E-Discovery Risk Management Is the "New New Thing"

KBA Bench and Bar September 2005. Vol. 69, No. 5, page 24

When a billionaire wins a $1.45 billion judgment as Ronald Perelman recently did in a law suit against Morgan Stanley it does not warm the heart, but it does catch the eye. The suit is fascinating in itself involving allegations of fraudulent sale of stock, but what is instructive about it is the way discovery of electronic documents was mismanaged by Morgan Stanley and apparently its lawyers.

During the suit Morgan Stanley continued its policy of overwriting e-mail every 12 months notwithstanding an SEC requirement to retain e-mails for two years. This led to an agreed order for Morgan Stanley to produce backup tapes, review e-mails, conduct searches, provide responsive e-mails, and provide a privilege log. Morgan Stanley was required to certify compliance with the order which was done while knowing that 1,423 backup tapes had been found in an off-site location that had not been reviewed. There is more, but you get the picture – a real horror story of botched e-discovery. The judge found willful and gross abuse of discovery obligations, gross negligence, willful disobedience of an agreed order, and that the certification of compliance was false. The plaintiff asked for and got an adverse inference instruction and an award of $1.45 billion. There is talk of a malpractice claim against Morgan Stanley's lawyers.[i]

The purpose of this article is to alert you to the growing malpractice and bar discipline risks involved in e-discovery requests for records maintained in electronic format – *e-documents*. Don't think this is an issue only for large litigation firms. With the explosion of the ways that information is stored electronically in both business and private endeavors, e-discovery requests can occur in virtually any litigation undertaken regardless of the nature or complexity of the case. What follows is an overview of the lawyer's role in e-discovery from the perspective of ethics rules, the malpractice standard of care, and methods for managing the risk. This is a dynamic aspect of modern law practice driven by rapid technological advances in electronic data creation that requires constant attention. CLE does have its uses.

The Lawyer's Role in E-Discovery

Lawyers assist clients with e-discovery both before and after the fact of a law suit. Before the fact lawyers work with clients in establishing records retention and destruction programs. This is when a proactive lawyer is of great service to a client by helping establish programs that protect against claims of spoliation; *i.e.*, destruction of evidence, material alteration of evidence, and failure to preserve evidence. Destruction of documents in paper or electronic format is the most sensitive aspect of any program. Risk managing this kind of advice is the subject of my article "*Shredded Any Good Documents Lately?*"[ii] That article provides information on advising clients on records retention programs and covers law and ethics rules applicable to records destruction. It is suggested reading to supplement this article which concerns primarily e-discovery issues after a law suit is filed.

After suit is filed and a client is in receipt of an e-discovery request, the lawyer's role is to assure a timely, good faith response. Depending on the complexity of the client's e-records this can be anything from careful oversight to hands-on, day-to-day management of the whole process. It is important to understand just how complex this can be. You must know the answer to these questions:

> *Where are the e-documents?* E-documents can be stored in desktop computers, laptop computers, hand-held computers, mainframe computers, network servers, floppies, CD-ROMs, DVDs, backup tapes, etc. They can all be in a central location or dispersed off-site in branch offices, employee homes, storage facilities, etc.
>
> *Are the e-documents accessible?* E-documents used in current operations of the client are usually readily accessible, but older files may be damaged or readable only with obsolete software that is no longer supported by the supplier. Even if e-documents are accessible, can they be indexed or organized in a way that permits accurate computer identification of responsive documents? E-mail proliferates in such an *ad hoc* manner that it virtually defies indexing. Often meaningful review can be accomplished only by reading all e-mails in the system – a time consuming and expensive method.
>
> *How much of it is there?* We all know that e-documents are proliferating exponentially. There are estimates that thirty-five billion e-mails will be sent a day in 2005. There can be one copy of an e-document or hundreds of copies in numerous locations. The point is that the potential for receiving a crushing e-discovery request grows everyday. Responding can become overwhelming for the most diligent client and lawyer.

Rules and Standards

Kentucky Rule of Professional Conduct (KRPC), Rule 1.1, Competence, provides "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[iii]

There is little practical difference between this rule and the malpractice standard of care for Kentucky lawyers:

> ...the standard of care is generally composed of two elements - care and skill. The first has to do with care and diligence which the attorney must exercise. The second is concerned with the minimum degree of skill and knowledge which the attorney must display....the attorney's act, or failure to act, is judged by the degree of its departure from the quality of professional conduct customarily provided by members of the legal profession.[iv]

My point in setting out these two basic concepts familiar to us all is to ask you to read them in the context of the complexities of e-discovery. Is your knowledge of e-document production, storage, retrieval, and review adequate for competent supervision of an e-discovery request? Do you possess the necessary skill in working with e-documents to meet your professional responsibility and avoid a malpractice claim?

