

10 Critical Decisions for Successful E-discovery

The Federal Rules of Civil Procedure's recent emphasis on producing electronically stored information requires that the e-discovery team understands the collection and processing choices to be made – and their ramifications.

Karen Unger

Today's explosion of electronic data, coupled with the December 2006 amendments to the Federal Rules of Civil Procedure (FRCP) concerning electronically stored information (ESI), requires information and legal professionals to expand their knowledge about handling electronic discovery.

The recent changes to the FRCP include:

- Definitions and safe harbor provisions for the routine alterations of electronic files during routine operations such as back ups [Amended Rule 37(f)]
- Information about how to deal with data that is not reasonably accessible [Amended Rule 26(b)(2)(B)]
- How to deal with inadvertently produced privileged material [Amended Rule 26(b)(5)]
- ESI preservation responsibilities and the pre-trial conference. [Amended Rule 26(f)]
- Electronic file production requests [Amended Rules 33(d), 34, 26(f)(3), 34(b)(iii)]

There are many opinions about how ESI should be planned for, managed, organized, stored, and retrieved. Some of the available options are extremely costly in terms of their required financial and time commitments.

Constantly changing technologies only add to the confusion. One area of confusion is the distinction between computer forensics and electronic discovery; there is a significant difference. These are described in the sidebar "Computer Forensics vs. Electronic Discovery."

At the Core

This article

- ▶ Discusses the 2006 amendments to the Federal Rules of Civil Procedure
- ▶ Explains the difference between computer forensics and electronic discovery
- ▶ Identifies critical questions to be resolved when planning for and executing the collection and processing of electronically stored information

Making the Right Choices

Successfully responding to e-discovery within the constraints of the amended FRCP requires organizations to make many critical decisions that will affect the collection and processing of ESI.

Collection Decisions

The following questions need immediate answers:

1. *Are e-mail files part of this project? If so, do any key people maintain an Internet e-mail account, in addition to their corporate accounts?*

The sheer volume of transactions for large e-mail providers prohibits the storage of massive amounts of mail files. Many Internet e-mail account providers, such as AOL, BellSouth, and Comcast, retain their e-mail logs no longer than 30 days. If a case could potentially require the exploration of e-mail from Internet accounts, the discovery team must expeditiously request the records, or they may be gone forever. This usually requires a subpoena. In rare cases, fragments of Internet e-mail may be recovered forensically from an individual's hard drive.

2. *Is there any chance illegal activity may be discovered?*

Many cases involving electronic data uncover wrongdoings. These situations may involve a member of the technology department or a highly technical employee. In these cases, an organization's first inclination may be to terminate the employee(s) involved and determine the extent of any damage prior to notifying law enforcement agencies.

This may be exactly the WRONG thing to do. If the wrongdoing is by a technical person, there is a chance that he or she is the only person who knows how to access the files, find the problem, or fix it. This is often the person who knows the passwords for mission-critical applications. The technical employee usually has the ability to work and access company files remotely. Unless such access is eliminated prior to the employee's termination, it is possible that a terminated or disgruntled employee may access the network and do great damage.

A better solution is to restrict the employee's complete access privileges, both local and remote. The employee is then notified of management's knowledge of the situation and given an opportunity to cooperate to minimize the damage. If the situation involves criminal matters, especially if financial or medical records have been compromised, a good decision is to involve law enforcement as early as possible. Electronic criminals frequently disappear and destroy all evidence of their activities.

3. *Is it possible that deleted or hidden files may play an important role in this case?*

There are three ways to collect electronic files for discovery:

- Forensically – as described in the sidebar
- Semi-forensically – using non-validated methods and applications to capture files
- Non-forensically – using simple cut-and-paste copy methods to move copies of files from one location to another. These methods do not include hashing files to ensure the

Computer Forensics vs. Electronic Discovery

Computer Forensics

The field of computer forensics was developed primarily by law enforcement personnel for investigating drug and financial crimes. It employs strict protocols to gather information contained on a wide variety of electronic devices, using forensic procedures to locate deleted files and hidden information.

Computer forensics tasks include capturing all the information contained on a specific electronic device by using either a forensic copy technique or by making an image of all or a portion of the device. A forensic copy provides an exact duplicate of the hard drive or storage device. None of the metadata, including the "last accessed date," is changed from the original. However, the copy is a "live" version, so accessing the data on the copy, even only to "see what is there," can change this sensitive metadata.

