Discovering ESI: Self-Reliance and FRCivP 26

By Daniel Kegan, <daniel@keganlaw.com>, Kegan & Kegan, Ltd, Chicago

ESI—Electronically Stored Information. Three little letters for three words that should substantially change 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.[1]

The Internet and Electronically Stored Information (ESI) make some discovery 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 non-attorneys may more efficiently surface relevant information.

"Courts cannot and do not expect that any party can meet a standard of perfection. Nonetheless, … By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records—paper or electronic—and to search in the right places for those records, will inevitably result in the spoliation of evidence," *Pension Comm. of Univ. of Montreal Pension Plan v Bank of Am. Secs., LLC*, 685 FSupp2d 456,461 (SD NY 2010) (Judge Scheindlin).

Lay discovery needs to be authorized and supervised by an attorney to avoid possible inadmissibility, sanctions, and ethical violations. Ill. R. Professional Conduct, Rules 4.2 (communication with person represented by counsel), 4.3 (communication with unrepresented person), 8.4(a)(2) (induce misconduct in another).

Failure to understand how your client maintains its ESI opens both client and counsel to severe sanctions. *See generally, Qualcomm Inc v Broadcom Corp.* (Order Declining to Impose Sanctions Against The Responding Attorneys and Dissolving the Order to Show Cause, Magistrate Judge BL Major, SD CA, 05 cv 1958)[2]. Attorneys cannot simply delegate to their clients the responsibility of understanding ESI and planning for ESI discovery. The attorney has a non-delegable responsibility to know.

Several federal statutes restrict covert and deceptive computer and information access. Electronic Communications Privacy Act (ECPA), 18 USC § 2510 includes the Wiretap Act, regulating the intentional interception and disclosure of communications, and the Stored Communications Act,

[1] A discovery plan must state the parties' views and proposals on: (C) any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced. FRCivP 26(f)(3)(C).

[2] Compare the Aug 6, 2007 order (539 FSupp2d 1214 (SD CA, Docket 593) finding of misconduct during litigation with the Apr 2, 2010 order (Docket 998) declining to impose sanctions against attorneys.

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.

The Illinois Eavesdropping Act prohibits eavesdropping, which may include intercepting electronic communications. 720 ILCS 5/14. Generally, all parties to a conversation must consent to its recording, law enforcement officials have some exceptions. *In re Marriage of Almquist,* 704 NE2d 68, 71 (Ill.App. 3d Dist 1998). 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; <http://www.hhs.gov/ocr/privacy/> (26Sept09). Bankendorf, Elliott & Sherry Rollo. *The Higher HIPAA Hurdle*, 46 ISBA Intellectual Property, #3, p. 10, March 2007.

An attorney needs to understand not only the client's information systems—traditional paper and ESI—but also those of the adverse party(ies). Discovery tasks include learning what information the client has, where and how it is maintained, how the discovery-relevant information[3] 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 sufficient parallel questions for the adverse discovery so that reasonable monitoring reduces the opportunity for oversight and intentional abuse.

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 being comfortable with computer and Internet basics[4]. Prerequisite knowledge includes knowing:

Q1. The difference between volatile random access memory (RAM) and non-volatile hard drive memory;
Q2. Generally, how your own email system works;
Q3. Where your email is stored, archived, and who can access to read, copy, or delete.
Q4. How to use email, word processing, spreadsheet.

---

[3] Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense…. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. FRCivP 26(b)(1).

[4] For those who want to understand how a computer really works, see Charles Petzold's *Code: The Hidden Language of Computer Hardware and Software*, 2000.

Q5. Basic database, how it differs from a spreadsheet.
Q6. How your ESI is backed up—all the places and times.
Q7. Differences among an Internet domain, a website, and an email address.
Q8. What html is and the difference between a webpage display and its coding.
Q9. What metadata is[5]

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. LLC v Lexington Ins Co.,* 527 FSupp2d 1355 (MD FL 2009)[6].