While a number of other professional conduct rules can come into play in e-discovery, KRPC 1.6 and KRPC 3.4(a) warrant special consideration:

- KRPC 1.6, Confidentiality of Information, invokes the duty to avoid negligently revealing in e-documents confidential information not properly discoverable (think metadata), work product, and attorney-client privileged communications. Failure to remove any qualifying confidential e-documents from those produced for an opponent could be malpractice.

- KRPC 3.4 (a), Fairness To Opposing Party And Counsel, provides "A lawyer shall not: (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act; …."

  Comment (2) to the rule provides "Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying evidence is also generally a criminal offense. **Paragraph (a) applies to evidentiary material generally, including computerized information**." *(emphasis added)*

  Obviously, violation of this rule can result in severe bar discipline.

Not to be overlooked is that criminal law applies if the management of e-discovery amounts to tampering with evidence, hindering prosecution or apprehension, and obstruction of justice.[v] Again being technically competent is crucial. Tampering with e-documents is much easier done than with paper documents and harder to detect. The ability to discern when this is happening is an important skill – if in doubt, use experts.

Applying Risk Management Methods to E-Discovery

1. Get Informed

Educate yourself and clients on how the discovery process applies to electronic records keeping and the need to preserve and retrieve responsive data in a timely manner. This requires at least a basic understanding of the technology involved in generating and

storing electronic records and an appreciation of your clients' computer systems and records management programs. You do not have to be an expert in computer technology to be competent to accept a matter that involves e-discovery, but you do have to know what you are doing. It is critical to understand what you know about electronic records keeping systems, what you don't know, and the difference between the two. Be quick to leverage your competence by bringing in experts to assist in determining effective ways to access a system to produce responsive e-documents. Make part of your client intake procedures an assessment of the potential in the matter for an e-discovery request. Tell clients up front what is involved, how time consuming and expensive it can be, and that there could be a need for technology experts that are costly. This is the time to inform clients about the danger of spoliation of evidence and its consequences.

2. Be Proactive

Whenever possible assist clients in developing their records retention programs. For more information on this aspect of risk management read "*Shredded Any Good Documents Lately?"* The following paragraph from that article is offered here to show what is involved in developing a records retention program.

> Of course, lawyers need some knowledge of an adequate records retention-destruction program to competently advise on the legal considerations. A typical program:
> - Covers all paper and electronic forms of record keeping the enterprise employs.
> - Involves information technology personnel in the system design and implementation to assure that electronic documents can be retrieved or confirm that all copies of an electronic record are destroyed.
> - Retains business records required for regular use.
> - Retains all records required by law including those related to pending litigation.
> - Provides upon notice of litigation a procedure for identifying records required for retention and protecting them from routine destruction.
> - Retains records identified as related to foreseeable or potential litigation.
> - Systematically collates retained records in a readily retrievable paper and electronic filing system format.
> - Provides for the destruction of all other records including e-mail on a reasonable schedule consistent with good business practices.
> - Documents the program's design, updates, implementation, and compliance enforcement.(*footnote omitted*)

3. Prevent Spoliation

Be sure that clients and all involved employees understand the significance of spoliation of evidence and that their duty to preserve evidence during litigation also includes those situations when the client should reasonably know that evidence may be pertinent to potential litigation. Sanctions for spoliation and abuse of discovery requirements include criminal charges, contempt orders, case dismissal, evidence preclusion, instructions on adverse inferences or presumptions, in some states the new tort of intentional spoliation of evidence,[vi] and bar complaints. (If a lawyer is responsible for spolia-

tion or careless response to an e-discovery request, a malpractice claim is also a possibility.)

