially relevant ESI:

1. The rules apply to every type of litigation. Class action lawsuits, complex corporate fraud, and employment cases (e.g., discrimination, wrongful termination, and harassment) involve e-discovery. Government investigations of fraud or improper conduct invariably dig into e-mail, instant messages, and appointment calendars.
2. Companies with at least \$1 billion in annual revenues are involved in an average of 147 lawsuits at any one time, while the corresponding number for companies with under \$1 billion in revenues is thirty-seven.
3. Everything from terabyte-sized databases to text messages and tweets may be *discoverable* (subject to discovery).

All computer systems, digital devices, and anything with a flash drive used by businesses, government agencies, health care and education institutions, and individuals store electronic documents (word processing, spreadsheets, calendars, presentations, etc.) and other forms of ESI. Contact lists on iPhones, instant messages on Blackberries, posts on MySpace, and GPS and EZ-Pass records may be part of the ESI universe.

5. E-DISCOVERY RULES & TIMELINE

Additions and revisions were made to Federal Rules 16, 26, 33, 34, 37, and 45 and to Form 35. Form 35 standardizes discovery agreements to avoid delays and motion practice around discovery later on.

The amendments actually introduced the term “electronically stored information” in Rules 26(a)(1), 33, and 34, to acknowledge that ESI is discoverable. This phrase is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

Amended rules, their requirements, and considerations that highlight the importance of managing ESI throughout its lifecycle—from creation to retention or destruction—are listed in Table 1.

| Federal Rule | Requirements | Questions and Considerations |
|---------------------|---|--|
| Rule 26(a)(1) | Requires an exhaustive search for all ESI, including e-mail that is "in the possession, custody, or control of the party." It must be disclosed "without awaiting a discovery request." The only exception to the disclosure rule is privileged information. The phrase "in the possession, custody, or control of the party" has not been interpreted by the courts. Requires presenting a copy or description by category and location of all ESI that the disclosing party may use to support its claims or defences. | Can an employee's laptop or BlackBerry device be considered <i>under the control of the company</i> , even if it is in a remote location? Companies should consider keeping a centralized copy or backup of everything, including e-mail that might be stored on a remote device. |
| Rule 26(b)(2)(B) | Even if one party identifies information "as not reasonably accessible because of undue burden or cost," its description, category, and location must be disclosed. This means that the information must be identified, even if it is difficult to retrieve. | Delay in producing requested or subpoenaed ESI is not an option. Nothing about the ESI can be left out and opposing counsel can challenge the claim that the ESI is not reasonably accessible. |
| Rule 26(f)(3) | It is expected that most documents will need to be produced in their original form, although the companies can discuss the form in which data is to be produced. | If requested, ESI must be submitted in readable electronic form and metadata must be preserved to facilitate searching potential e-evidence. |
| Rule 16(b) | The search for relevant ESI must be done at the beginning of a legal case and no later than the first pre-trial discovery-related meeting, which is required to be within 99 days of the filing of the legal action. | Extra caution must be taken with any information that could be used as evidence. A best practice is to place a "litigation hold" on documents and e-mail relevant to a case. |

| | | |
|----------------------------------|--|--|
| Rule 34(a) | Specifies that ESI is subject to discovery. This rule sets forth a clear duty to preserve and produce relevant electronic documents, databases, and communication once a company has notice of impending litigation. | When faced with pending or impending litigation or a regulatory investigation, a company must have a response plan to find and produce pertinent ESI. |
| Rule 37(e) "Safe harbor" rule | Provides that courts may not sanction parties for information "lost as a result of routine, good faith operation of an electronic information system." To come within the protection of Rule 37(e), a company would have to show that: (1) the information was lost due to the routine operation of an information system (IS), and (2) the routine operation of the IS was operated in good faith. | Rule 37(e) does not provide any protection if the information is lost outside the routine operation of an IS. Even if good faith does exist, a court may find that "exceptional circumstances" trump the responding party's good faith such that the imposition of some sanction may be justified. |

The rules are mapped onto a timeline in Figure 4. While their purpose is to provide early structure, uniformity and predictability to the litigation process, the reality is that from Day 1 of a lawsuit, a party must be ready to start evaluating with IT, legal, and perhaps computer forensics experts where it stands in terms of its ESI.

