Title:
10 Critical Decisions for Successful E-discovery Part 1

Word Count:
957

Summary:
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.

Keywords:
computer forensics, electronic discovery, litigation support, document imaging, document scanning, form processing

Article Body:
The Information Management Journal/September / October 2007- 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.

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 ะ as described in the sidebar

* Semi-forensically ะ 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 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 ะ who created them, how they are kept, how they have been accessed, if they have been changed or deleted ะ 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.

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.