E-DISCOVERY IN FEDERAL COURT:

SIX CHANGES YOU SHOULD MAKE TO YOUR PRACTICE AT THE OUTSET OF THE CASE

By Kary Pratt

1. AS SOON AS YOU ARE ENGAGED, YOU MUST GET YOUR CLIENT TO EXPLAIN WHAT ELECTRONIC INFORMATION IT CREATES AND WHAT ELECTRONIC INFORMATION IT STORES.

- The duty to preserve arises when a reasonable person would anticipate litigation.

- This may require a discussion with your client's IT staff. If the systems are very complex, or you are completely unfamiliar with understanding the technology, you should consider hiring an e-discovery/forensics firm to assist you.

    - Check out Form 2.3 in *The Electronic Evidence and Discovery Handbook*, Sharon D. Nelson, Bruce A. Olson, John W. Simek, available from the American Bar Association for $129 – 1-800-285-2221 or online at www.ababooks.org. This form provides guidelines for hiring an electronic discovery or computer forensics expert.

- Information you will need to obtain from your client:

    - detailed descriptions of computer systems used by the company, including hardware systems, primary operating systems, and major software systems, including any customized software.

    - detailed description of how those computers are networked or connected to others outside of the company

        - If your client operates from multiple locations, you will need to consider all potential data locations, including geographic locations as well as storage locations such as file shares, archival tapes, and hosted email.

    - detailed description of computer systems used by relevant employees outside of the corporate system (home computers, PDAs)

    - detailed description of backup processes and schedules, document retention and destruction schedules, organized by type of data, with locations for each of the systems.

Kathryn Mary Pratt prattkary@hotmail.com

- the company's document retention and destruction policy, email and internet usage policies and litigation hold policies if any.

- whether and how the company monitors employees' computer usage.

- whether any third parties have access to the company's data, identify them and get contact information.

- Distinguish between accessible data and inaccessible data- The new rules distinguish between data that is readily accessible and data that is not. FRCP 26(b)(2) clarifies that a party need not produce information that is not reasonably accessible because of undue burden or cost.

  - Examples of data which is not reasonably accessible include: deleted information, information on backup systems for disaster recovery purposes, and legacy data remaining from systems no longer in use.

2. YOU MUST ADVISE YOUR CLIENT OF ITS OBLIGATIONS TO PRESERVE ELECTRONIC EVIDENCE AS SOON AS YOU ARE ENGAGED.

- Once you have an idea of where the data is and who might have it, you need to prepare letter to your client advising them of their obligation to preserve evidence, including electronic evidence.

  - Should you fail to advise your client of its obligation in sufficient detail, and your client is ultimately sanctioned, you can wind up with a claim against you.

- You should assist your client in crafting a litigation hold to prevent the destruction of responsive evidence.

  - You can use the Sedona Guidelines at http:www.thesedona conference.org/publications_html, which provides recommended best practices for electronic document retention and production, to help develop electronic information policies.

    - Make sure that the litigation hold is issued not only to the employees whose conduct was at issue, but any employee who may have been likely to have had any contact with the issues in the lawsuit.

    - Make sure the litigation hold is issued to the IT department if any, and ensure that they understand the obligations to preserve electronic evidence.

- Consider whether it is necessary to send a letter regarding preservation duties to any third party vendors or contractors of your client who might have evidence relating to the claim.

- Sanctions can be awarded when counsel fails to cause the defendant to adopt a litigation hold to prevent destruction of responsive information. See, eg *Metropolitan Opera Assoc. v. Local 100*, 212 FRD 178 (SDNY 2003)

- IMPORTANT NOTE: You must make it clear to your client that the duty to preserve evidence trumps the client's standard information retention/destruction policies.

3. YOU MUST DIRECT YOUR CLIENT TO IDENTIFY AND SEARCH ALL SOURCES OF DISCOVERABLE EVIDENCE AND YOU NEED TO OVERSEE THE PROCESS.

- If you don't ensure that your client searches and preserves all of its electronic archives and then produces complete, unaltered copies of the discoverable information, your client may be subject to a wide variety of harsh sanctions, including dismissal, adverse inference instructions, striking of claims and defenses, monetary penalties, and paying the opposing party's attorney fees. *Zubalake v. UBS Warburg,* 2004 WL 1620866 (SDNY 2004).

- Consider whether your client has the necessary expertise to ensure that the evidence can be gathered without destroying metadata that might be required to be produced. If not, hire an expert to preserve all relevant electronically stored data.