4. Know How to Supervise E-Discovery Responses

It is the ultimate duty of the parties to a suit to preserve and provide responsive documents to discovery requests. As a practical matter lawyers for the parties bear the burden of showing to a court that a good faith effort was made to timely produce and that any failure to do so was excusable. A dissatisfied court may impose sanctions on both the parties and their lawyers. In short e-discovery response is a joint effort by client and lawyer.[vii]

First, an e-discovery horror story: *Metropolitan Opera Association, Inc. V. Local 100, Hotel Employees and Restaurant Employees International Union*[viii] involved a claim by Metropolitan that Local 100 improperly involved it in a labor dispute between Local 100 and Restaurant Associates Corporation, the Metropolitan's food service provider. The decision is a lengthy description of both incompetence and apparent bad faith on the part of Local 100 and its lawyers in responding to e-discovery. The following paragraphs from the decision are a lesson on how not to supervise discovery:

> The court concludes that defendant and its counsel failed in a variety of instances to conduct any reasonable inquiry into the factual basis of its discovery responses.... Such an inquiry would have required, at a minimum, a reasonable procedure to distribute discovery requests to all employees and agents of the defendant potentially possessing responsive information, and to account for the collection and subsequent production of the information to plaintiffs.
>
> Counsel's primary defense to their Rule 26(g) violation is to assert that there is no requirement that counsel "personally supervise every step of the discovery process" and that "counsel is expected to rely on the client's initial document production." While, of course, it is true that counsel need not supervise every step of the document production process and may rely on their clients in some respects, the rule expressly requires counsel's responses to be made upon reasonable inquiry under the circumstances. *See* Fed.R.Civ.P. 26(g) Advisory Committee Notes to 1983 Amendment (attorney's certification under Rule 26(g) signifies "that the lawyer has made a reasonable effort to assure that the client has provided all the information and documents available to him that are responsive to the discovery demand."). Here, there is no doubt whatsoever that counsel failed to comply with that standard in that, among other things, counsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, what constitutes a "document" or about what was specifically called for by the Met's document requests; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who (at least until July 2001) did not

> even understand himself (and was not instructed by counsel) that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had "establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests," and (5) in the face of the Met's persistent questioning and showings that the production was faulty and incomplete, ridiculed the inquiries, failed to take any action to remedy the situation or supplement the demonstrably false responses, failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced. Indeed, given the almost complete disconnect between counsel (who had the document requests but knew nothing about the documents in the Union's possession other than that the files were in disarray and there was no retention system) and defendants (who had the documents but were entirely ignorant of the requirements of the requests), there is simply no way that any discovery response made by counsel could have been based on a reasonable inquiry under the circumstances. (*footnotes and citations omitted*)

Zubulake v. UBS Warburg LLC [ix] involved a charge of gender discrimination. As it progressed the judge determined that UBS, in spite of its lawyer's clear instructions to retain relevant electronic information, deleted relevant e-mails and failed to produce other discoverable e-mails. Before ordering sanctions the judge provided this analysis of a lawyer's e-discovery duties:

> In sum, counsel has a duty to effectively communicate to her client its discovery obligations so that all relevant information is discovered, retained, and produced. In particular, once the duty to preserve attaches, counsel must identify sources of discoverable information. This will usually entail speaking directly with the key players in the litigation, as well as the client's information technology personnel. In addition, when the duty to preserve attaches, counsel must put in place a litigation hold and make that known to all relevant employees by communicating with them directly. The litigation hold instructions must be reiterated regularly and compliance must be monitored. Counsel must also call for employees to produce copies of relevant electronic evidence, and must arrange for the segregation and safeguarding of any archival media (*e.g.,* backup tapes) that the party has a duty to preserve. Once counsel takes these steps (or once a court order is in place), a party is fully on notice of its discovery obligations. If a party acts contrary to counsel's instructions or to a court's order, it acts at its own peril.

Ms. Zubulake received a jury award of $29,000,000.

The best way to meet these duties is to have litigation response plan for clients that includes procedures for a litigation hold notice. The plan should:

> [Q]uickly identify the types and location of records, both paper and electronic, in the companies possession, custody or control that are potentially relevant to the litigation or investigation. The critical parts of the litigation response plan are the instructions for identifying, capturing and preserving, in the format in which they were maintained in the normal course of business if possible, the company's relevant records so as to maintain the status quo of the records during the pendency of the action.
>
> ….
>
> [T]he company should have a process under which it can quickly evaluate whether it needs to suspend, in whole or part, the document-destruction component of its retention policy, and to distribute notice to all employees who are likely to have relevant records in their possession, custody or control. Such notices generally referred to as preservation notices, should advise employees of the pendency of the litigation or investigation, their obligation to preserve relevant records and the suspension of the usual retention policy.
>
> ….
>
> The preservation notice should also include, in clear, concise and bold language, a description of the types of records – by subject if necessary -- that are relevant, and therefore subject to preservation, and instructions on how to preserve them. It is also important that the preservation notice inform employees that they must preserve relevant records until advised otherwise.[x]