PROTECTIVE ORDER

Early in many cases, especially intellectual property cases, a protective order for confidential information will be needed. Some tribunals deem a standard protective order in effect for the parties, while inviting the parties to submit stipulated proposed modifications for their particular situations. ND IL Local Patent Rules, LPR 1.4[7]; Trademark Trial and Appeal Board, Standardized Protective Agreement[8]

Some tailoring of a standard protective order may be necessary, especially for individual parties, pro se parties, non-corporate entities, actively involved inhouse 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 "clawback" provisions should be included. F.R.Evid. 502(b).[9]

Courts are public institutions, and disfavor unneeded confidentiality. Even if a district court grants a protective order, an appellate court may have a stricter standard for maintaining sealed

---

[5] *Lake v City of Phoenix*, 218 P3d 1004 (Ariz, 2009）(if a public entity maintains a public record in an electronic format, then the electronic version, including any embedded metadata, is subject to disclosure under our public records laws).
[6] Inhouse legal secretary affidavit that exporting IQWare data impossible; however IQWare merely a customized MS SQL database, which could readily have been copied and produced.
[7] LPR 1.4 Confidentiality. The protective order found in LPR Appendix B shall be deemed to be in effect as of the date for each party's Initial Disclosures. Any party may move the Court to modify the Appendix B protective order for good cause. The filing of such a motion does not affect the requirement for or timing of any of the disclosures required by the LPR.
[8] <http://www.uspto.gov/trademarks/process/appeal/guidelines/stndagmnt.jsp>
[9] When made in a Federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)."

documents.[10]

Useful provisions for a protective order contemplating ESI production include:

> a) Because Electronically Stored Information (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.
>
> b) ESI shall be produced in a manner to permit reasonable identification of documents, and document sub-parts, or their approximate equivalent for unpaged ESI.
>
> c) Upon receipt, all produced ESI shall be treated initially as Confidential—Attorneys Eyes Only in its entirety until thirty (30) days after receipt, unless the parties expressly agree otherwise. Within thirty (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 document(s) 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 thirty (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.[11] 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. And remember at the conclusion of the case to review and attend to those wrapup provisions.

---

[10] "Sealing Portions of the Record . (a) Requirement of Judicial Approval. Except to the extent portions of the record are required to be sealed by statute (e.g., 18 U.S.C. §3509(d)) or a rule of procedure (e.g., Fed. R. Crim. P. 6(e), Circuit Rule 26.1(b)), every document filed in or by this court (whether or not the document was sealed in the district court) is in the public record unless a judge of this court orders it to be sealed." 7th Cir. Operating Procedures 10 (Dec. 1, 2009).

[11] Eg, ND IL Local Rule LR26.2(g), "Restricted Documents. (g) Disposition of Restricted Documents. When a case is closed in which an order was entered pursuant to section (b) of this rule, the clerk shall maintain the documents that have not been filed electronically as restricted documents for a period of 63 days following the final disposition including appeals. Except where the court in response to a request of a party made pursuant to this section or on its own motion orders otherwise, at the end of the 63 day period the clerk shall return the restricted documents in the sealed enclosure to the attorney or party who or which filed it." Also see, SD NY, Standing Orders of Chief Judge Michael B Mukasey, Oct. 5, 2001 & Apr. 30, 2002.

CASE AND DISCOVERY CONFERENCE 26(F)

FRCP 26(f) outlines the topics to be *knowledgably* discussed by counsel for the early case conference and discovery plan[12]. 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, custodians, and for larger clients business units. If counsel if not conversant with 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. FRCP 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.[13] 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. [14] Even negligent litigation hold practices may subject the party to strong sanctions. Moreover plaintiff's duty to preserve is usually triggered before litigation begins because the plaintiff controls the timing of the suit. *Id.*

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, FRCP 26(b)(1), is often efficiently performed by computerized searching of keywords. Boolean searching can eliminate false hits. For example, in a trademark case, SURVEY NOT LAND.

Common native electronic file formats are text (.txt), Word processing (.doc), Since 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.

---

[12] Judge Colleen McMahon's *Rules Governing Electronic Discovery* provides a good start for preparing for the 26(f) ESI conference (SD NY, May 29, 2007). Also consider non-paged documents, such as databases. <http://www1.nysd.uscourts.gov/judge_info.php?id=73>.

[13] Some attorneys, and clients, seek to inflict cost and pain on the adversary; such a goal interferes with justice, is likely unethical, and if discovered by the court may cause strong sanctions.

[14] *Pension Committee of the University of Montreal Pension Plan v Banc of America Securities, LLC,* 685 FSupp2d 456 (SD NY 2010).

The control group of the client should be interviewed for their individual information habits, including personal communication devices, eg, 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 consistent practice of placing a distinctive short privilege text at the beginning of communications an attorney evaluates as actually privileged. For example, " ## Privileged ##." The multi-line 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 it's 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, nonrelevant (and unlikely to reasonably lead to admissible evidence), and unviewable files.

