Discovering ESI: Self-Reliance and Rule 26

By Daniel Kegan – November 4, 2010

ESI—Electronically Stored Information. Three little letters for three words that are substantially changing how attorneys think about and practice litigation. The Federal Rules of Civil Procedure now require an early conference among attorneys to discuss and plan discovery, including ESI. *See* Fed. R. Civ. P. 26(f)(3)(C).

The Internet and ESI make some discovery processes easier but may also increase the volume of materials to be reviewed. Fed. R. Civ. P. 26 (b)(2)(B). Some discovery costs may be reduced by active research by the party itself. However, uncontrolled lay discovery may create serious liabilities, including making illegally obtained evidence inadmissible. A party in litigation generally knows its industry and some relevant facts of the case better than its attorney initially will. Active participation in discovery by nonattorneys may produce relevant information more efficiently. However, lay-person discovery needs to be authorized and supervised by an attorney to avoid possible inadmissibility, sanctions, and ethical violations.

Failure to understand how your client maintains its ESI opens both client and counsel to severe sanctions. *See generally, Qualcomm, Inc. v. Broadcom Corp.*, 539 F. Supp. 2d 1214 (S.D. Cal. 2007). Attorneys cannot simply delegate to their clients the responsibility of understanding ESI and planning for ESI discovery. The attorney has a nondelegable responsibility to know.

Several federal statutes restrict covert and deceptive computer and information access. Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2510, includes the Wiretap Act, regulating the intentional interception and disclosure of communications, and the Stored Communications Act, regulating intentional access, attainment, alteration or prevention of access to facilities storing electronic

communications. The Computer Fraud and Abuse Act (CFAA) prohibits unauthorized access to computer systems, which may include access with inappropriately obtained, or guessed, passwords.

Anything involving medical patents, insurance company trademarks, electronic health system software, and more may invoke the restrictions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). 42 USC § 201.

An attorney needs to understand not only the client's information systems—traditional paper and ESI—but also the information systems of the adverse party. Discovery tasks include learning what information the client has, where and how it is maintained, how the discovery-relevant information can be efficiently gathered and transmitted to the attorney, sequentially numbering files and/or pages, how the information will be reviewed for privilege and confidentiality, how responsive discovery information will be produced to adverse counsel, and corresponding parallel questions relating to the adverse party's discovery.

A partial solution has developed in tandem with the new federal rules —commercial services. However, since the attorneys on the case remain responsible for ESI discovery, they also need to know enough about email, computers, file archiving, the client's business, and human nature to competently supervise the commercial technicians.

This article presents an efficient procedure for a small law firm to successfully manage the ESI discovery process. Large firms can also utilize these procedures, although they may feel less economic need. Guidelines are presented for both Macintosh and Windows computers.

Prerequisites
Successfully managing ESI discovery is not difficult, but does require a comfort level with computer and Internet basics. Prerequisite knowledge includes an understanding of:

- the difference between volatile random access memory (RAM) and nonvolatile hard-drive memory;
- generally, how your own email system works;
- where your email is stored or archived, and who can access it to read, copy, and delete;
- how to use email, word processing, and spreadsheet;
- basic database and how it differs from a spreadsheet;
- how your ESI is backed up;
- the differences between an Internet domain, a website, and an email address;
- what hypertext markup language (html) is and the difference between a webpage display and its coding; and

- what metadata is.

Proceeding in litigation assuming that ESI doesn't exist or can't be retrieved dangerously invokes strong sanctions and law-firm liability. *Bray & Gillespie Mgmt. L.L.C. v Lexington Ins. Co.,* 527 F. Supp. 2d 1355 (M.D. Fla. 2009).

Protective Order

Early in many cases, especially intellectual property cases, a protective order for confidential information will be needed. Some tailoring of a standard protective order may be necessary, especially for individual parties, pro se parties, noncorporate entities, actively involved in-house attorneys, and other common situations.