Finally, one commentator recommends this protocol for ensuring that relevant documents and data are preserved:

1. Advise your clients to adopt and follow an electronic document retention policy.
2. Retain an expert, if necessary, to map your client's computer network and determine where information is stored.
3. Delete data pursuant to the policy; make sure the data is actually deleted.
4. Develop policies to avoid saving unnecessary information.
5. Be wary of the existence of metadata.
6. Pay special attention to digitalized voicemails and e-mails.
7. In the event of a lawsuit or claim, institute a means to preserve all relevant evidence.
8. Anticipate discovery requests.
9. Consider cost-shifting.
10. If the court permits an adverse party to invade your client's computer, develop a protocol to protect confidential or privileged information, prevent damage and avoid interference with on-going operations.[xi]

5. Protect E-Documents that are Attorney-Client Privileged, Lawyer Work Product, or Non-Discoverable Client Confidential Information.

Protecting against the inadvertent release of non-discoverable documents is part of any discovery response. The sheer magnitude of saved e-documents by many clients can make this obvious duty onerous in the extreme, but all released e-documents must be

screened to assure that privileged documents are not released. This is a relatively straight forward proposition for attorney-client privileged documents and attorney work product. It may, however, require training of client employees to recognize these e-documents and lawyer review to assure accurate results.

The current major issue in protecting client confidential information in e-discovery concerns metadata. A New York State Bar ethics opinion[xii] describes the issue well and offers sound guidance on a lawyer's metadata professional responsibility. In the absence of any known Kentucky guidance the following extracts from the New York opinion should be helpful in understanding and dealing with metadata issues in e-discovery:

> Word-processing software commonly used by lawyers, such as Microsoft Word and Corel WordPerfect, include features that permit recipients of documents transmitted by e-mail to view "metadata," which may be loosely defined as data hidden in documents that is generated during the course of creating and editing such documents. It may include fragments of data from files that were previously deleted, overwritten or worked on simultaneously. Metadata may reveal the persons who worked on a document, the name of the organization in which it was created or worked on, information concerning prior versions of the document, recent revisions of the document, and comments inserted in the document in the drafting or editing process. The hidden text may reflect editorial comments, strategy considerations, legal issues raised by the client or the lawyer, legal advice provided by the lawyer, and other information. Not all of this information is a confidence or secret, but it may, in many circumstances, reveal information that is either privileged or the disclosure of which would be detrimental or embarrassing to the client. ..... For example, a lawyer may transmit a document by e-mail to someone other than the client without realizing that the recipient is able to view prior edits and comments to the document that would be protected as privileged attorney-client communications. Or, more dramatically, a prosecutor using a cooperation agreement signed by one confidential witness may use the agreement as a template in drafting the agreement for another confidential witness. The second document's metadata could contain the name of the original cooperating witness, and if e-mailed, could expose that witness to extreme risks.
>
> ….
>
> When a lawyer sends a document by e-mail, as with any other type of communication, a lawyer must exercise reasonable care to ensure that he or she does not inadvertently disclose his or her client's confidential information. What constitutes reasonable care will vary with the circumstances, including the subject matter of the document, whether the document was based on a "template" used in another matter for another client, whether there have been multiple drafts of the document with comments from multiple sources, whether the client has commented on the document, and the identity of the intended recipients of the document. Reasonable care may, in some circum-

> stances, call for the lawyer to stay abreast of technological advances and the potential risks in transmission in order to make an appropriate decision with respect to the mode of transmission.
>
> ….
>
> Lawyer-recipients also have an obligation not to exploit an inadvertent or unauthorized transmission of client confidences or secrets. In N.Y. State 749, we concluded that the use of computer technology to access client confidences and secrets revealed in metadata constitutes "an impermissible intrusion on the attorney-client relationship in violation of the Code."
>
> ….
>
> Some commentators have suggested that a lawyer has an affirmative duty to remove metadata whenever documents are exchanged with opposing counsel or disclosed to the public. *See, e.g.,* David Hricik & Robert R. Jueneman, The Transmission and Receipt of Invisible Confidential Information, 15 The Professional Lawyer no. 1, p. 18 (Spring 2004) ("To comply with their duty of confidentiality, lawyers should take steps to remove metadata from documents exchanged with opposing counsel or disclosed to the public"). While exercising reasonable care under DR 4-101 may, in certain circumstances, require the lawyer to remove metadata (for example, where the lawyer knows that the metadata reflects client confidences and secrets, or that the document is being sent to an aggressive and technologically savvy adversary), in general the level of care required varies with the particular circumstances of the transmission. (*footnotes omitted*)