Some computer files likely will arrive in a compressed state, some as a self-extracting archive.[15] The "parent" compressed files, if any, will exist in the received ESI, and receive sequential numbering. After de-compression, the "children" should receive their own, unique, but related sequential numbers, for example by adding a two-digit decimal when fewer than 99 children are expected (for example "123.45"; use leading zeros for the first nine children, some computer sort routines treat "1" and "01" differently).

Some produced ESI files will not be viewable. This may be due to the file on your client's computer (or that of the adverse party) being accidentally corrupted, it may simply be due to lack of the appropriate viewing application, or infrequently it may be due to intentional evidence destruction.

If you cannot view a file, do not immediately produce it, but 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, such as QuickBooks and Quicken.

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

[15] .http://en.wikipedia.org/wiki/Self-extracting_archive.

sequentially numbered, reviewed, categorized, and processed ready for production, it may be burned to optical disk(s) (DC-ROM or DVD), 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:
first, ensure you preserve the original, unaltered, received version of the file;
second, understand and promptly document what was changed;
third, promptly disclose to adverse counsel 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 you document your chain of custody and only process copies. Of course, also establish and follow a procedure for redundant, multiple, redundant, 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 how to gather past email or how to get two years' of email to the attorney for review.

An attorney should especially attend to helping the client's staff assisting with discovery and document gathering of the broad reach of discovery. Of special concern is that the client's personnel 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. While good attorneys can deal with all the facts, surprises from withheld documents and information create costly difficulties for the client and its case.

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. FRE 1003[16]. For some client computers, it may be helpful for the client to clone the entire hard drive, send the clone to the attorney, and in detail discuss the folder/subdirectory structure and the relevance, and irrelevance, to the litigation.

[16] A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original.

EMAIL AND ATTACHMENTS

Although email usage approaches universal, its users do not always understand where their messages are stored, where the backups are, and how email works.[17] Users retrieve email through a web browser and/or an email client, using POP or IMAP standard protocols or specific proprietary protocols of Lotus Notes or Microsoft Exchange. Diverse utility applications are available to translate email between formats.

RFC-822 was the standard for Internet email for almost two decades, and remains the official standard. RFC-2822 was introduced in 2001. Email formatted under Multipurpose Internet Mail Extensions, MIME, is becoming more common.

Email originally developed as a simple, robust text communication medium, but for some has now 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. Among other concerns, the attachment may require special viewing software (see Chain of Custody, above).

DATABASE

Unlike word processed 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. For example, Quicken and QuickBooks formats have differed over the years.

INDUSTRY-SPECIFIC AND CLIENT-SPECIFIC SOFTWARE

Industry-specific and client-specific software requires specific attention during the discovery conference. Beyond user guides and technical specifications, confidentiality and access needs to be determined. Obtaining an authorized version of licensed software needs to 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, often with a letter prefix identifying the producing entity. However, it becomes inefficient for ESI documents to print them to paper, number the paper, and then rescan the documents to electronic form. It is inefficient even if the ESI documents are not rescanned. Additionally, database documents do not readily print to paged format.

[17] <http://en.wikipedia.org/wiki/Email>

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.

We had a simple, small utility program written that recursively numbers all the files and/or folders within a chosen set of hierarchical folders, on a Macintosh computer.[18] The conservative procedure was:
a) copy original ESI data, separate the originals and modify the copy;
b) run the recursive script on the copied data;
c) record the last used number, to help set the initial number for the next batch of received discovery documents.

KEYWORD AND BOOLEAN SEARCHING

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

Virginia Systems' Sonar Professional provides a robust Boolean text retrieval application for Windows and Macintosh; its WebSonar provides a similar web ability that may be (securely) accessed by authorized people in differing locations.[19] Complex search queries using synonyms, phonetic matches, wild cards and word proximities can be easily created with Sonar. A typical query would look for any synonym of the word "Bronco" ("utility vehicle", "sport vehicle", "Ford", "truck", etc.) within 10 words of either June 17th or any word starting with "injur" (injury, injuries, and so on).

Sonar provides associated word and associated subject display. All words or subjects found near a search phrase can be displayed by relevancy or in alphabetical order. For example, if "Suspect" was your search phrase and "knife" appeared frequently near it, then "knife" would appear near the top of the Associated Word list. Selecting "knife" would then take you to the places in the documents where "knife" and "Suspect" appear. Associated Subjects is similar, but the English around the search phrase is parsed and any subjects are extracted. For example, a subject found near "Suspect" might be "John Q. Smith" or "Switchblade knife."