The confidentiality protective order is now an expected place to deal with common privilege matters, especially inadvertent disclosure. With large amounts of ESI, all should assume that there will be some inadvertent disclosure, despite the reasonable review efforts of attorneys, so appropriate claw-back provisions should be included. *See* Fed. R. Evid. 502(b).

Useful provisions for a protective order contemplating ESI production include:

- Because ESI often involves megabytes and gigabytes of information, some confidentiality and privilege review procedures for ESI need to be different from procedures from more modest amounts of paper production and exhibits.
- ESI shall be produced in a manner to permit reasonable identification of documents, and document sub-parts, or their approximate equivalent for unpaged ESI.
- Upon receipt, all produced ESI shall be treated initially as confidential —attorneys eyes only—in its entirety until 30 days after receipt, unless the parties expressly agree otherwise. Within 30 days after receipt of produced ESI, the producing party may designate in writing portions of the information with a category of confidentiality and shall identify the ESI documents and path name, if appropriate. If the producing party previously designated portions of information with a confidentiality category or as not confidential information, the producing party need not designate those portions of the ESI during the 30-day period unless the producing party changes the designation.

For the protective order proposed to the court, include appropriate provisions for return or certified destruction of confidential information after the conclusion of the case. The court likely will mandate retrieval or destruction of all sealed court documents a few months after closure of the case. Remember to include in your proposed protective order practical provisions for confidential data in the custody of e-discovery service providers, computer forensic experts, the adverse party, and the adverse law firm. Remember to review and attend to those wrap-up provisions at the conclusion of the case.

Case and Discovery Conference 26(F)
Fed. R. Civ. P. 26(f) outlines the topics to be knowledgably discussed by counsel for the early case conference and discovery plan. To be prepared, counsel should know the client's information systems, ESI storage systems, and formal and actual business practices. Counsel should also be able to identify all relevant ESI machines and custodians. If counsel is not conversant with the native format, network mapping, metadata, encryption, and other ESI terms, a knowledgeable person from the client may be needed at the conference.

ESI production might not be required if it is not reasonably accessible because of undue burden or cost. Fed. R. Civ. P. 26(b)(2)(B). If the parties cannot agree, then the court will decide and specify conditions for discovery and potential cost shifting.

Both parties benefit when discovery costs are reduced. One of the easiest ways to reduce discovery costs—for both the producing and receiving parties—is to reasonably limit the scope of discovery, by time period, custodian, types of data, and the like.

At the first reasonable inkling of litigation, counsel should advise the client of the need for a litigation hold on potentially relevant information. An informed notice requires understanding the client's information systems and the full array of people responsible for creating, maintaining, storing, archiving, and destroying corporate information—both paper and ESI. Failure to issue a written litigation hold may constitute gross negligence because that failure is likely to result in the destruction of relevant information. Even negligent litigation hold practices may subject the party to strong sanctions. Moreover, a plaintiff's duty to preserve is usually triggered before litigation begins because the plaintiff controls the timing of the suit. *Pension Comm.*, 685 F. Supp. 2d 456.

Search terms are typically discussed by counsel. Given large amounts of data and documents, identifying relevant documents and information that may be reasonably calculated to lead to the discovery of admissible evidence is often efficiently performed by computerized searching of keywords. Boolean searching can eliminate false hits (e.g., in a trademark case, "SURVEY NOT LAND").

The control group of the client should be interviewed for their individual information habits, including personal communication devices (e.g., Blackberry, Palm, iPhone, flash drives, and their backup, storage, and deletion procedures and habits).

Identifying attorney-client privileged communications is facilitated if the attorney, well before any particular dispute, adopts a firm-wide practice of placing a distinctive short privilege text at the beginning of communications an attorney evaluates as actually privileged. For example, "## Privileged ##." The multiline confidentiality boilerplate at the conclusion of all email communication from a firm does not help identify documents for which a good faith privilege claim may be made.

Chain of Custody and Processing

As with any important evidence, establish strong procedures to document the chain of custody and processing for ESI. It is very easy to alter electronic information. Sometimes simply viewing a computer file will alter its last modification date. Secure the original ESI you receive against use or change, process a cloned copy, and make additional copies before each major stage of processing. Some of the major stages will be the ESI as received, the ESI after file name sequential numbering for document control, the ESI segregated for privilege, confidentiality, relevance, irrelevant (and unlikely to reasonably lead to admissible evidence), and unviewable files.

