

Attorneys should know how to pilot electronic discovery

Attorneys are discovering that dealing with electronic evidence in litigation is becoming the norm and not the exception. Recent cases such as Zubulake v. UBS Warburg, Coleman v. Morgan Stanley, and Mosaid Technologies v. Samsung, highlight the need for a comprehensive approach to electronic discovery.



ELECTRONIC DATA DISCOVERY

PETER COONS

The three aforementioned cases all involved adverse inference findings stemming from the mismanagement of electronic data and illustrate that electronic evidence and the role it plays in litigation can no longer be ignored.

The discovery and production of electronic evidence is governed by the same rules addressing paper discovery set

forth in the Federal Rules of Civil Procedure (FRCP). However, in reference to electronic data, the rules don't go much further than a mere mention of "electronic data compilations" in Rule 34.

The good news is that change is coming and proposed changes to the FRCP deal specifically with electronic evidence. The new rules will become effective on December 1, 2006 absent intervention by Congress.

For guidance today, there are widely accepted and used bodies of work. The Sedona Conference (www.sedonaconference.com) papers on electronic discovery and more recent endeavors like the Electronic Discovery Reference Model (www.edrm.net) specifically address the handling and production of electronic data. Additionally, the number of opinions and the case law addressing electronic discovery is shifting from a trickle to a steady flow.

Below are some tips for managing your next experience with electronic evidence.

• Prepare before litigation begins.

Preparing an organization to manage electronic data for litigation should begin

before the threat of it is on the horizon. Every organization should have clear and reasonable written policies addressing the management of its electronic information.

Among other details, policies should focus on the retention and destruction of data along with the suspension of such policies to fulfill preservation requirements in conjunction with real or threatened litigation or situations mandating regulatory holds.

Cooperation and understanding between the information technology department, in-house, and outside counsel is critical for establishing and implementing such protocols.

• E-mailing the hold is not enough.

Litigation holds sent via e-mail are not sufficient in meeting preservation obligations. Follow-up interviews should be conducted with key players to ensure adherence to the notice. All interviews should be well documented and maintained throughout the litigation. It is vital that counsel take an active role in monitoring compliance of the litigation hold.

In Zubulake v. UBS Warburg LLC (02 Civ. 1243, S.D. N.Y. July 20, 2004), the court opined, "Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents." The court went on to say, "It is not sufficient to notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information."

• Get to know IT.

Counsel must understand how his or her client stores and manages its electronic data. In Zubulake v. UBS Warburg the court stated, "Counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture."

This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy."

This should not be interpreted that every attorney needs to become a technical guru, however, a basic understanding of the orga-

nization's IT infrastructure is important for dealing with electronic evidence.

• Get your 30(b)(6).

A Rule 30(b)(6) witness is one with intimate knowledge of how an organization stores and manages its data and records.

Consider making your first deposition the opposing party's system administrator or its 30(b)(6) witness. You will gain invaluable insight as to how it manages and maintains its electronic information.

Information gleaned from this deposition will also assist with crafting a targeted discovery request, one that the court will look upon favorably.

• Meet and confer early and often.

FRCP Rule 26(f) requires parties to meet and confer regarding discovery issues. These meetings should be used to discuss what electronic data needs to be preserved and how that data will be produced.

Use technology to your advantage.

It may not be possible to interview each employee or manually search entire networks for relevant electronic data. Courts have deemed it acceptable to use an automated search method such as a system-wide keyword search to identify and preserve potentially relevant data.

Get creative and use technology to solve your electronic discovery dilemmas.

• Collect with the future in mind.

In Treppel v. Biovail Corp. (2006 WL 278170, S.D.N.Y. Feb. 6, 2006), the court suggests that any data preserved should be done so in a manner that does not hinder access at a later date.

The court stated "The Second Circuit has held that conduct that hinders access to relevant information is sanctionable, even if it does not result in the loss or destruction of evidence. (See Residential Funding Corp. v. DeGeorge Financial Corp. (306 F.3d 99, 110, 2d Cir., 2002).) Accordingly, permitting the downgrading of data to a less accessible form — which systematically hinders future discovery by making the recovery of the information more costly and burdensome — is a violation of the preservation obligation."

• Preserve metadata.

Metadata is usually poorly defined as

data about data. The next best definition I located was "metadata is evidence, typically stored electronically, that describes the characteristics, origins, usage and validity of other electronic evidence." ("Make Friends with Metadata" by Craig Ball, Law Technology News, Jan. 26, 2006.)

Metadata is evidence and as more attorneys realize its potential value it will grow in importance. Attorneys should expect to receive requests or court orders to preserve and produce metadata. In Williams v. Sprint/United Management Co. (230 FRD 640, D. Kan., 2005), the court ruled that "when a party is ordered to produce electronic documents as they are maintained in the ordinary course of business, the producing party should produce the electronic documents with their metadata intact, unless that party timely objects to production of metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order."

• Don't peek.

Many attorneys review custodian's documents and e-mail prior to its proper preservation or collection. Don't be lured into this trap. While this activity may be seemingly harmless, you may be destroying or altering metadata that is relevant to the case. Take the steps to properly preserve any material prior to its review.

• Don't overlook the obvious.

Discoverable electronic information is not only stored on hard drives, networks, and backup tapes. Data may be stored on a wide array of USB devices, zip disks, custodian's home computers, voicemails, and cell phones. Relevant data may also be housed by third parties such as Internet Service Providers.

Having to deal with electronic discovery is unavoidable. If the thought of it makes you cringe, start delving into relevant case law or tap the numerous experts in the field to help you along the way. The more you know, the less intimidating it becomes. Plus, it's always fun to throw terms like "metadata" around at cocktail parties.

Peter Coons is Director of digital forensics and collections at Doculegal in Rochester.