

E-DISCOVERY: BASIC CONCEPTS

By James L. Cook¹

The amendment to the Federal Rules of Civil Procedure (Rules) concerning the discovery of Electronically Stored Information (ESI) that was effective December 1, 2006 has spawned countless articles about “electronic discovery” or E-discovery and the effect that the amendment will have on discovery under the federal Rules. However, E-discovery is not a new concept. The 1970 advisory committee notes to Rule 34 state:

“The inclusive description of ‘documents’ is revised to accord with changing technology. It makes clear that Rule 34 applies to electronics [sic] data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent’s devices, respondent may be required to use his devices to translate the data into usable form. In many instances that means that respondent will have to supply a print-out of computer data.” Advisory Committee Notes, 1970 Amendment, Fed. R. Civ. P. 34 (2007).

Although the 1970 amendment made it clear that electronic information was discoverable, the implication was that the discoverable information would be produced in paper form as a print-out. Over the last 37 years, the focus of discovery is gradually shifting from discovery of information in print form to discovery of information in electronic form.

“In today’s paperless world, discovery has focused less on hard copy documents and more on electronically-stored information. Requests for electronic information have become so commonplace that one judge has remarked, ‘[I]t is black letter law that computerized data is discoverable if relevant.’” Shira A. Scheindlin and Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 Mich. Telecomm. Tech. L. Rev. 71, 71 (2004) available at <http://www.mttr.org/voleven/scheindlin.pdf>.

The December 1, 2006 amendment explicitly recognizes this shift and brings the discovery of information in its native electronic form to the forefront of discovery practice. This in turn will mean that attorneys must, depending upon the case, deal with technology as an integral part of discovery practice. This article briefly summarizes basic concepts that an attorney must understand to avoid some of the perils that are inherent in E-discovery.

WHAT’S SO DIFFERENT ABOUT E-DISCOVERY?

E-discovery is inextricably intertwined with technology knowledge including: 1) general information technology knowledge; 2) specific knowledge about software tools and services used to search, review, and analyze ESI; 3) client specific information technology systems and practices; 4) case specific knowledge of what ESI may or may not be discoverable or relevant; and 5) client specific knowledge of the costs and burdens associated with preserving, identifying, and producing ESI. Without this

¹ The author is an Associate Attorney with Noeding & Jarrett, a Professional Corporation.

knowledge, it will be difficult or impossible to develop an effective discovery plan; prevent or minimize the risk of inadvertent loss or modification of ESI; effectively prepare or respond to discovery requests; or effectively handle discovery disputes.

E-discovery requires legal knowledge to be *effectively* combined with several different areas of technology knowledge through the efforts of multiple people who do not speak the same “language”. The “language” and concepts of technology are very different from the “language” and concepts of law. It takes effort and time for people skilled in one area to work effectively with people skilled in the other area.

ESI files are fundamentally different than physical files. Several areas of difference between ESI files and physical files are that ESI files:

- are intangible, invisible, easily duplicated, easily transferred to remote locations, and may be found almost anywhere;
- may be automatically altered or destroyed without explicit individual action, awareness, or knowledge;
- have wings – they can be sent anywhere in the world nearly instantly;
- are difficult to destroy – and destruction will probably leave a trail;
- may contain thousands to billions of times more information;
- contain data and relationships about the “primary” information (metadata); and
- may be intertwined with or located in the ESI of other individuals or entities.

Rule 26(f) requires the parties to confer concerning disclosures required by Rule 26(a)(1) and to develop a proposed discovery plan that, among other things, requires them to discuss “any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced.” Rule 26(f)(3).

“The amendment to Rule 26(b)(2) is designed to address issues raised by difficulties in locating, retrieving, and providing discovery of some electronically stored information.” Advisory Committee Notes, 2006 Amendment, Fed. R. Civ. P. 26 (2007). “Under this rule, a responding party should produce electronically stored information that is relevant, not privileged, and reasonably accessible, subject to the (b)(2)(C) limitations that apply to all discovery. *The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing.* The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.” *Id.* (emphasis added).

Rule 37(f) provides that “[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.” Fed. R. Civ. P. 37 (2007).

