The Top 10 Things to Know About Electronic Discovery

By Steven J. O'Neill, Attorney at Law

10 Electronic Discovery will be part of your next lawsuit or arbitration. Electronic Discovery can be defined as the process in civil litigation and arbitration which permits the discovery of electronic information that has been created, reviewed, edited, transmitted or stored by computers or other digital devices. Electronic evidence is no less discoverable than paper evidence and in the opinion of U.S. District Court Judge for the Southern District of New York, Shira Scheindlin, "virtually all cases" now involve the discovery of electronic evidence. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (2003).

9 The volume of electronic information continues to grow. Whether through the increasing use of email, digital drawings, the internet, project management software digital photography or PDA's, the overall amount of information generated and stored doubled in three years. According to a study published by UC Berkeley's School of Information Management and Systems (SIMS), over 5 exabytes of new information was created and stored in 2002. Placed in perspective, 5 exabytes (5 X 10^{18} bytes) is the data equivalent of multiplying the entire print holdings of the Library of Congress 500,000 times! In comparison, the estimate for 1999 was 2-3 exabytes. Over this period the growth in paper, magnetic and optical (CD/DVD) data has been 36%, 80% and 28% respectively. See, http:www.sims.berkeley.edu/research/projects/how-much-info. This continuing explosion of data has affected all types of organizations.

8 Why not save Everything? Once a legal duty to preserve your electronic evidence arises you must avoid a claim of spoliation (destruction) of evidence. One strategy is to save everything. While the cost of storage of electronic data is negligible compared to paper documents, there is a downside to such a pack-rat strategy. One danger is that if you are ever required to produce electronic evidence in a dispute you may be responsible for the costs of recovering the data. In general, the party required to produce the electronic evidence is the party responsible for the costs. Thus, the more you have the more expensive it could be, not only in terms of computer technician time but also in terms of the time for your lawyers to review the electronic documents. In addition, there might be a "smoking gun" email or other damaging evidence that could have been legitimately purged (according to a Document Retention Policy) before the dispute arose and the duty to preserve evidence was triggered.

7 What Electronic Evidence is Discoverable? In general, all relevant and non-privileged electronic evidence is discoverable even if it has never been printed out or transmitted. It is discoverable even if you thought that you deleted it. It is discoverable even if you didn't know it was there. A competent computer forensics technician can access and recover deleted files, early drafts of documents, email from backup tapes and so called metadata containing information about who viewed a file and when.

6 Why not destroy Everything? Subject to the individual requirements of record keeping laws (e.g., OSHA, ERISA, IRC) mandating that certain documents be maintained for specific periods of time, another strategy for dealing with the ever-growing volume of electronic documents is to regularly purge unneeded documents. A written and regularly followed "document retention policy" is really a policy for the *destruction* of documents, including electronic documents. For instance, a document retention policy can require (on a regular basis such as at the end of each project) that hard copies of project email be printed out and archived in paper form. A document retention policy can specify the routine deletion of email. In this way, prior to litigation or anticipated litigation, all electronic copies and other data not needed for the archives can be completely purged from the systems and not even available by forensic recovery.

(continued)

About the Author

Steven J. O'Neill is an experienced litigator with extensive knowledge of computer data systems architecture, electronic records issues and eDiscovery law. He has presented numerous seminars on these topics throughout the U.S. His practice areas include business law, litigation and technology law focusing on eDiscovery, Document Retention Compliance and Information Security Compliance. He is admitted to practice in state and federal court in MA and CT and available to serve clients nationally.

Steven J. O'Neill
Attorney at Law
245 First St., 18th Floor
Cambridge, MA 02142
617.575.9044 Main
888.766.3455 Toll-free
413.267.0554 Fax
soneill@atttorneyoneill.com
attorneyoneill@gmail.com

Massachusetts
Connecticut

attorneyoneill.com

5 **Triggering a Duty to Preserve.** Once you are a party (or anticipate being a party) to a suit or arbitration or once you have received a lawyer's letter demanding that you preserve evidence, it is too late to adopt a document retention policy for documents relevant to the dispute. The law is clear that once the legal duty to preserve is triggered, you must retain and preserve all relevant documents then in existence. You must also preserve any relevant documents created after the duty attaches.

