

Know how to identify, collect and preserve ESI

It's been roughly seven months since amendments to the Federal Rules of Civil Procedure have been implemented.

The rules were amended to address the ever-increasing volumes of electronically stored information (ESI), which is so pervasive in litigation today.



ELECTRONIC DATA DISCOVERY

PETER COONS

You have likely read about the harsh penalties and sanctions imposed upon parties for the gross mismanagement of the discovery and production of ESI. How do you mitigate these risks as an attorney or a corporation?

The best way is to address the two most important parts of the discovery process — the identification and preservation of ESI. Luckily, the amended rules and committee notes provide a pathway to ESI nirvana and help us answer the age-old questions: why, when, who, where, what and how.

Why is ESI important?

It's evidence. A party must preserve and eventually produce ESI that supports its claims or defenses. The obligation to preserve evidence does not change simply because the information is an e-mail stored on a server as opposed to a "real" piece of paper in a filing cabinet.

Studies show that more than 90 percent of all business records are created and stored electronically. Most litigation today will, or could, involve some form of ESI.

When should preservation start?

Prevailing wisdom and case law point to this guideline: When a party can reasonably anticipate litigation, it should begin preserving evidence. For example, if a disgruntled worker files an Equal Employment Opportunity Commission claim, one can reasonably anticipate litigation.

It may be difficult to pinpoint a time, but I wouldn't wait until the papers reach your desk. The "when" can also be addressed by asking when parties should address issues

surrounding preservation of ESI.

"Whether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case. It is often useful for the parties to discuss this issue early in discovery," the committee notes read. "Rule 26(f) is also amended to direct the parties to discuss any issues regarding preservation of discoverable information during their conference as they develop a discovery plan."

Repeat this mantra: Meet early and often.

Who has the data?

Identifying key custodians or systems that contain relevant data is an essential part of the discovery process. A party is obligated, without awaiting a discovery request, to identify persons likely to have discoverable information.

As stated in the FRCP, a party must also provide "a description by category and location, of all documents, ESI, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses." This process may involve interviewing key employees or information technology (IT) professionals with intimate knowledge of electronic record management and storage.

Where does ESI live?

Make friends with the nerd. That's right, talk to your in-house IT folks or a technology consultant proficient in electronic discovery. They can be your best friend, your digital sherpa, helping to avoid claims that you didn't do enough to locate every nook and cranny where ESI may live.

Rarely does the discovery of ESI involve just e-mail or a couple of word-processing documents. There may be databases or legacy servers storing years' worth of important data that is no longer online or readily accessible. The IT staff or consultant can help identify these potentially vital sources of ESI.

Wouldn't it be easier if the FRCP listed all the potential sources of ESI? The rules purposely do not define ESI. The term has

Rarely does the discovery of ESI involve just e-mail or a couple of word-processing documents.

a broad meaning primarily because technologies transform so rapidly.

"The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of Electronically Stored Information" (Committee note to FRCP).

What should be preserved?

Preservation is different than production and should be handled with kid gloves. It also is important to note that just because you preserve information doesn't mean that it is going to be produced.

Rule 26(b)(2)(b) states that "a party need not provide discovery of Electronically Stored Information from sources that the party identifies as not reasonably accessible because of undue burden or cost ... the court may nonetheless order discovery from such sources if the requesting party shows good cause."

Basically, if you know that important, relevant data are or may be stored on a 10-year-old backup tape, it must be preserved.

Do not fall into the trap of thinking that backup tapes (or any other offline media) are inaccessible and therefore can be thrown out or reused. The committee notes to Rule 26(b)(2) are clear: "A party's identification of sources of Electronically Stored Information as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."

Another thing to consider when preserving ESI is whether or not you need to preserve metadata. The committee notes to Rule 26(f) define metadata as "information describing the history, tracking, or manage-

ment of an electronic file."

In practical terms, metadata is underlying data relating to the history of a document, such as author and when the file was modified. The simple act of copying a file from one medium to another modifies the created and accessed time to the time of the transfer. This may not seem important until you are asked to produce all electronic documents created before 2006, for example.

How should data be preserved?

Electronic data has some neat characteristics. It can be searched almost instantaneously — type in a few keywords, and voila, the results appear before your eyes. However, print a document to paper, and it loses that ability. "A party who produces documents for inspection shall produce them as they are kept in the usual course of business ..." (Rule 34[b][i]).

The committee notes expand on this: "The responding party must produce ESI either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable," they state.

Earlier I stated that preservation does not equal production. But think a few steps ahead. If you preserve it, you may have to produce it, and produce it in a form that represents the ESI as it was normally maintained. In plain English, don't convert or mutate an electronic record to a format that is not usable. Don't preserve an e-mail by printing it out. If it's an electronic record, such as an e-mail or a Microsoft Word document, find a way to preserve it as such.

Technology can be confusing. Add in the complexities of litigation, and you have the potential for some serious headaches. If you aren't sure about what to do, don't be afraid to ask questions of other attorneys, IT professionals or electronic discovery consultants.

You only get one shot. ESI is volatile, and not identifying and preserving it properly and in a timely manner could cost your client or corporation the case.

Peter Coons is director of digital forensics at D4, a DocuLegal affiliate. Based in Rochester, he can be reached at pcoons@d4discovery.com.