“Subdivision (f) is new. It focuses on a distinctive feature of computer operations, the routine alteration and deletion of information that attends ordinary use. Many steps essential to computer operation may alter or destroy information, for reasons that have

nothing to do with how that information might relate to litigation. As a result, the ordinary operation of computer systems creates a risk that a party may lose potentially discoverable information without culpable conduct on its part.” Advisory Committee Notes, 2006 Amendment, Fed. R. Civ. P. 37 (2007). “Good faith in the routine operation of an information system may involve a party’s intervention to modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation.” *Id.*

Key E-discovery issues must be addressed in the initial Rule 26 conference of the parties. The Rule 26 conference is not the time to discover what is not known about a client’s information systems and ESI relevant to the litigation. So, the first things an attorney must address is: where potentially discoverable ESI is maintained by the client; where ESI may be found even when it is not maintained by the client; and whether there is a potential for routine operation to alter or destroy the information.²

Thus, the first steps in E-discovery are to determine: where ESI can be found; what ESI exists; and what proactive steps need to be taken to preserve potentially discoverable ESI. Since it may not be possible to initially determine what ESI is potentially relevant or discoverable, it may be advisable to preserve ESI until it can be determined if the ESI is relevant or discoverable.

WHERE IS ESI FOUND?

The short answer – Everywhere!

Discovery of ESI is generally thought of from the perspective of typical business documents³ such as email, word processing documents, or spreadsheets. However, ESI that could be relevant to a particular litigation can be found in many forms and many places. The client may not even be aware of where all of its ESI is maintained. More importantly, the client probably is not aware of where all potentially relevant ESI that is outside of its control, but that may be accessible to the adverse party, may exist.

The first task is therefore to find out where the client maintains ESI. This will require the assistance of people responsible for the client’s Information Technology (IT) systems. Although these people will generally have good knowledge of the actual systems and software used, they may not have good knowledge of the types of information maintained. They will almost certainly not know what information will be important to the litigation.

An attorney must have enough knowledge of typical ESI locations and information content to communicate with IT personnel and guide the search for ESI. A brief summary of some of the more important ESI sources is provided in the following sections.

² This article is written from the perspective of an attorney defending a corporate client.

³ The term “document” as used in this article is an expansive concept that means “a discrete physical or virtual container holding one or more information elements or other documents.” Thus, a music CD is a document and a single track on that CD is also a document. A typical cell phone contains many possible documents: a phonebook document that contains individual phone record documents; a recent calls received or calls made document that contains individual call records; or a memo document that contains individual voice memo documents. The concept of a document is expansive, recursive, and unbounded.

Email

Email is often a high value source of information important in litigation. Email is used ubiquitously and is often not used carefully. The content of email may be very informal and subject to very differing interpretations. Email is also not confined to a single source. Email may be found on company email servers; email backup tapes; general server backup tapes; individual PCs used by company employees; personal PCs used by employees who do work at home; Blackberrys; Personal Digital Assistant (PDA) devices; servers of external email or Internet service providers; service provider archive tapes; printed pages; or individual storage devices such as USB drives.

This list of sources is not limited to a company or its employees. Email is used for outside communications and is often forwarded, copied, or blind copied. Thus emails can end up on the same list of devices noted above for many different individuals or entities. Emails can also be archived or converted to different formats and copied and posted on web pages or sent to email list servers (listserves) with distribution to hundreds or thousands of recipients.⁴

Email can be maintained in different directories (folders) on various devices. Some of these directories may not be visible or known to the email user. For example, most email programs will keep copies of mail sent in a “Sent Folder” or copies of deleted email in a “Deleted Folder” and each email program may use different names for these typical folders.

Email deleted from an individual PC may not be deleted from an email server that received or sent the email. Email may also be filtered out by spam filters at both a server and an individual PC level and thus be found in different directories than email that is not filtered out. Email may also be simply deleted without human intervention by a spam filter or by limits placed on individual email accounts by an IT administrator. However, even if deleted, email may still be recoverable.

Email may also contain attached digital files that contain hundreds or thousands of pages of printed information, video or audio recordings, or information only accessible with specialized software such as a database or accounting program.

PC Based Digital Files

This category of ESI covers the entire range of documents that can be produced with a personal computer. Typical documents include word processing files, spreadsheet files, and presentation files. However, this category of documents also includes pictures, scanned images, and video or audio recordings.

Digital files can be easily copied, modified, combined with other files, and then transferred to a PC or server located anywhere in the world.⁵ Digital files can be found

⁴ Listserves often have publicly visible webpages that can be found in an Internet search. See <http://lists.ibiblio.org/pipermail/cc-cn.mbox/cc-cn.mbox> for an example of such a page.

