A Practical Guide To Conducting Electronic Discovery

(With Forms)

William "Mo" Cowan and Kwabena Abboa-Offei

New technology calls for new approaches.

William "Mo" Cowan is Partner in the Litigation Practice Group of Mintz Levin Cohn Ferris Glovsky & Popeo. Mr. Cowan's practice involves all manner of complex litigation matters including director and officer liability defense, securities fraud, and class action defense. Mr. Cowan also serves as Chair of Mintz Levin's Hiring Committee and is President of the Massachusetts Black Lawyers Association. **Kwabena Abboa-Offei** is an Associate in the Litigation Practice Group of Mintz Levin Cohn Ferris Glovsky & Popeo. Special thanks and acknowledgment is due the following colleagues who contributed a great deal of thought, planning and content for this article: Beth Boland, Esq., Craig Tiedemann, Esq., and Paul Abbott, Esq. This article is based on a paper the authors prepared for the Minority Corporate Counsel Association's Second Annual CLE Exposition.

SOONER OR LATER, most in-house lawyers and their outside counsel will face either a demand or need for electronic discovery. Our clients and our adversaries are communicating more and more by electronic means. "Each day, 9.8 billion e-mail messages are composed and sent, accounting for about half of the 13 terabytes of new electronic information created and stored each year. In fact, nearly 100 percent of all information is now created and stored electronically." Virginia Llewellyn, *The Key to Containing Cost: Explosion of Electronic Information*, 16 Corp. Couns. 6 (Feb. 2002). *See also, Thompson v. U.S. Dept of Housing and Urban Dev.*, 219 F.R.D. 93, 97 (D.Md. 2003) ("E-mails have replaced other forms of communication besides just paper-based communication. Many informal messages that were previously relayed by telephone or at the water cooler are now sent via e-mail"). According to one study, "93% of all information generated during 1999 was generated in digital form, on computers. Only 7% of information originated in other media, such as paper." *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437, 440 n. 2. (D.N.J. 2002). As a general rule, almost all of this information is subject to discovery as if it were in hardcopy form. A recent document preservation order defined documents in the following manner: " 'Documents, data, and tangible things'…electronic messages; voicemail; E-mail; telephone message records or logs; computer and network activity logs; hard drives; back-up data; removable computer storage media such as tapes, disks, and cards; printouts; document image files; Web pages; databases; spreadsheets; software.…" *Pueblo of Laguna v. United States,* 60 Fed. Cl. 133, 143 (2004). As a result, lawyers must engage in electronic discovery intelligently

to maximize the usefulness of their own electronic discovery requests and minimize the damage that the production of electronic discovery may cause.

HOW TO DO IT WELL • If parties choose to engage in electronic discovery, their attorneys must diligently search for it and produce it. Lawyers that fail to do so not only risk malpractice, but also expose their clients to the very real possibility that the court will impose sanctions that may devastate the merits of the client's case. What we offer below is a practical guide to engaging in electronic discovery.

1. Know Your Document Retention Policy

Corporate counsel must take a hands-on approach in creating a document retention policy. Many organizations ignore the discovery consequences that result from either the lack of a document retention policy, or the failure to enforce an existing document retention policy. In *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, 2002 WL 246439 at *2 (E.D. La. Feb. 19 2002), the Court noted that the e-mail issue over which the parties were fighting would have been moot had defendant simply destroyed its e-mail back-up tapes after 45 days in keeping with its own document retention policy. However, defendant maintained its e-mails for a 14-month period. Those back-up tapes included communications about the underlying litigation issue. After litigation begins, corporate counsel may be surprised to learn that for years the Information Services department has been saving thousands of e-mail and back-up storage data, the staff have been communicating with indelicate language about sensitive topics, and—worst yet—this information might be discoverable. For example, in *Linnen v. A.H. Robins Co.*, 1999 WL 462015 (Mass. Super. Ct. 1999), "the family of a woman who died after taking the diet pill combination of the prescription drugs fenfluramine and phentermine (known as fen-phen) sued the drugs' makers. The plaintiffs claimed the drugs, taken in combination, caused the woman to develop a deadly lung disorder. Computer forensic engineers hired by the plaintiffs were able to recover an e-mail from one A.H. Robins employee to another that read: 'Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?' Shortly after this revelation, the case settled." Kristin M. Nimsger, *Digging For E-Data*, 39 Trial 56 (Jan. 2003).