By contrast, making a forensic image of the required information puts a protective electronic wrapper around the entire collection. The collection can be viewed with special software, and the documents can be opened, extracted from the collection, and examined without changing the files or their metadata.

Other forensic tasks include locating and accessing deleted files, finding partial files, tracking Internet history, cracking passwords, and detecting information located in the slack or unallocated space. *Slack space* is the area at the end of a specific cluster on a hard drive that contains no data; *unallocated space* contains the remnants of files that have been "deleted" but not erased from the device, as "deleting" simply removes the pointer to the location of a specific file on a hard drive, not the file itself.

Electronic Discovery

Electronic discovery has its roots in the field of civil litigation support and deals with organizing electronic files using their attached metadata. Because of the large volume encountered, these files are usually incorporated into a litigation retrieval system to allow review and production in an easy methodology. Legal data management principles are used, including redaction rules and production methodologies.

Electronic discovery tasks usually begin after the files are captured. File metadata is used to organize and cull the collections. Documents can be examined in their native file format or converted to TIF or PDF images to allow for redaction and easy production.

Common Capabilities, Different Philosophies

Computer forensics and electronic discovery methodologies share some common capabilities. One is the ability to produce an inventory of the collection, allowing reviewers to quickly see what is present. Another is the ability to determine a common time zone to standardize date and time stamps across a collection. Without this standardization, an e-mail response may appear to have been created before the original e-mail.

Each of these disciplines, though, has a different philosophy about capture and processing, employs different procedures and software applications, and sometimes requires vastly different time, effort, and monetary resources for processing files.

files have not changed, which involves using a hash algorithm to create a mathematical “fingerprint” of one or more files that will change if any change is made to the collection.

For some matters, the content of electronic documents is all that matters. The context of the files – who created them, how they are kept, how they have been accessed, if they have been changed or deleted – is not as important.

For other cases, contextual information, including finding deleted files, is vital and requires a forensic collection. This includes

- Ensuring legal search authority of the data
- Documenting chain of custody
- Creating a forensic copy using validated forensic tools that create hash records
- Using repeatable processes to examine and analyze the data
- Creating a scientific report of any findings

Determining the value of electronic forensic file collection must be done prior to any data being captured. Once semi- or non-forensic methods have been used, it is impossible to return records to their original states.

4. *Are backup tapes part of an active collection?*

Some cases involve historical issues, making the method of handling computer backups important to address immediately.

Most businesses use a schedule of rotating their backup media. For example, in a four-week rotation, daily backups are done for a week and then those tapes (or drives) are taken offsite for storage. A new set of media is used for the second, third, and fourth weeks, and then those three tapes are stored offsite. On the fifth week, the tapes/drives from the first week are reused. This process is done for financial reasons, as it is extremely cost-efficient.

Determining the value of electronic forensic file collection must be done prior to any data being captured. Once semi- or non-forensic methods have been used, it is impossible to return records to their original states.

Backup tapes may become part of the active information required to be kept under a litigation hold. This requires cessation of any rotation schedule, and the 2006 amendments to the FRCP make it critical for the legal team to convey that information to the technology employees responsible for business continuity processes.

Processing Choices

Because of the volume of information available in even the smallest of collections, it becomes necessary to manage the process to control time and budget. The following questions need to be answered:

1. *Who are the key people?*

The people important to a case should be identified. These key individuals include not only executives, but also assistants and other support personnel from the technology, accounting, sales and marketing, operations, and human resources departments.

2. *Where are the files located?*

All the potential locations of electronic evidence should be identified. These include home computers and all computers that a key person would use elsewhere (such as a girlfriend or boyfriend’s home), cell phones, PDAs, Blackberries, and any other digital device that might be used. It is important to note that MP3 players, such as iPods, can also be used to store documents or important files.

3. *How can the collection be culled?*

Methods for limiting the number of files collected may include collecting only those in certain date ranges or only those containing selected key words or terms. This can be done either before or after an entire hard drive is collected forensically. “Known file filtering” can also reduce the collection by removing standard application files common to all computers (such as the Microsoft Windows® logo file).

4. *How should password-protected/encrypted files be handled?*

Encrypted files cannot be processed until the encryption is broken. In some instances, files with exact or similar names may be available without using passwords or encryption. File locations may also provide information about the value decryptions provide. Decryption may require significant time. Sometimes a password can be obtained simply by asking for it, so this should be the first step. If that fails, using a subpoena may be successful.