⁵ A video of Cohen & Grigsby's Seventh Annual Immigration Law Update seminar held on May 15, 2007 was posted on its website. The Programmers Guild abstracted a portion of this video, added their own content to it and posted the resulting video on YouTube. The video has been viewed about 200,000 times since it was posted on June 16, 2007. See <http://www.youtube.com/watch?v=TCbFEqFajGU>. Cohen &

on all of the same devices and storage media listed above for email. As with email, the devices and media containing digital files may be controlled or owned by many different individuals or entities.

Digital files may be copied onto archival or backup media automatically or manually. Archival processes may remove the digital file from its original location. Backup processes will usually leave the digital file in its original location.

Although digital files are easily copied, modified, and transferred, actual permanent deletion of these files is not easy and often will leave traces of the deletion activity. Deleting a file from a PC or server simply removes its name from the visible list of files stored on the PC or server. However, there are many different software programs (tools) that can be used to recover a deleted file and all or a portion of the information that was contained in that file. If it is suspected or known that relevant or discoverable files have been deleted, a forensic computer expert may be able to recover them. Even if the files cannot be recovered, the typical programs and processes used to permanently delete files and the information they contain will cause an “absence” of deleted or temporary files that are present on any PC or server. This absence of “deleted files” can often be a definitive indication that files have been intentionally deleted.

Other Types of ESI

Although the first two categories of ESI are daunting enough, relevant or discoverable ESI may exist in many different forms and locations based on the issues that are in dispute. The following examples show the range of ESI that may have to be considered in discovery planning.

- Company data repositories are typically databases containing business information. This information can be accounting records, personnel records, payroll records, manufacturing and sales records, mailing lists, customer lists, or any other large quantity of information that a company needs or wants to retain and use over time. The important concept with regard to database repositories is that the relationships between individual data records may be more important than the actual data elements. Print copies of ESI records will not generally reveal the metadata that is most valuable. Only actual production of the ESI file and analysis of it with an appropriate software program will reveal this information.
- Fax server or fax machine logs show dates, times, phone numbers, and the number of pages sent. Internet fax service provider logs may provide several years of activity.
- Network system records maintain an extensive record of all activity performed on a computer network and on individual PCs connected to the network. These records may contain login identification, dates and times of logins and logouts, dates and times that a file was accessed, modified, or deleted. These records may also contain records showing all Internet activity including the

Grigsby subsequently removed the video but the YouTube posting is still active as of July 5, 2007 and has probably been copied and forwarded by hundreds of individuals.

- date and time that a web page was accessed, the log of all web activity by individual users. These logs typically are limited as to how much data is saved and if not preserved quickly, past data may be permanently lost.
- Company and individual voice mail systems and telephone answering devices may contain phone messages for long periods of time. Recorded messages may be automatically deleted after a period of time if they are not saved.
 - Individual PC operating system logs maintain similar data as network system records although the level of detail is generally not as extensive.
 - Phone records show dates, times, phone numbers, and the length of calls made. Cell phone records will typically show every call while land line records may only show toll calls. The telephone service provider logs may provide a year or more of activity.
 - Credit card records will show dates, times, amounts, and the vendor for charges made. Scanned copies of the actual charge slip may also be available.
 - Bank records will show dates, times, amounts, and the transmitting or receiving entity for each transaction. Scanned copies of checks may also be available.
 - Government records may include records of government benefits or records of an individual's civil or criminal conduct.
 - Web sites may show relationships between individuals or entities and contain information about past, present, or planned activities. Web sites may also contain information that has been deleted from other locations. Google search results have a small link shown as cached in the search results pages. Clicking on this link will provide the content of the web page that is stored on Google servers even though the original page is no longer available. Other websites have a goal of providing an archival record of websites. See <http://www.archive.org/index.php> for an example.
 - Company security systems will generally have a record of date, time, and the entry code or id code used by the individual making entry. Systems that use Radio Frequency Identification (RFID) tags can also record the date and time that an identification card comes within range of a sensing station.
 - Many automobiles, trucks, and most commercial transportation vehicles have sensors and recording systems that record data for several seconds or minutes before events that are severe enough to trigger the recording system.
 - Many cell phones now have Global Positioning System (GPS) chips installed that can be turned on by law enforcement agencies or the owner of the phone. There are Internet based service providers that can track the location of a GPS enabled cell phone over an extended period of time. See <http://www.ulocate.com/>.
 - Many automobiles have GPS navigation devices that maintain a record of the automobile's location and speed over an extended period of time.