Some computer files will arrive in a compressed state, and some as a self-extracting archive. The “parent” compressed files, if any, will exist in the received ESI and will contain sequential numbering. After decompression, the "children" should receive their own unique, but related, sequential numbers.

Some produced ESI files will not be viewable. This may be caused by accidental corruption of the file on your client’s computer (or that of the adverse party), the absence of the appropriate viewing application, or intentional evidence destruction.

If you cannot view a file, do not immediately produce it. Sequester it in the "unviewable" group. Seek to learn—whether from your client, the custodian of that file, your technology expert, or adverse counsel—the type of file and why you cannot view it. Sound and video files are not meaningfully viewed but can be perceived with appropriate players. Some files may have incorrect or missing extensions. Some require particular viewing applications.

Avoid commingling case ESI with your routine computer files. If you have an infrequently used computer, designate that for viewing and processing case ESI. When the raw ESI has been sequentially numbered, reviewed, categorized, and processed for production, it may be burned to a disk, read by your computer, and produced to adverse counsel.

If you suspect or know that an electronic file has been altered in any way—content or metadata, insignificantly harmless or materially—you should do three things:

- ensure you preserve the original version of the file;
- understand and document what was changed; and
- promptly disclose a nonprivileged description of the problem.

Most unintentional changes to ESI are immaterial to the evidence needed by the court and would not influence the case outcome, but you want to avoid ancillary litigation on spoliation. Moreover, most inadvertent ESI changes during your discovery processing can be repaired, provided that you document your chain of custody and that you process only copies. Of course, also establish and follow a procedure for redundant, multiple, backups on separate physical media with some at an offsite location.

Transmittal to Attorney

After the client has gathered some discovery and other case documents, they need to be properly transmitted to the attorney for review and processing. Large corporations have Information Technology departments, familiar with technology but likely not as familiar with legal terms and procedures. Small companies may even be at an initial loss of how to gather past email or how to get two years' of email to the attorney for review.

An attorney should help the client's staff that is assisting with discovery and document gathering. The client's personnel must understand that "relevant or reasonably calculated to lead to the discovery of admissible evidence" is a legal definition. Client document collectors should not make their own relevance decisions but discuss all questions with supervising counsel.

For small and medium cases, many clients of only modest computer abilities will be able to burn a CD-ROM or DVD, transmitting several gigabytes on a few discs. Some documents are likely to be paper transmitted in a box. Many business clients are now comfortable scanning documents and can retain the original paper unless the authenticity of the copy is questioned. Fed. R. Evid. 1003. It may be helpful for the client to clone the entire hard drive of some computers, send the clone to the attorney, and discuss in detail the folder/subdirectory structure and the relevance to the litigation.

Email and Attachments

Email use is nearly universal, but users do not always understand how it works. Diverse utility applications are available to translate email between formats.

Email has evolved to include rich, formatted text, graphics, video, sounds, and other attachments. Attachments are handled in diverse ways by differing email systems and clients. An attorney reviewing email with attachments will need to pay special attention to them.

Database
Unlike word processing documents, email, and spreadsheets, databases are not page oriented. Typically, a database file may not be self-explanatory, but often requires a user manual to explain what variables are in what fields and in what formats. Many common commercial database programs change their data formats with newer versions.

Industry-Specific and Client-Specific Software
Industry-specific and client-specific software requires careful attention during the discovery conference. Beyond user guides and technical specifications, confidentiality and access must be determined. Obtaining an authorized version of licensed software must be considered and likely budgeted. In some cases, there are low cost limited versions of viewer software, lacking all the functions of the fully licensed, name-brand application. However, some of the viewer software may not display evidence of inconsistency or evidence spoliation, such as file creation dates inconsistent with witness testimony.

