E-DISCOVERY: BURDENSOME, EXPENSIVE, AND FRAUGHT WITH RISK

If your company is involved in civil litigation, the Federal Rules of Civil Procedure regarding preservation and production of electronic documents ("e-docs") require you to pay close attention to your computer system, your electronic records, your record retention policies, and how you respond to discovery requests. The case law regarding discovery of e-docs is also evolving, and affects how you must preserve your data, especially when there is even a possibility of litigation. The case law regarding who bears the work burden and expense of searching for and producing e-docs is also changing, and requires that you plan ahead and develop an organized system that will help you to respond to discovery requests and avoid sanctions.

E-Discovery Under the Federal Rules of Civil Procedure

Your lawyers must follow these rules in Federal lawsuits. Most states have also adopted versions of these rules, so expect the rules to apply in some form in state court cases as well. The Federal amendments regarding e-discovery took effect on December 1, 2006. In a nutshell, the Rules include the following:

- "Electronically stored information" is required to be produced just like paper; there is no longer any doubt that you must search for it and produce it (with some limitations) just like you would if it was on paper; this includes your e-mail, your back-ups and all storage devices – see below;
- The parties are required to meet and resolve issues regarding production of e-docs before formal discovery begins – that means that your lawyer needs to have an understanding of how your e-docs are preserved and what is involved in recovering them, before the initial scheduling conference with the Court;
- When your lawyer files an "initial disclosure" with the court (relevant documents about the case, filed before formal discovery begins), e-docs must be included;
- When you answer Interrogatories, respond to a Request for Production, or respond to Requests for Admission, e-docs must be reviewed and the information included in your Answers must reflect the content of those materials;

- When you present a representative to testify for the company at a deposition, the witness should understand what e-docs are available, and to some extent, the content of those e-docs (depending upon the scope of the deposition notice).

Developments in Case Law

Courts are looking at e-docs and the Federal Rules, and making decisions that increase your burdens in discovery and threaten your company with serious sanctions if you do not comply fully. Some of the most significant decisions include:

Columbia Pictures v. Justin Bunnell, et. al., (C. Dist. Ca., 2007): Court ordered defendants to preserve and produce transient data stored in random access memory ("RAM"), despite defendants' arguments that the data was not normally stored by the company and was so transitory that it would be unduly burdensome to preserve. In its ruling, the court noted that the defendants had the technological ability to store and manipulate such data and that it would only amount to about one gigabyte of information per day. The court decided against sanctions for previous failure to preserve because there was no precedent for ordering preservation of RAM, but did require the defendant to preserve RAM going forward.

Williams v. Taser International, Inc., (U.S. Dist. Ct. Ariz., 2007): The parties deadlocked on the scope of an e-mail search, and the court ordered defendant Taser to run 21 specific searches to identify a collection of "presumptively responsive documents." Taser then had 30 days from entry of the Order to produce all such documents and 45 days to complete any associated privilege review of these documents and produce a comprehensive privilege log to the requesting party. Taser was barred from excluding presumptively responsive documents from the production on any grounds other than privilege.

Muro v. Target Corp., (N. Dist. Ill., 2007): Court granted plaintiff's motion to compel production of Target's e-mail correspondence based upon the insufficiency of Target's privilege log, even though some of the e-mails contained legal opinions.

United Med. Supply Co., Inc. v. United States, (U.S. Ct. of Appeals, Federal Circuit, 2007): This case illustrates the consequences faced by litigants who do not produce everything they should have. An attorney for the government sent out a litigation hold e-mail to various medical facilities but did not follow up to confirm that it had been received and that the facilities were responding to the request. Counsel for the government then made representations to the court that were based on inaccurate information about what documents were actually being preserved and produced. When it turned out that certain documents were not being preserved the court imposed sanctions. The sanctions included the inability of the government to cross-examine the plaintiff's expert on various aspects at trial and requiring the government to reimburse the plaintiffs for any additional discovery-related costs due to this spoliation issue.