Some Policy Basics

An organization, therefore, should have a data storage policy that:

- Clearly defines how, and for what purpose, e-mail is to be used;
- States how long old e-mails and back-up files will be stored;
- Organizes data storage in a way that allows for easy retrieval; and
- Instructs employees to use standard and appropriate business language while e-mailing to make conducting word searches of the e-mails easier, and also to help avoid embarrassment.

In *United States v. Microsoft Corp.*, the government's antitrust case against Microsoft was largely supported by pages of e-mails, which the government introduced to show that Microsoft engaged in anti-competitive behavior as a matter of course. Bill Gates' top lieutenants spent days trying to explain e-mail communications about "choking off the air supply" of Microsoft's competition.

Having an intelligently crafted electronic discovery policy will give you an advantage over an opponent who has failed to take the time to implement and enforce a policy for its own organization.

2. Understand Your Client's Electronic Data

The process of talking with your client about documents—including electronic data—and reviewing that information should start as soon as litigation is imminent. It should not be left until after the complaint and answer are filed. It is important for in-house and outside counsel to understand what electronic data may become relevant to the matter. Understanding the electronic data will play an important role in shaping the overall legal strategy and the content of your complaint, answer, or initial motions. The client may not be aware of the legal import of certain electronic data and the discoverability of that data. Having a conversation with your client about electronic data will also help to prevent the destruction of relevant electronic data.

3. Be Aware Of The Duty
To Preserve Electronic Evidence

As soon as you become aware of the relevancy of evidence to a future dispute, regardless of whether litigation has actually commenced, the duty to preserve electronic data attaches. A party must preserve electronic "evidence that it has notice is reasonably likely to be the subject of a discovery request even before a request is actually received." *Wiginton v. Ellis*, 2003 WL 22439865, at *4 (N.D. Ill. Oct. 27, 2003); *Lewy v. Remington Arms Co.,* 836 F.2d 1104, 1111-12 (8th Cir. 1988) (obligation to interrupt regular recycling practices arises if party knows or should know that documents may be material to a future dispute). Another articulation of the "duty-to-preserve" rule states that: "while a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request." *Turner v. Hudson Transit*, 142 F.R.D 68, 72 (S.D.N.Y. 1991). "Moreover, in the world of electronic data, the preservation obligation is not limited simply to avoiding affirmative acts of destruction. Since computer systems generally have automatic deletion features that periodically purge electronic documents such as e-mail, it is necessary for a party facing litigation to take active steps to halt that process." *Conlove, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 175-76 (S.D.N.Y. 2004). Sanctions may be imposed for counsel's negligence in failing to advise clients to preserve potentially relevant electronic data. *Applied Telematics Inc. v. Sprint*, 1996 U.S. Dist. LEXIS 14053, at *6-14 (E.D. Pa. Sept. 17 1996). *See also*, Paul M. Robertson & Charles R. Kellner, *Massachusetts Expert Witnesses*, Vol. I, Ch. 11, Computer Forensics §11.5 (Massachusetts Continuing Legal Education, 2000).

Danger Of Sanctions

For example, in *In re Prudential Ins. Co. of America Sales Practice Litigation*, 169 F.R.D. 598 (D.N.J. 1997), the court ordered an insurer to preserve documents, yet the insurer did not distribute that order its employees. Instead, the insurer issued to its employees a clumsily and vaguely communicated instruction to preserve documents that failed to prevent the destruction of relevant documents. The court

first stated that the burden of instituting reasonable retention polices lied with upper management. The court then sanctioned the insurer, requiring it to, among other things:

- Mail to every employee a copy of the court's prior order regarding document retention, along with an explanation of the underlying legal action;
- Draft a written document retention policy manual for the court's approval; and
- Pay a fine of $1 million.

For a similar holding, see *Zubulake v. UBS Warburg*, LLC., 2004 WL 1620866 at *12 (S.D.N.Y. July 20, 2004). In this case the court said: "In sum, while [defendant's] personnel deleted e-mails, copies of many of these e-mails were lost or belatedly produced as a result of counsel's failures.… Counsel failed to communicate the litigation hold order to all key players. They also failed to ascertain each of the key players' document management habits. By the same token, UBS employees—for unknown reasons—ignored many of the instructions that counsel gave. This case represents a failure of communication, and that failure falls on counsel and client alike."