- The United States Post Office and commercial delivery services such as FedEx, UPS, DHL, and Airborne allow tracking of packages and mail that shows mailing time and location, delivery time and location, and may also show the recipient's signature.
- Companies often elect to install or are required by law to install video or audio surveillance equipment covering a portion or most of their facilities.

Many of these sources of ESI may require specialized software and personnel with the technical expertise to extract the information that is to be produced or analyze the information that was produced.

Thus individuals with the necessary skills and expertise required to obtain information from ESI sources and to authenticate and testify as to its relevance to the issues being litigated may need to be retained. Other ESI sources may only make the information available in print-out form, thus limiting or eliminating the need for technical skills to assess the information to be produced or that was produced.

WHAT ESI EXISTS FOR THIS CASE?

Using global knowledge about what potential sources of ESI could exist, an attorney must then determine what sources are most likely to produce discoverable information for his or her case. The ESI that may be discoverable and that may exist depends upon the parties involved in the litigation; the issues involved in the litigation; and the relationships that the parties may have with other individuals and entities. This topic is beyond the scope of this article but a few examples illustrate the general concepts and considerations involved in developing an ESI discovery plan.

- *Employment discrimination involving sexual harassment.* ESI sources that should be considered include: email, phone records, Internet activity logs, files maintained on personal computers and network servers, personnel records, or voice mail. Other sources such as company surveillance logs, security logs, or bank records could be important depending upon individual fact situations. It may be very important to review network and email server logs to determine if email or files were deleted or sent outside of the employer's facilities to other individuals. It may also be important to identify non-party individuals who may have discoverable email or phone records if the parties do not have sufficient ESI.
- *Automobile accident involving employee during work hours in a company vehicle.* ESI sources that should be considered include: personnel record, employee driving record, GPS records of vehicle location and travel history, cell phone call records before and after the accident, or vehicle sensor and recording systems.
- *Employee theft or embezzlement.* ESI sources that should be considered include: company video surveillance recordings, bank records, credit card records, company accounting records. Other sources could be criminal records or credit records of the individual(s) involved. Personal and work phone records and email may also be of value if conspiracy is suspected.

WHAT ESI MAY BE LOST IF NOT PRESERVED OR IMMEDIATELY PROTECTED?

ESI, like physical records, is subject to document retention policies and thus may be intentionally destroyed as part of a legitimate document retention policy. However, if litigation is reasonably anticipated, there is an obligation to suspend standard document retention policies and preserve discoverable information. Determining this exact point is difficult and beyond the scope of this article.

However, IT staff responsible for implementing document retention policies with respect to ESI may not even be aware that there is an obligation to preserve ESI that they destroy on a routine periodic basis. Failure to notify responsible IT staff of what ESI must be preserved so that ESI is not destroyed could subject a company to sanctions.

IT staff perform a variety of activities in response to events such as the discharge or resignation of an employee. For example, it is common for network and server accounts to be disabled; email accounts to be disabled; and voice mail accounts to be deactivated. Sometimes the disabling of these accounts will result in or be accompanied by destruction of ESI associated with those accounts. Individual PCs may be "recycled" and reissued to another employee or even disposed of and all the ESI on the PC may be destroyed as a result.

ESI, unlike physical records, is also subject to automatic destruction without any explicit action. Network and computer log files are usually limited by time or size so that new activity overwrites old activity. There may be a need to suspend the automatic destruction of ESI so that discoverable ESI that is subject to preservation obligations is not inadvertently destroyed.

CONCLUSION

A basic overview article can only scratch the surface of all that may be involved in E-discovery planning and practice. This article has addressed some of the basic concepts involved in identification, collection, and preservation of discoverable ESI. Other major E-discovery planning and practice areas include:

- review, analysis and processing of discoverable ESI;
- determining what software, systems, and personnel will be needed; and
- determining what form(s) and formats in which ESI will be produced.

Underlying all of E-discovery practice and planning is an understanding of basic technology concepts, the client's document management and retention processes and systems, and the tools and expertise needed to identify the relevant information that exists within a nearly unbounded amount of information. E-discovery is an intellectually challenging task that is labor and time intensive.

Because the December 1, 2006 amendment explicitly makes discovery of ESI an issue at a very early stage in litigation, attorneys should discuss E-discovery issues with clients before litigation ensues. Waiting until after a lawsuit is filed may put the attorney and his or her client at a significant disadvantage if the adverse party is aggressive and knowledgeable about E-discovery.