Sequential Numbering for Document Control
Discovery documents are traditionally sequentially numbered by counsel before production It is, however, inefficient to print ESI documents on paper, number the pages, and rescan the documents—regardless of whether the documents are rescanned. Additionally, database documents do not readily print to paged format. An easy solution is to electronically prefix sequential numbers to ESI documents and folders. This maintains the data and structure of the original ESI data while permitting document control.

Keyword and Boolean Searching
Search protocols should be discussed, and perhaps agreed upon, at the initial 26(f) discovery conference. After digging into the data, the attorneys likely will find refinements to the earlier search strategy to be necessary for efficiency.

Large corporations likely have databases with tagged fields. Small clients have less structured data. Each set of attorneys should be flexible enough to respect the data sophistication of its adverse party. It is unreasonable to expect a small business to translate all of its text documents and email into a format that a large corporation uses. Likewise, the small party should realize that overbroad discovery

requests may yield unmanageable mountains of responsive documents.

Privilege Review
With ESI, attorneys should expect that some privileged documents will be inadvertently produced. To support a claw-back motion, counsel likely will need to show that disclosure occurred despite reasonable privilege review procedures.

The privilege log needs to describe the nature of the documents, communication, or tangible things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties and the court to assess the claim. Fed. R. Civ. P. 26(b)(5)(A)(ii).

Most clients do not label their communications to attorneys as privileged, perhaps not even as confidential. Not all communications with an attorney are privilegedFed. R. Civ. P. 26(b)(3) provides a qualified protection from discovery in civil actions when materials are (a) documents and tangible things otherwise discoverable; (b) prepared in anticipation of litigation or for trial, and (c) by or for another party or by or for that other party's representative. To overcome the qualified protection, the party seeking discovery must show (a) substantial need for the materials; and (b) inability to obtain the substantial equivalent of the information without undue hardship. Epstein, Edna Selan, The Attorney-Client Privilege and the Work-Product Doctrine, 5th ed., ABA 2007, at 797. Even upon such a showing, the Court is required to protect the attorney's mental processes from disclosure to the adversary. *Hickman v Taylor,* 329 U.S. 495 (1947); *Upjohn Co. v United States,* 449 U.S. 383 (1981).

Difficult to find are secondary communications where an attorney's comments on a case or a control group member's query to answer a question from an attorney is communicated to another client employee. This will not be an email to or from the attorney. His or her name may not even appear in the email yet the content may be highly privileged and potentially prejudicial. Allow time for privilege review.

Confidentiality Review
When confidential information is expected in a case, its review may be associated with a privilege review. The protective order for confidential information should recognize that a "confidential" marking may not be made on a paper copy. A sample provision is:

ESI shall be marked in an appropriate manner. For ESI Confidential Information produced on physical media, it shall be indicated in a way prominently visible to a person without the aid of a computer, such as

on the label of a computer disk. For ESI Confidential Information produced not on physical media, for example by email or File Transfer Protocol (FTP), it shall be prominently indicated on the documents or by the transmittal correspondence assured to be noticed by the recipient.

Contemporary Special Issues

Cloud Computing. Currently, "cloud" computing is the celebrated technology. Cloud computing is Internet-based computing where provision of some resources, software applications, data, and/or technology support is provided by independent contractors. The shadow of cloud computing is that the data may be physically located in another state, or in nations outside the United States, raising more questions of trade secret confidentiality, privilege retention, subpoena procedures, and the difficulty of adequate discovery disclosure when the subvendor possessing data, and the data location, are unknown. Legitimate data destruction, in routine practice and not in anticipation of litigation, may be difficult given the cloud vendor's backup and archival procedures. Who has access, or ownership, of your data when you terminate your service or the vendor goes out of business or files for bankruptcy are additional questions to consider.

Software as a Service. Software as a Service is a subset of cloud computing, where the software application is hosted on a vendor's server somewhere on the Internet, rather than being hosted on the user's computer or the company's local network server. Data may reside on the user's local computer, on the company server, and/or on the vendor's server(s).