5. *How should duplicate and near-duplicate documents be handled?*

Electronic file collections almost always include duplicates. Multiple individuals may have the same e-mail, with the same attachments. Two or more people may have reviewed key documents, saving them on their hard drives during the process. In processing electronic collections, it is possible to identify exact duplicate files and limit the number of documents that require review.

Identifying exact duplicates usually occurs during the phase in which the metadata is identified and extracted from

the files. De-duping the collection will minimally delay the processing.

Standard de-duping involves identifying files that are exact duplicates and eliminating them. If anything has changed within a document, including formatting such as a change of font, it is no longer an exact duplicate and is not de-duped.

It is imperative that both sides of a case agree on what is meant by “de-duping.” Many electronic discovery systems literally delete the files so they are gone from the collection. The forensic tools used in law enforcement, however, usually do not delete the duplicates, but merely identify them for future use.

Discussing this definition during the pre-trial conference to ensure that all sides of a case use the same definition is imperative to ensuring that there is not a discrepancy in the number of files that each side later has.

A more significant portion of any collection will be “near duplicates.” This includes files that have been significantly altered or contain only a portion of the main document. For some projects, the sheer file volume requires that near duplicates be identified and reviewed as a group. This significantly reduces review time and costs when compared to traditional linear review.

Identifying near duplicates requires comparing each document to every other document or using sophisticated software applications that require additional processing time. This technology increases consistency of review categories, reducing the chance of near-duplicate documents being identified as both privileged and non-privileged.

6. What form should the collection take?

The new rules state that the parties will meet and determine the format in which they wish to receive electronic evidence. In the absence of an agreement, the format will be that “in which it is ordinarily maintained” or in a “reasonably usable” format.

The choices a legal team has include whether each side prefers to receive the electronic evidence in native file format,

converted to TIF or PDF, or in some other form. Often, this will depend upon the team’s standard litigation review system.

Such systems handle both native and converted files, with or without associated metadata and full text. There are pros and cons for both options. Native files with extracted metadata reflect the exact original file; however, they cannot be Bates labeled, which is a technique to mark documents with a unique identification code as they are processed, and are subject to inadvertent change.

Converting native files to TIF or PDF is time-consuming and is the most expensive task in electronic discovery. Because 60 to 80 percent of the files in a collection may be non-responsive or irrelevant, both the time and finances

expended in conversion may be counter-productive.

The best compromise involves receiving files in native format, reviewing them for relevancy, and choosing only those that may be produced or used extensively for conversion to image format.

Managing the vast amount of electronic files for litigation requires preparation – planning for the production, organization, and retrieval of pertinent and relevant documents and managing both cost and time budgets. Because every case presents unique circumstances, there are no absolute correct answers to the questions above. But a team that understands the choices and their ramifications is prepared to make the informed decisions that will result in the best possible outcomes for the case and the organization. ■

Karen Unger is CEO of American Document Management and is a Certified Computer Examiner through the International Society of Forensic Computer Examiners. She has written on related topics for and been quoted in numerous publications, including the National Law Journal, Privacy and Data Security Law Journal, and E-Commerce Times. She may be contacted at ksunger@amdoc.com.

References

- Ball, Craig. “Hitting the High Points of the New EDD Rules.” *law.com*, 27 December 2006.
- Denny, William R. and O’Connell, John A. “The Impact of the New E-Discovery Rules.” Potter Anderson & Corroon LLP. Available at www.potteranderson.com/news-publications-0-189.html (accessed 17 August 2007).
- Lynn, Cecil A. Esq. “Top 10 Tips to Prepare for FRCP Changes.” *The Discovery Standard*. Available at <http://law.lexisnexis.com/litigation-news/articles/article.aspx?groupid=eQ5qfLggRQQ=&article=MHJ7YPzhI84=> (accessed 17 August 2007).
- U.S. Department of Justice Technical Working Group for Electronic Crime Scene Investigation. *Electronic Crime Scene Investigation, A Guide for First Responders*. Washington, D.C.: U.S. Department of Justice, 2001. Available at www.iwar.org.uk/ecoespionage/resources/cybercrime/ecrime-scene-investigation.pdf (accessed 17 August 2007)
- Wade, Colleen and Yvette Trozzi, eds. *Handbook of Forensic Services*. Washington, D.C.: U.S. Federal Bureau of Investigation, 2003.

Read More About It

- Discovery Resources: www.discoveryresources.org/
- Michigan State University Libraries: www.lib.msu.edu/harris23/crimjust/cybercri.htm
- National Center for State Courts: www.ncsconline.org/
- The International Society of Forensic Computer Examiners: www.isfce.com