NEXSEN | PRUET

FIVE COMMON MISTAKES LAWYERS MAKE IN ELECTRONIC DISCOVERY – MAY 2011 UPDATE

by
Gary L. Beaver

No. 1: Failing to understand what electronically stored information (ESI) your client or the opposing party has.

- You must force your client to explain what ESI it creates and what ESI it stores. All forms of ESI have long been discoverable (Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y.1988); see, e.g., Smith v. Cafe Asia, 2007 WL 2847579 (D.D.C. Oct. 2, 2007) (plaintiff ordered to preserve and allow inspection of pornographic images stored on his cell phone) and may be so even if the data has been deleted but is recoverable at substantial additional cost. Your client contact is unlikely to know everything about the client's IT system so you must find out to whom else you must speak. Do not expect your client to always know if its production is complete or if the disks it is producing contain ESI beyond that which was requested. It is your job to find out from your client's IT personnel. For example, electronic documents have "metadata" – information about when a document was created, edited, sent, and received or how data on a spreadsheet was calculated – embedded in them that does not appear when the document is printed or seen on the screen. You may unknowingly produce metadata that waives a privilege or gives away a trade secret or fail to produce metadata if it was required to be produced leading to sanctions for discovery failures. For example, in Williams v. Sprint/United Management Company, 230 F.R.D. 640 (D.Kan.2005) the defendant was ordered to show cause why it ought not be sanctioned for scrubbing metadata from spreadsheets when previously ordered to produce the electronic spreadsheets in the manner in which they were maintained.

- In document requests, you will have to specifically request that ESI be produced in the form you want; there may be fights over such requests. See, e.g., Nova Measuring Instruments Ltd. V. Nanometrics, Inc., 417 F.Supp.2d 1121 (N.D.Cal. 2006) (production in TIFF format left plaintiff with 36,000 apparently unsearchable documents; court ordered production in native file format with original metadata and Bates numbers). Preliminary depositions of the opposing party's IT personnel may be necessary prior to merits discovery as noted in In re Carbon Dioxide Industry Antitrust Litigation, 155 F.R.D. 209 (M.D.Fla.1993).

No. 2: **Failing to understand what hardware and software your client or the opposing party has and what capabilities they have.**

- Again, your client contact is not likely to know all this. You must push and dig for this information from your client's IT personnel. Do not forget to find out about offline storage (such as backup tapes) and external electronic data sources like company laptops, Blackberries, cellphones, iphones, etc., and permitted use of personal computers and PDAs to link into the company IT system from outside the office.

- You should discover this from your opponent in your first round of written discovery and/or in initial depositions. Once you know what the potential ESI sources are on both sides, you may have to ask the court to establish a search protocol if you do not trust the opposing party or that party is obstructive or if the universe of discoverable electronic data is large. See, e.g., In re Priceline.com Inc., 233 F.R.D. 88 (D.Conn. 2005) (court set out detailed e-discovery "directives" for the parties to follow); Flagg v. City of Detroit, 252 F.R.D. 346 (E.D.Mich.2008) (court set protocol for review and production of text messages); ClearOne Communications, Inc. v. Chiang, 2008 WL 920336 (D.Utah Apr. 1, 2008) (court refined search protocol to add search terms and ordered conjunctive and disjunctive keyword searches).

No. 3: Failing to tell your client and the opposing party to preserve ESI immediately upon your being engaged and ensuring they continue to preserve it throughout the case. They should be preserving it as soon as there is "pending or foreseeable litigation" so that duty may have arisen before you were hired. See Silvestri v. General Motors Corp., 271 F.3d 583 (4th Cir.2001).

- You and your client must identify any potentially relevant ESI immediately and your client must preserve it. This usually entails using litigation hold communications to immediately notifying key players to preserve all potentially relevant evidence and identifying all locations of such evidence, and putting in place both communications and technology to preserve the evidence, such as suspending automatic destruction of ESI under company's document retention/destruction policies. In Metropolitan Opera Association v. Local 100, 212 F.R.D. 178 (S.D.N.Y. 2003), the court entered judgment against the defendant as sanctions for a variety of discovery failures including counsel's failure to cause the defendant to adopt a retention policy to prevent destruction of responsive information. In QZO, Inc. v. Moyer, 358 S.C. 246, 594 S.E.2d 541 (S.C.Ct.App. 2004) the court struck defendant's pleadings where it concluded defendant's destruction of ESI by reformatting computer was willful.
- If you expect that the opposing party has important ESI evidence, you should send a letter to opposing counsel (or to the opposing party if unrepresented) immediately at the outset of the case reminding him/her of the opposing party's preservation duties and the consequences of spoliation. May also need to send similar messages to non-parties.

- You must follow-up with your client and make sure that it is continuing to observe the legal hold. See, e.g., Samsung Elec. Co. Ltd. v. Rambus, 439 F.Supp.2d 524 (E.D.Va.2006), vacated on other grounds, 523 F.3d 1374 (Fed.Cir.2008) (counsel must instruct client about what to preserve and then follow-up to make sure the litigation hold is working).

No. 4: Failing to ensure that your client or the opposing party has gathered all requested, discoverable electronic information.

- If you do not ensure that your client searches all of its electronic archives and produces complete, unaltered copies of the discoverable ESI, your client may be subject to a wide variety of sanctions, including dismissal, adverse inferences, striking of claims and defenses, monetary penalties, and paying the opposing party's attorney fees. In Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004 (Zubulake V), the court stated that counsel "must take affirmative steps to monitor compliance so that all sources of discoverable

information are identified and searched." Court found willful destruction of relevant emails and ordered adverse inference and costs; jury returned verdict of $9.1M in compensatory and $20.2M in punitive damages. See Phoenix Four v. Strategic Resources Corporation, 2006 WL 1409413 (S.D.N.Y. May 23, 2006) (sanctioned defendant and its counsel; counsel's failure to identify sources of relevant ESI including a server and computers that were formerly used at defendants' old office was gross negligence; court relied in part on proposed Federal Rule change and Zubulake V re: counsel's duty to locate records)

- If you do not inquire deeply enough of the opposing party, you will likely either fail to get complete discovery or fail to put the opposing party in the adverse litigation position it would richly deserve for its discovery production failures.

No. 5: Failing to think creatively or seriously.

- Stay current about the latest technology used to create, transmit, and store ESI. Who knew 15 years ago about universal series bus (USB) drives, personal digital assistants (PDAs), digital cameras, iphones, memory cards, and text messaging? New methods of creating and storing ESI are constantly being developed or evolving. You need to know about them so that you can ask the right questions and find all of the relevant evidence.

- Your own clients will not have a grasp of all of the forms of ESI they are using. You will have to push hard to learn about your clients' IT hardware and software, the users of the clients' ESI devices, and even what ESI devices key players may be using outside the clients' IT systems. Failure to investigate your own client can lead to sanctions against you personally. The days of sending letters and discovery requests to clients and just accepting what they mail back without further investigation are over.