Zubulake v. UBS Warburg, LLC, 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake II)*, and an earlier decision in the same case, at 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (*Zubulake I*), seminal case law in this area, established that:

1. A litigant is obligated to **preserve** electronic documents when some probability of litigation arises; the "probability" required is a minimum standard – "more than a possibility" ;
2. Counsel is obligated to work closely with the litigant's IT personnel, and to gain a complete understanding of the client's data retention systems;
3. Once the duty to preserve e-docs arises, a party must put a "**litigation hold**" in place, preserving all relevant e-docs (including e-mail and back-ups); this means all existing deletion/destruction/overwrite systems must be suspended and all potentially relevant documents must be preserved. This process must be repeated at reasonable intervals during the litigation, to assure that new employees are advised, existing staff is reminded, and new equipment is properly included;
4. **The destruction of electronic documents warrants sanctions**;
5. Directors and officers must communicate the "hold" to employees who may have such electronic documents, and advise them NOT to delete;
6. Failure to do so is negligence at least, and probably **spoliation**;
7. Sanctions can include costs, monetary sanctions, limiting instructions, preclusion orders, default judgments, and/or dismissal.

Bottom Line: Once there is a fair chance that litigation will follow, it is up to senior management to make certain that key e-docs are comprehensively identified and preserved, and that all automatic deletion systems that affect those e-docs are suspended. If management fails to do so, it risks losing the case on that failure alone, without a trial on the merits, or incurring severe sanctions that will cost money or cripple its ability to litigate. The client is then obligated to designate an appropriate IT person or persons to work with counsel, to assure that all documents are identified, preserved, and searched as required for production. This selection is critical – as is counsel's ability to understand exactly what exists and how to retrieve it. Sloppy work will lead to the same risk of sanctions.

Coleman Holdings v. Morgan Stanley & Co. 2005 WL 679071 (Fla. Cir. Ct. March 1, 2005): This case illustrates how severe sanctions can be when there is a substantial failure to comply with the rules. Morgan Stanley was found to have made misrepresentations to the Court regarding the completeness of its production of e-docs after failing to produce e-mail attachments and "newly discovered" back-up tapes. The individual coordinating the e-doc search did so improperly, and was placed on leave after the errors were discovered. The Court imposed sanctions, and an adverse $1.3 billion verdict followed.

Phoenix Four, Inc. v. Strategic Resources Corp., et al., No. 05 Civ. 4837, 2006 WL 1409413 (S.D.N.Y. May 23, 2006): Court imposed monetary sanctions against the defendants and their lawyers for failing to produce electronic data that was on an unknown partitioned section of the server. The data was not produced to the plaintiffs until after the plaintiff had conducted the depositions of key defense witnesses. The court ordered the defendant and the defense counsel – and *not* their insurers – to split the plaintiff's costs and attorneys' fees in bringing the motion for sanctions. The defendant and defense counsel also had to pay an additional $10,000 for each of the new depositions of the already deposed defendants, resulting in total sanctions of $45,162.00.

Planning Ahead – Issues and Systems

Faced with these duties and responsibilities, what should you do?

I. Designate an IT/Litigation Contact Person

You need to designate a member of your IT staff to work with counsel throughout the litigation. Such a designation is required in some courts, and certainly helpful in all. Before you make the decision, consider the following:

1. The contact needs to have an absolutely comprehensive understanding of your data retention systems - that includes servers, back-up systems, PCs, PDAs, notebooks, voice mail systems, e-mail systems and any other equipment that holds any data – on or off site.

2. The contact must have the authority to place a litigation hold on all such data, no matter where it is or whose it is;

3. The contact must have the authority to search all data, no matter where it is stored or who created it;

4. The contact must have (or acquire) an understanding of the litigation process; they are likely to be deposed, and need to have the ability to explain the systems and the e-doc searches to laymen;

5. The contact needs to be available; someone whose existing responsibilities take up most of their time will not be able to handle the extra burden, and this work is extremely time sensitive. Short cuts and rushed work lead to errors and sanctions.

6. The contact must be available to attend discovery conferences, meet with counsel, perform or supervise comprehensive searches, document the process of those searches, handle telephone inquiries, attend court hearings, review e-docs produced by other parties, and otherwise assist in all aspects of electronic discovery. The bigger the data retention, the heavier the work load;

7. The contact should likely be a long-term employee; this is a specialized set of knowledge and skills, and a substantial asset once developed. You do not want to incur the cost of training a new contact every year or two, nor do you want to run the risk of errors inherent in frequent turnover.