PRIVILEGE REVIEW

In the past, many attorneys did not insist on production of a privilege log, trusting the

[18] For our Macintosh computers, we used an earlier version of Autograph Systems' IconIDr, http://www.iconidr.com. Windows users may find Bulk Rename Utility useful. http://www.bulkrenameutility.co.uk/Main_Intro.php.
[19] < http://www.virginiasystems.com/products.html#pro>

professionalism of adverse counsel, and wishing to save their own clients the expense of such work. With ESI, attorneys should expect that some privileged documents will be inadvertently produced. To support a clawback 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. FRCP 26(b)(5)(A)(ii).

Most clients do not label their communications to attorneys as privileged, perhaps not even as confidential. And not all communications with an attorney are privileged.[20] Epstein considers the most useful definition of the attorney-client privilege that proposed in 1972 as Federal Rule of Evidence 503(b) by the Chief Justice of the US Supreme Court (*id.* at 4):

> A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services to the client, (1) between himself or his representative and his lawyer or his lawyer's representative, or (2) between his lawyer and the lawyer's representative, or (3) by him or his lawyer to a lawyer representing another in a matter of common interest, or (4) between representatives of the client or between the client and a representative of the client, or (5) between lawyers representing the client. (*Id.* at 3).

Federal Rule of Civil Procedure 26(b)(3) provides a qualified protection from discovery in civil actions when materials are 1) documents and tangible things otherwise discoverable; 2) prepared in anticipation of litigation or for trial, and 3) 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 4) substantial need for the materials; and 5) inability to obtain the substantial equivalent of the information without undue hardship. Epstein 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 US 495 (1947); *Upjohn Co v United States,* 449 US 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.

One effective form of Privilege Log has 12 columns:
1) Sequential number; 2) Date; 3) By/From; 4) For/to; 5) Others; 6) Document Type (eg. email, web pages, notes, letter, etc); 7) Purpose; 8) Attorney Advice (Yes or No); 9) Subject; 10) Business related; 11) Privilege (Ac Attorney client communication; Wp Attorney work product); 12) Confidentiality (C Confidential; Hc Highly; Aeo Attorneys Eyes Only; None).

[20] *See* Epstein, Edna Selan, The Attorney-Client Privilege and the Work-Product Doctrine, 5th edn, ABA 2007.

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:

> Electronically Stored Information (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.

PRODUCTION TO ADVERSE COUNSEL

In the ideal, there would be no issues that arise in transmitting ESI discovery to adverse counsel.[21] In the ideal, counsel agree on the format for producing ESI information would during the early Rule 26 discovery conference.[22] Practically, one or more of the counsel may have overlooked these production issues.

ESI IN DEPOSITIONS

Many courts currently are more comfortable with paper-based evidence than electronic evidence. While ESI may be gathered, evaluated, produced, and sometimes presented in deposition, to present as an exhibit to a court, ESI evidence may need to be reduced to paper at some stage of the litigation. Know your data and its formats; avoid a deposition disaster as did occur from careless printing of ESI spreadsheets:

> Q. These are typically Excel spreadsheets, correct?
> A. I don't know.
> Q. All of these appear to be the same thing.
> A. I don't know what these are. What is this? Is this some type of problem again with the printing? As you see, these don't look like those (indicating).
> Q. Yeah. They—on a format-wise, I agree with you; they do look somewhat different.
> Q. Is there anything here that—what is this document?
> A. It looks like a bunch of lines. I mean, it looks like a skewed—like we talked about, an application for payment.
> Q. Okay. Is there anything there substantively that would tell you one way or

[21] While the federal rules only require offering the opportunity "to inspect and copy," counsel often provide copies of discovery documents--as a professional courtesy and for the reciprocal cost reduction. FRCP 34 (a)(1).

[22] A document request "(C) may specify the form or forms in which electronically stored information is to be produced." FRCP 34(b)(1)(C).

another whether this was the final request?
A. Not with the way this thing's skewed. It'd be impossible.

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.[23] Advocates of cloud computing emphasize the economies of scale, lower fixed investment, and the ability of the vendors to "chase the cheapest electrons" and have labor and electricity provided by the least expensive locales in the world.