Notwithstanding the New York opinion, it is anything but clear that lawyers have a professional duty not to exploit metadata. To protect against this risk metadata can be removed from e-documents in native format (an e-document in the form in which it was originated) or the e-documents can be converted to petrified images such as PDF or paper documents. Of course, the specifics of the discovery request and court instructions must be considered to avoid a spoliation allegation. Samantha L. Miller in her article "*Metadata is major factor in discovery*"[xiii] offers this advice in deciding what format to release e-documents:

> There is no one format that is appropriate for all occasions. Attorneys should consider the following factors when determining the format or formats to use for production: requirements imposed by statute, rules, regulations and case law; the dictates of any applicable court orders; approaches mandated by governmental organizations such as the Justice Department and the Federal Trade Commission; opposing counsel's production request or preferences; the ways in which the producing attorneys intend to use the e-discovery during the course of the litigation; redaction requirements; usability of e-discovery produced in the various formats; costs associated with producing e-discovery in the various formats; and agreement of the parties. If there is a finite amount of e-discovery requested and no file format stipulated, attorneys might do well to produce it in TIFF, PDF or paper format, especially if it is

felt that metadata contained in e-mails and/or documents are telling. Some programs provide tools for quickly converting native files to petrified images.

Summing Up

Not covered in this article are the issues of voice mail discovery, discovery involving inspection of a client's computer system, cost shifting to the requesting party, and rules revision efforts at the ABA and at the federal and state level to more directly address e-discovery. I point this out to stress the scale and fluidity of the situation. As technology progresses so does the complexity of risk managing e-discovery. So I conclude with the same message I began with – e-discovery is risky business. The scope of e-discovery now reaches virtually all areas of litigation. No matter the size of your firm or the kind of litigation you practice, there is the potential for an e-discovery request. My hope is that this article will give you a jump start on implementing good risk management practices as you address the latest "New New Thing" in this exciting profession we enjoy.

---

[i] *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co*., Inc., 2005 WL 679071 (Fla. Cir. Ct., 3/1 2005)

[ii] Kentucky Bar Association *Bench & Bar* Vol. 66 No. 5, page 55, Sep. 2002; available on Lawyers Mutual's website in the Risk Management section at www.lmick.com.

[iii] The Kentucky Rules of Professional Conduct are contained in SCR 3.130.

[iv] *Daugherty v. Runner*, 581 S.W.2d 12 (Ky., 1979).

[v] See, KRS 520.120, Hindering Prosecution or Apprehension in the First Degree, a Class D felony; KRS 520.130, Hindering Prosecution or Apprehension in the Second Degree, a Class A misdemeanor; and Sarbanes-Oxley Act of 2002 (H.R.3763), Title VIII – Corporate and Criminal Fraud Accountability.

[vi] In *Monsanto Co. v. Reed*, 950 S.W.2d 811(Ky., 1997), the Kentucky Supreme Court rejected the tort of spoliation holding that adequate remedies were provided by evidentiary rules, missing evidence instructions, and civil penalties.

[vii] *See generally*, Brady and Cohen, *Ethics rules and electronic discovery*, The National Law Journal, page 13, 11/22/2004.

[viii] 212 F.R.D. 178 (2003).

[ix] 2004 WL 1620866 (S.D.N.Y.), 94 Fair Empl.Prac.Cas. (BNA) 1, 85 Empl. Prac. Dec. P 41,728.

[x] Brady and Cohen, *Protecting against claims of spoliation*, The National Law Journal, page S1, 7/5/2004.

[xi] Frank H. Glasser, *Electronic Discovery: New Issues For Risk Management*, manuscript article, ABA 2004 National Legal Malpractice Conference Materials at page 287(4/28/2004).

[xii] The New York State Bar Ass'n Comm. on Professional Ethics, Op.782, 12/8/2004.

[xiii] The National Law Journal, page S1, 8/16/2004.