Social Networking.
Many organizational members discuss work matters on social networks and in personal email. Key actors and potential witnesses in a dispute should be asked about their use of social networks; discussion of work matters in noncompany email; and all their Internet screen names, email addresses, and perhaps passwords.

Computer Forensics. If forgery, evidence tampering, or related misdeeds are suspected, a forensic examination may be appropriate. The goal of computer forensics is to explain the current state of a digital artifact—a computer system, storage medium, electronic document, or sequence of packets moving over a computer network.

When witness prevarication, mendacity, or lying is suspected, lay evaluation of readily available metadata may be sufficient. For example, the untruth of an author's claim that he created a work from scratch without relying on a similar preexisting work may be shown by the identical file creation dates for the original electronic work and the suspect derivative work.

Conclusion

Goldilocks remains a useful guide in producing, objecting, and responding to discovery. Discovery requests should not be so broad as to invite reasonable objection, nor so narrow as to overlook key evidence. A significant disparity in the size and resources of parties may influence a court's decision on cost-shifting for burdensome ESI discovery. Attorneys may zealously represent their clients and still collaborate in pursuing efficient discovery of relevant ESI.

As an officer of the court, as well as a fiduciary to the client, litigation attorneys now must be somewhat knowledgeable of computers, the Internet, and ESI, and often must have on their litigation team someone who is sufficiently knowledgeable of ESI in general and the client's information practices in particular. Striking the ESI balance "just right" fulfills the attorneys' duties, reduces client costs, and should reduce otherwise likely sanctions.

Keywords: Litigation technology, electronically stored information, discovery, Federal Rules of Civil Procedure, Rule 26.

Daniel Kegan is a licensed organizational psychologist and an attorney at Kegan & Kegan, Ltd., Chicago, Illinois.

Related Resources

Common native electronic file formats are text (.txt), Word processing (.doc), 2003 Office Open XML (.docx), Excel spreadsheet (.xls), portable document format (.pdf), joint photographic experts group graphic (.jpg), and tagged image file format (.tiff). File formats for databases and custom designed information systems are likely uncommon; more explanation of the format and possible viewing applications likely will be needed.

The Sedona Conference is a nonprofit research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. Through a combination of conferences, working groups, and dialogue, The Sedona Conference seeks to move the law forward in a reasoned and just way. It produces several well-respected conferences and papers on e-discovery. Sedona publications include Electronic Document Retention and Production (WG1); Protective Orders, Confidentiality & Public Access (WG2); International Electronic Information Management, Discovery and Disclosure (WG6).

The district courts of the Seventh Circuit launched the Principles Relating to the Discovery of Electronically Stored Information, October 2009. The Principles seek to provide incentives for the early and informal information exchange on commonly encountered issues relating to evidence preservation and discovery, paper and electronic, as required by Fed. R. Civ. P. 26(f)(2). The principles are included in a proposed standing order relating to the discovery of ESI which several district court judges, magistrates, and bankruptcy judges in the Seventh Circuit have agreed to use in selected cases during the pilot test. The principles highlight the 2006 amendments to the Federal Rules of Civil Procedure, but go beyond those rules in several helpful particulars.

In May 2010 a report on phase one of the Seventh Circuit Electronic Discovery Pilot

Program was released. Phase Two, which continues to May 2011, expects to expand the geographic reach of the pilot program, increase the number of cases and participating judges, and more comprehensively test the Principles.

Other federal and state courts are addressing electronic discovery. If you are involved in litigation beyond your accustomed state court, prudence suggests inquiring if the more distant court has special procedures or commentary for ESI. About 20 states have e-discovery rules. Note: Even without new rules, many courts are expecting more attorney civility and reasonable cooperation in discovery.

More Information

- » Technology for the Litigator Home
- » News & Developments
- » Articles
- » Case Notes
- » Programs & Materials
- » Newsletter Archive
- » Related Resources
- » Technology for the Litigator Committee
  - • About
  - • Join

CLE & Meetings

8th Annual Pharmaceutical/Medical Device CLE Workshop

November 11, 2010
New Brunswick, NJ

» View Section Calendar
