Title:
10 Critical Decisions for Successful E-discovery Part 2

Word Count:
1138

Summary:
The Federal Rules of Civil Procedureีs 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- Todayีs 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.

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 boyfriendีs 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

Windowsจ 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 าde-duping.ำ 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 าnear duplicates.ำ 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 าin which it is ordinarily maintainedำ or in a าreasonably usableำ 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 teamีs 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.