Finally, when your opponent has willfully destroyed or failed to preserve electronic data, counsel may seek the appointment of a computer forensics expert to assist in recovering electronic data. Also, counsel is entitled to request that the offending party bear the costs of the computer forensics expert. *Aero Products Intern., Inc. v. Intex Recreation Corp.*, 2004 WL 417193, at *4 (N.D. Ill. Jan. 30, 2004).

4. Get An Expert To Help With Electronic Discovery

A computer forensics expert may be a useful, if not essential, addition to your litigation team when considering, seeking, or producing electronic discovery. The technical proficiency of most legal professionals has not kept pace with the increased role that technology plays in the way that businesses transfer and store information. Building a relationship with a skilled computer forensics expert will enable outside counsel to deal with requests with fewer burdens, reduced cost, and fewer mistakes.

Practical Skills

When selecting an expert, experience and practical knowledge are of primary importance. The field is relatively new; therefore, some experts may not have advanced degrees. So take care not to dismiss a very experienced person with good references because he or she lacks an advanced degree. Select a person who has an understanding of the cost involved in producing electronic discovery. He or she may be able to help you address the all-too-common battles over cost. Robertson & Kellner, supra, at §§11.2-11.3. Select a person who has both responded to requests and made requests for electronic discovery. An expert who has made electronic discovery requests in the past is more likely to know what type of requests are common and will be considered reasonable by a court. Therefore, they will be able to help you convince a court that a request is either reasonable or unreasonable. Be sure to verify the technical skill of your expert. You must examine your expert's references and experience, do not take his or her skill for granted—this lack of diligence may lead to disaster for your client and your own career. In *Trigon Ins. Co. v. United States*, 204 F.R.D. 277 (E.D. Va. 2001), a taxpayer brought action against the IRS, and in the course of expert discovery many documents requested by the taxpayer, such as draft expert reports, were destroyed. The taxpayer's own expert was able to locate evidence of the destroyed

documents, but was not able to restore all of the documents. The court allowed an adverse inference instruction both as to the substance and credibility of the government's experts' testimony. *See also*, Robertson & Kellner, supra, at §§11.2-11.3.

To avoid sanctions, your expert must understand the law. The law governing production, spoliation, retention, and admission of electronic data is becoming more specialized as the practice of conducting electronic discovery becomes more common. *Id.*

You want an expert who can speak to you and your client in layperson's terms, so that everyone involved in the process can make a reasoned decision regarding what steps are necessary regarding the electronic discovery request process. A good electronic discovery request is a result of a healthy marriage between the technical and practical skill of the forensics expert and the strategic know-how of the lawyers. The lawyers must be able to explain to the forensics expert exactly what information they wish to obtain through the electronic discovery process, and the forensics expert must communicate to the lawyers whether electronic discovery is necessary in light of the lawyers' goals and where exactly the litigation team should search for electronic discovery in light of the lawyers' goals.

Also, to avoid the appearance of impropriety, should an accident happen resulting in the destruction of evidence, you will want your expert to appear to be impartial. In other words, do not use your own corporation's Information Services Department as your primary forensics expert. This may help you avoid sanctions or an adverse inference charge for failing to produce evidence.

The Expert Can Help You Determine Whether You Should Engage In Electronic Discovery

Conducting electronic discovery can be extremely expensive. Before you seek to discover electronic data from your opponent, you need to determine if there is an added benefit from electronic data in your particular case. This benefit should be weighed against the (considerable) costs of such discovery, along with the fact that your opposition likely will retaliate with a similar request for your client's electronic data. Talk to IT sources and perhaps your forensics expert to determine the anticipated breadth and cost of the endeavor. Unless you have a thoughtful focused plan, the cost can accumulate beyond what the returns justify.

5. Conduct A Pretrial Discovery Conference

Work with your forensics expert and opposition, if possible, to propose reasonable record preservation and production methods. The more you do up front, the faster and cheaper production may be. This will also allow you to gauge how cooperative opposing counsel will be regarding electronic discovery and will help you determine whether a preservation order, along with other motion practice, is necessary to facilitate the discovery process.

Before you can draft a substantive request for electronic information, it is best practice to ask preliminary questions about the information that will help you frame your inquiries. For example, try to determine:

- What kind of computer system, network, and software are used by the opponent;
- How and where information is stored and backed up; and
- What the company's retention policy requires.