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 sub-vendor 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 (SaaS) 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. Social networking creates Internet communities of people sharing a common interest. Facebook began in 2004 to connect Harvard students, expanded to other colleges, and now is the world's second most popular website, attracting more than 400 million active users, half of which log on in any given day.[24] LinkedIn launched in 2003 as a business-oriented social network, and now has more than 65 million registered users in more than 200 countries.[25] Twitter is currently a dominant social network for brief, under 141 character, comments; YouTube is a leading site for user-posted video. There are many other social networks, including Yahoo! Groups[26] and Google Groups,[27] which readily enable novice computer users to establish a social networked group with virtually any focus, from as small as a family to as large as international groupings.

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 non-company email, and all their Internet screen names,

---

[23] <http://en.wikipedia.org/wiki/Cloud_computing>
[24] <http://www.facebook.com/press/info.php?statistics>
[25] <http://en.wikipedia.org/wiki/LinkedIn>.
[26] <http://groups.yahoo.com/>.
[27] <http://groups.google.com/>.

email addresses, and perhaps passwords. In an important case, your adversaries are likely to be finding such Internet information.

Computer Forensics. If forgery, evidence tampering, or related misdeeds are suspected a forensic examination may be appropriate.[28] The goal of computer forensics is to explain the current state of a digital artifact—a computer system, storage medium such as hard disk or CD-ROM, an electronic document such as an email message or PDF or a 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 pre-existing work may be shown by the identical file creation dates for the original electronic work and the suspect derivative work.

Under Illinois PA 96-262 it is a Class 4 felony for a person required to register as a sex offender to access or use a social networking website. Under Illinois PA 96-362 sex offenders are prohibited from knowingly using any computer scrub software on any computer that the sex offender uses.

CAUTIONS WITH DOCUMENT SERVICES

Commercial document services may not be familiar with the wider variety of ESI formats that can appear in litigation, and thus may need guidance. Some problems--and easy solutions-- we have encountered from adverse document productions include:

* Counsel transmitting an unreadable CD-Rom from an uncooperative adverse party (counsel should check ESI before transmitting);
* Document service claiming they could not copy an advertising CD-ROM (it only had a printed label, no electronic data);
* Document service paper copies ("blowback") of spreadsheet malformed—see deposition transcript above (look at discovery product more than the night before a deposition);
* Inability of document service to read older floppy disk formats (find appropriate computer specialist that retains older equipment).

CONTINUING TRADITIONAL (PAPER) ISSUES

Although ESI brings new discovery issues such as metadata and encryption, the traditional paper-focused discovery concerns remain, including without limitation, preservation letters, non-party discovery, authentication and admissibility, and hearsay.

ADDITIONAL RESOURCES

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

[28] <http://en.wikipedia.org/wiki/Computer_forensics>.

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. < http://www.thesedonaconference.org/>. 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.[29] 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 FRCP 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.[30]

May 2010 a report on phase one of the Seventh Circuit Electronic Discovery Pilot Program was released[31]. 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[32]. 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[33]

Even without new rules, many courts are expecting more attorney civility and reasonable cooperation in discovery.

CONCLUSION

Goldilocks remains a useful guide in producing, objecting, and responding to discovery.[34] 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.

---

[29] < http://www.7thcircuitbar.org/displaycommon.cfm?an=1&subarticlenbr=109>

[30] Principles include Zealous Representation, Proportionality, Meet and Confers, E-Discovery Liaison, Preservation, Scope of Preservation, Identification of ESI, Production Format, and Education.

[31] < http://www.7thcircuitbar.org/associations/1507/files/05-2010%20Report%20on%20Phase%20One%20with%20Bookmarks.pdf>

[32] Eg., Electronic Discovery in the New York State Courts, February 2010.

[33] Klinger, Elenore Cotter, States with e-discovery rules growing while some 'wait and see,' ABA, Winter 2010.

[34] <http://en.wikipedia.org/wiki/Goldilocks>.

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.

Biography. Daniel Kegan, PhD, JD, focuses on intellectual property and providing second opinion counseling to other professional firms. He is admitted to the United States Supreme Court, on the Lanham Act (Trademark) Mediation Panel of Neutrals for the Northern District of Illinois, a qualified expert witness on forensic survey research, and is a licensed (organizational) psychologist in Illinois and Massachusetts. He obtained the first US registration of a touch trademark and the first US copyright registration for iconic, non-hierarchical computer programming.

An abridged version of this article appeared as Discovering ESI: Self-Reliance and Rule 26, 5 *Technology for the Litigator* (ABA Litigation Section, November 2010).