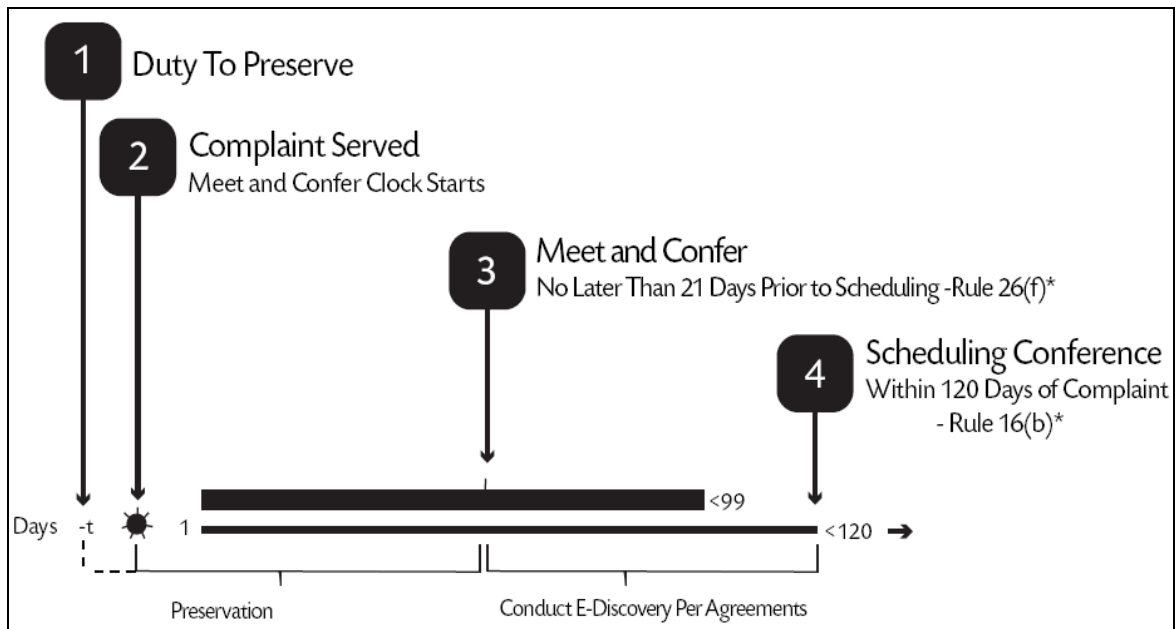


Figure 4. Timeline of the litigation process created by the e-discovery rules.

Time minus zero: Duty to preserve. You need to take 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 because the scope of what needs to be preserved and as of when are not clear. 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. When the lawsuit is filed and complaint is served on the defendant, it starts a clock that counts off days.

By Day 99: Meet and Confer conference. The meet and confer conference (more simply referred to

as the *meet and confer*) 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 costs in terms of difficulty, risk, time, and money of producing the ESI.

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.

By forcing these events early on in a case, by way of the FRCP amendments and case law, parties really have no choice but to be ready to move forward with e-discovery at the start of a case. An alarming example of the potential magnitude of e-discovery and the consequences of not fulfilling e-discovery duties is the ongoing case of *AMD vs Intel*, which is discussed in §6.

6. E-DISCOVERY CASE: AMD V INTEL (2005 - 2010)

In July 2005, Advanced Micro Devices (AMD) brought a lawsuit against its arch-rival Intel for alleged anticompetitive practices in the chip-maker market. In charges filed in federal court, AMD says Intel used its huge size to coerce customers into shunning AMD's chips. Intel had about 80 percent of the market for PC processors while AMD had about 20 percent. The long-running *AMD v. Intel* case is scheduled for trial in February 2010. Both parties recognized that they faced the largest e-discovery ever. Estimates of production were roughly "a pile 137 miles high."