4 **What are the Preservation Obligations?** Even if you have a carefully drafted and regularly followed document retention policy, once the duty to preserve evidence is triggered the destruction policy must be immediately suspended in order to avoid a claim of spoliation of evidence and a finding of adverse inferences (i.e., if you destroyed evidence or allowed it to be destroyed, then it must have been unfavorable to your position). This status has been called "litigation hold." Recognizing that there are many ways to manage electronic data, there is no set way to meet your preservation obligations. In general the preservation obligations should address at least the following topics: "imaging" of the relevant computer systems to preserve a complete evidentiary copy at the time the duty attaches; suspension of the overwriting of backup tapes; and suspension of any destruction of evidence including the inadvertent overwriting of deleted files by continued use of a computer that has not been "imaged." Although there is some expense involved in purchasing new backup tapes and replacing hard drives with "ghosted" copies, business interruption is minimized and the legal requirement of preservation is met at a controllable cost.

3 **Using the Preservation Obligations as a Sword.** Especially if your anticipated adversary has no document retention policy, your litigation strategy should consider the need to trigger the preservation duty before the shredding and erasing begins. This is accomplished by having your attorney send your adversary a letter requesting that all relevant evidence be preserved in anticipation of litigation/arbitration. A preservation letter is designed to be sufficient notice to trigger the legal duty of preservation. A preservation letter can be as specific as the circumstances dictate. If you have a particular concern about certain records disappearing then those should be identified. The preservation letter is also an opportunity to notify your adversary of the broad definition of electronic evidence that must be preserved, including for example: home AOL email accounts used by employees; PDA data as of the time of the request; Internet Service Provider data; personal notes and even voice mail.

2 **Developing and Using a Document Retention Policy as a Shield.** Understanding the implications of Electronic Discovery can reduce risks and help minimize costs in the event a dispute arises. Prior to a dispute arising, as part of a company's development of a document retention policy, care should be taken to train office and field personnel to generate accurate and effective documentation. Business documentation should address issues clearly and succinctly by recording facts (not opinions) concerning what happened, who was notified, who was responsible and what was impacted. Employee email habits should be of particular concern. Most people send email without editing or considering what some stranger might later read into an incomplete thought written in a stream-of-consciousness style. Consideration should be given to developing email templates or forms for recording regularly occurring events and data. The "Subject" line in email is often provided as part of a preliminary index in discovery; factual and innocuous subject lines may not invite special scrutiny. If business documentation is developed factually and accurately and if unneeded extraneous information is regularly purged under a document retention/destruction policy, the available evidence in any potential dispute can be analyzed and produced cost-effectively.

1 **The Golden Rule.** Courts and lawyers are only beginning to wrestle with the strategic, legal, procedural and financial implications of electronic discovery. Technological developments such as "cloud computing" place information outside of the physical control of the owner. The ease of creating and storing mountains of electronic evidence guarantees that in litigation somebody will want to access that data – and want the other side to pay for it. If not carefully planned and controlled, the costs of forensically accessing electronic data could match or exceed the amount of attorney's fees necessary to prepare and present a case. These new developments alter the economics of dispute resolution. Before we "let slip the dogs of war" and aggressively push for electronic discovery, we must recognize that our adversaries may very well mirror our requests for electronic discovery as a litigation tactic. Where a client has followed a document retention policy there should be little fear of the cost and disruption of electronic discovery; the costs have already been managed and the existence of potentially damaging documents is easy to assess. In many cases it may be advisable to negotiate a set of Electronic Discovery Protocols between counsel. The Protocols can address myriad legal and technical topics such as: how privilege review is to be handled; how relevancy determinations will be reviewed; the form in which the data is to be produced; how to avoid business interruption while computer systems are copied; and the definition and protection of confidential information both during and after the dispute. As part of the development of the Protocols, the divisive issue of cost-sharing for forensic recovery can be reserved for the judge or arbitrator. Notwithstanding the uncertainty and potential pitfalls surrounding electronic evidence, the fact that "documents" are increasingly created and stored in digital form necessitates that electronic discovery is now indelibly part of civil dispute resolution.