II. Develop an Electronic Discovery Response Plan

Rather than reinventing the wheel every time e-docs are implicated in a case, develop a response plan that fits your business and your systems. Include the following basic steps, and document the plan so that the contact and your counsel can refer to it as needed:

1. Map the systems: The contact and counsel need a current and complete plan of your hardware, so that all retention locations can be identified and searched.

2. Revise your document retention policies: The old, simple "dispose of all data after 18 months" policies are no longer sufficient in the era of e-docs and e-discovery. You will not be sanctioned for following a reasonable data deletion system, assuming that your policy explains the costs and burdens of extended storage or other business reasons for purging old data. You are less likely to be penalized for such a policy if it is written, has been in place for an extended period, and is uniformly followed.

   NOTE: An important discovery distinction exists between "accessible" and "inaccessible" e-docs. "Accessible" e-docs are usually those directly retrievable on your network. They are treated like paper documents for most discovery purposes, and your retention policy must address the timely deletion of unnecessary data so stored.

   Remember – once there is a likelihood of litigation, that material is "frozen", and you cannot delete it, even if your policy called for it to be removed years ago. Your retention policy should address a regular search for outdated data stored in all locations and permanent removal or overwriting of that data, with a clearly stated business justification for such deletion.

   "Inaccessible" e-docs are those stored in back-up systems or similar media, often in formats that require recovery or restoration operations, and not directly readable by system users.

   Courts will analyze closely the costs and burdens of searching and producing such data, and may limit the scope of such searches, require sampling of data, or switch the economic burden of production to the requesting party. Again, your retention policy should spell out in detail what is stored, where, and for how long, and in clear terms, why recovery is difficult and expensive. There is a balance to be struck – you maintain back-up and archival systems to protect the integrity of your data, but the more e-docs you preserve, the more the other side will ask for in production. Document your policy carefully, and follow it.

3. Establish your e-discovery team: It takes time to get your counsel and IT personnel up to speed on these procedures, and you may not have the time needed if you wait until suit is filed. There will certainly be an inquiry into your policies and systems pre-dating any loss or suit, so you need to have these in place before controversies arise. Do it now; put your counsel and your IT people together and give them the opportunity to put their house in order. Require updates and revisions at intervals that make sense in your business.

4. Think about attorney-client privilege: Internal electronic communications with counsel acting in the role of legal adviser are likely to be privileged, but that protection is sometimes blurred by cc's sent to outside parties, messages that are a mixture of legal discussions and business analysis, or even just the lack of a "privilege" header. Preservation of the attorney-client privilege in e-docs is essential, and your response plan should clearly set standards to be met in an effort to avoid waiver. Searching hundreds of thousands of pages of e-docs for privileged communications that are not clearly designated or segregated is a nearly impossible task, and if you cannot separate them, you may end up giving your opponent a window into your strategy and legal planning.

5. Establish a "litigation hold" procedure: When you become aware of the possibility of litigation, you need a mechanism for identifying everyone in the company who has control over relevant e-docs, and telling them what to do. A general "do not destroy" is probably inadequate. Work with your counsel to design an internal notification method, taking into consideration who must be notified, the scope of e-docs to be preserved, the location of that data, and documentation of the hold to justify your procedure and demonstrate good faith. This process is critical – if you cannot demonstrate that you took adequate steps to prevent destruction of data, you stand to lose cases that you should win.

6. Think offensively, too: Your e-discovery team is not just about responding to the other side's requests for documents. It can also be an offensive weapon, used for analyzing the other side's e-discovery responses, uncovering "hidden" data in electronic media produced by opposing parties, and formulating discovery requests. Think creatively, and use every ounce of expertise that is available.

III. Critique the Results

On an ongoing basis, critique the results of the operation of your team and your response plan. Are the IT contact and counsel communicating effectively? Is the systems map being updated as your equipment changes? Are you locating documents as needed? Is your "litigation hold" working, or are e-docs being purged after the hold is issued? Are you successfully defending Motions to Compel seeking additional documents?

The Rules and case decisions are dynamic, and will continue to evolve; stay current, review your program, and you can avoid the nasty consequences of errors in

handling e-discovery. Stay in touch with your counsel for updates as rules change, and try to stay ahead of the curve.

Robert B. Smith
Laurie R. Bishop
Nelson, Kinder, Mosseau & Saturley, PC
45 Milk Street
Boston, MA 02109
617.778.7500
rsmith@nkms.com
www.nkms.com