Intel, the world's largest chipmaker with 99,000 employees worldwide and an e-mail load of 3 million messages per day, was ordered by the court in March 2007 to recover 1,000 lost e-mails that it was required to keep. The court gave Intel 30 days. When the company was unable to find them, it pleaded with the court for an extension. The court granted a 10-day extension to come up with a report to AMD on how the e-mail search was progressing or whether the corporation will be able to produce the e-mails at all.

Intel's e-mail system running on Microsoft Exchange servers is automated to expunge e-mail sent or received by employees every 35 days. For senior executives, e-mail is purged every 60 days. Some of the e-mails may be recoverable from backup tapes or by employee-initiated backup. However, Intel used non-indexed backup tapes designed for disaster recovery, but not e-discovery. Trying to find all e-mail messages with specific keywords is tedious and requires a staggering amount of time. One problem is that individual backup tapes have to be mounted one at a time, and then have their contents restored to get them into shape to be examined.

With an understanding of the e-discovery rules and timeline--and a look at e-discovery chaos, we examine the widely used and respected reference model for e-discovery.

7. ELECTRONIC DISCOVERY REFERENCE MODEL (EDRM)

EDRM is an organization composed of numerous working groups that develop guidelines and standards for e-discovery; and help reduce the cost, time and manual work associated with e-discovery. Their widely used Electronic Discovery Reference Model (EDRM), downloadable from <http://www.edrm.net/>, is shown in Figure 5. For excellent and the latest details on each stage in the

EDRM, visit their interactive website.

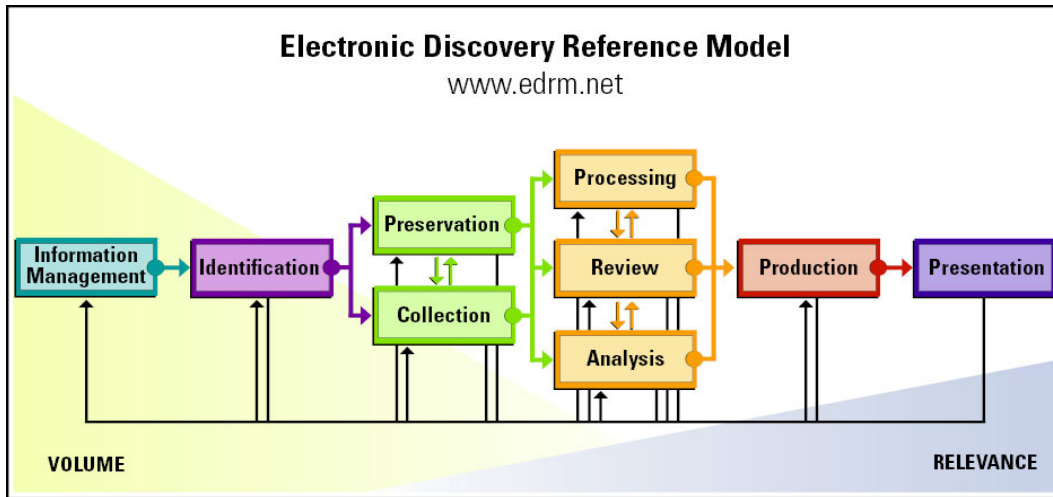


Figure 5. The Electronic Discovery Reference Model (EDRM). Source: <http://www.edrm.net/>

Figure 6 integrates the EDRM with the e-discovery timeline to create the EDRM document production model.