    - Sometimes the act of printing the electronic data for production can destroy some of the metadata. In *Gates Rubber Company v. Bando Chemical Industries,* 167 FRD 90 (D Colo. 1996), the court held a defendant's employee destroyed electronic information by overwriting 7-8% of it during an unnecessary download to copy it for production in discovery and awarded sanctions.

- Be sure your client considers alternative names when it conducts searches, such as name changes, different usernames, nicknames, so that the searches are sufficiently thorough.

- Consider chain of custody issues - Be sure the client documents where the media has been, whose possession it has been in and the reason why that person had possession during the collection process.

4. YOU SHOULD CONSIDER WHETHER OR NOT TO ADVISE THE OPPOSING PARTY OF ITS OBLIGATION TO PRESERVE EVIDENCE.

- If you have any reason to think that the opposing party may have electronic evidence, you should send a letter to that party if unrepresented, or its counsel, reminding him/her of the duty to preserve such evidence and the consequences of spoliation.

    - Be sure to advise the opposing party that the obligation to preserve evidence related to the suit trumps their usual document retention policies. Later, if documents have been destroyed under those policies, you may be able to seek an adverse inference instruction based on your preservation letter.

    - The preservation letter is today's clarion call that underpins tomorrow's "I told you so." Your goal is to slam the door on the "it was an oversight excuse." You will likely need to use it as the basis for establishing bad faith in failing to preserve relevant data and a subsequent claim for spoliation. The more you give notice and convey what must be retained, including methodologies for preservation and consequences of failure, the greater the likelihood your opponent will be punished for failing to preserve evidence.

    - The preservation letter should:

        - call for a halt to routine business practices that destroy potential evidence;

        - as appropriate, it should call for an end to server back up tape rotation, electronic data shredding, scheduled destruction of back up media, re-imaging of drives, drive hardware exchanges, sale, gift or destruction of computer systems, and when computer forensics may come into play, disk defragmentation and maintenance routines;

        - advise your opponent to communicate the retention obligations to all those with access to the systems

        - point out that paper preservation of ESI is not adequate and advise them that, if the evidence exists in both paper and electronic form, both should be kept.

        - be specific in identifying the scope of the relevant evidence, that, at a minimum should be preserved

- Try not to compel the opposing party to preserve more data than your client could reasonably sustain. Doing so could hurt your credibility with the court right out of the box.

- Who to send the letter to- think about the person who is most likely to unwittingly destroy evidence and make sure that person receives a letter.

- CONSIDER STRATEGY: Sending preservation letter to a person likely to intentionally destroy evidence is different than sending it to those likely to inadvertently destroy evidence. Here, you may need to balance the desire to give notice against the potential for triggering irretrievable destruction.

5. YOU MUST PAY CAREFUL ATTENTION TO ANY PRESERVATION LETTERS YOUR CLIENT RECEIVES FROM THE OPPOSING PARTY

- Your opponent's goal is to slam the door on any "it was an oversight excuse" on the part of your client. Be sure to advise your client as to the consequences of not preserving the types of evidence listed and go over your client's plan to communicate the need to preserve to its employees.

6. YOU MUST BE PREPARED TO DISCUSS ELECTRONIC DISCOVERY AT THE MEET AND CONFER UNDER FRCP 26(f)

- Under our local rules, this conference is required to takes place 30 days after the last defendant is served.

- Under revised FRCP 26(f) this conference is to include consideration of issues related to disclosure or discovery of electronically stored information, including the form of production, the identification of any distinctive or recurring problems occurring from the fact that the information is stored electronically, issues related to preservation of electronically dynamic information, and inadvertent production of privileged information in discovery.

    - Parties are encouraged under the commentary to develop agreed upon protocols to facilitate discovery that are faster and less expensive and can be included in the court case management order.

- You'll need to know the systems and applications your client has or have someone sit in on the conference who does.

- Your client may want you to arrange for some relief from some of the measures it has employed to preserve evidence. This is your opportunity to request an agreement to allow for that relief.

- Be prepared if your opponent asks that it be permitted to rotate server back up tapes, replace systems or delete older emails. Don't concede that your opponent can destroy any information in any form unless the party demonstrates that the information lost is not likely to be relevant to any issue in the case or lead to the discovery of admissible evidence.

- If you anticipate that the volume of electronic discovery in your case will be very large, at this point you should consider and discuss quick peek and claw back agreements so that no privileges are waived.

    - However, as noted in the article entitled "*Dangers In The Use Of Quick Peek And Claw Back Agreements Under The New E-Discovery Rules*" with these materials, there are some dangers in using these agreements you should be aware of before entering into one.