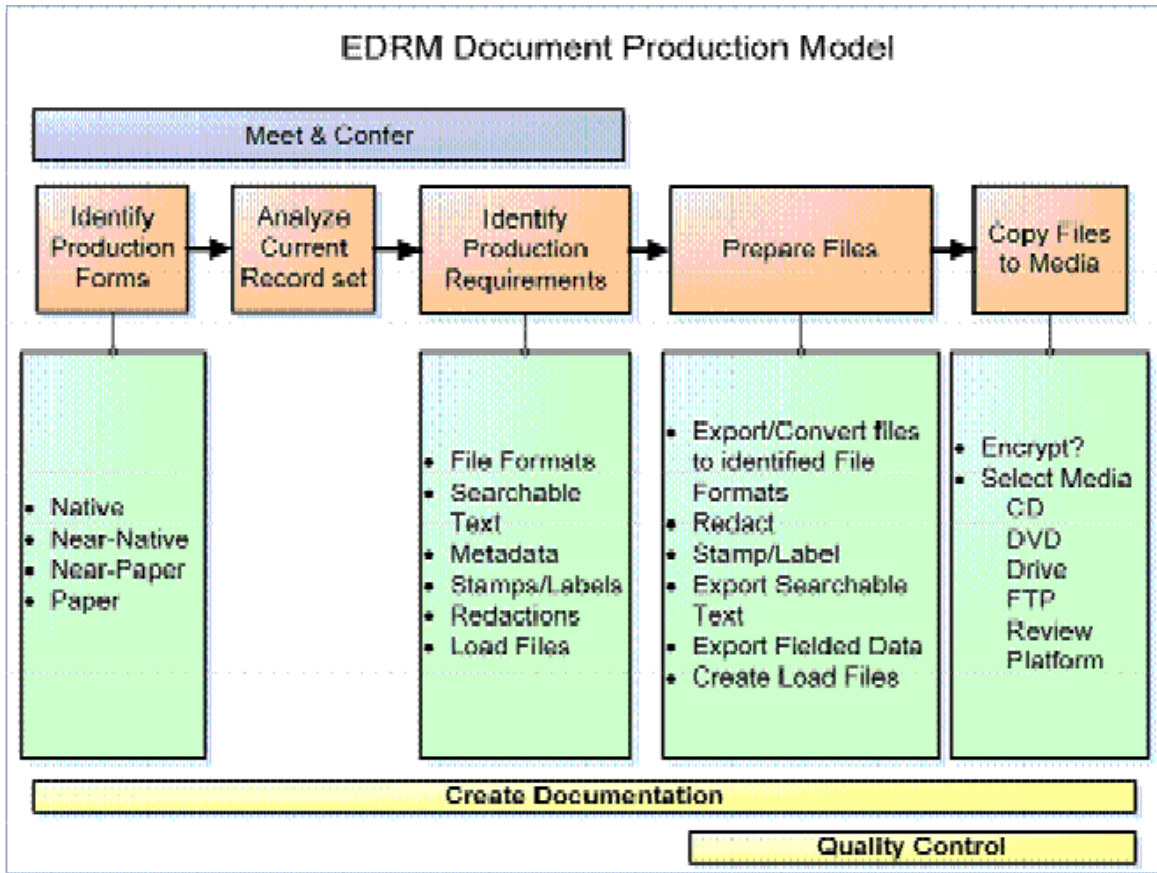


Figure 6. EDRM Document Production Model. Source: <http://edrm.net/blog/archives/146>

The EDRM Document Production Model shows areas where computer forensics experts can help with e-discovery duties and procedures. One crucial function is to keep the IT department and anyone else from touching data on servers and PCs unless and until the ESI has been preserved and/or the corporate legal department confirms that it is safe to do so. As a member of an e-discovery response team, computer forensics professionals can guide decisions regarding native or non-native formats, preservation, effective keyword searches, and the production of ESI.

8. AUTHOR INFORMATION

Linda Volonino, Ph.D., CISSP, ACFE is a professor of Information Systems at Canisius College. She has published six books (Prentice-Hall and Wiley publishers) on IT, information security, and computer forensics. Currently, she's writing *E-Discovery For Dummies* (Nov. 2009) and is a computer forensics investigator with Robson Forensic.

9. REFERENCES

Amended Federal Rule of Civil Procedure (2008). <http://www.uscourts.gov/rules/CV2008.pdf>

EDRM. <http://edrm.net/>

EDRM News. <http://edrm.net/blog/archives/146>

Judicial Conference Committee On Rules of Practice and Procedure (2005). Committee on Rules of Practice & Procedure of the Judicial Conference of the United States, Summary of the Report of the Judicial Conference.

Legal Information Institute (LII, 2006), Cornell Law School, <http://www.law.cornell.edu/rules/frcp>

U.S. Courts, Federal Rulemaking, <http://www.uscourts.gov/rules/index.html>