New Jersey Law Journal

VOL. CXCII - NO.11 - INDEX 890 JUNE 16, 2008 ESTABLISHED 1878

Complex Litigation & E-Discovery

All Things Are Presumed Against a Wrongdoer: Avoiding Spoliation Pitfalls

How to discover, preserve and produce e-discovery

By Angela Scafuri

Have you ever been lucky enough to experience the feeling that comes over you when you learn that your client did not retain e-mails that are pertinent to litigation, whether it be that the e-mails were simply deleted or that your client's computer crashed three years ago and sent potentially relevant e-mails straight into Dante's eighth circle of hell? Quite an unsettling feeling. Despite counsel's best efforts, preservation of electronic information seem to be a constant sore spot in complex litigation.

In a post-*Zubulake* and *Morgan Stanley* world, where the amendments to the Federal Rules of Civil Procedure ("FRCP") went into effect well over a year ago, the struggle with how to best manage electronic data discovery ("e-discovery") continues. *See Zubulake v. UBS Warburg*, 229 F.R.D 422 (S.D.N.Y. 2004); *see Coleman Holdings v. Morgan Stanley*, 2005 WL 679071 (Fla.Cir. Ct. March 1, 2005).

E-discovery, in simple terms, means the information requested by a litigant which is stored in an electronic format and which the litigant intends to use as evidence in a case. Electronically stored information is more commonly referred to as "ESI." ESI can encompass all forms of information kept in an electronic environment, such as data stored on backup tapes, retained in legacy systems or other data reserved for deletion on hard drives. *See Manual for Complex Litigation* (Fourth) §11.446 (2003). A client may retain data in a variety of data formats: as e-mail and spreadsheets (active); cookies and favorites (Internet); and embedded information (metadata).

Spoliation of evidence is "the intentional destruction of evidence…" *See Black's Law Dictionary* (Sixth Ed. 1990). Notably, intentional misconduct in withholding e-discovery is not required for a court to make a spoliation determination and sanction a party; instead, poor document retention practices, or failure to maintain such practices, may provoke sanctions from the court. *See Mosaid Technologies, Inc. v. Samsung Electronics Co., Ltd.*, 2004 WL 2550306 (D.N.J.), *aff'd*, 348 F.Supp. 2d 332 (D.N.J. 2004) (holding negligence standard). Sanctions may include monetary fines, an entry of default judgment or even criminal punishment.

It has become routine for courts to enter preservation orders requiring the parties to be "reminded of their duty to preserve evidence that may be relevant to this] action." Recently, the District Court for the Northern District of California entered one of these "gentle reminders." *See In re Flash Memory Antitrust Litigation,* 2008 WL 1831668 (N.D. Cal. 2008). The Order makes it clear that e-mails, voice-mails and electronic calendars such as Outlook are all considered e-discovery.

The 2006 amendments to the FRCP acknowledge the glaring distinctions between traditional paper discovery and ESI. The amendments address production and preservation of ESI, and require that e-discovery be given attention at the earliest stage of litigation. For example, scheduling orders must address e-discovery, and any agreements between the parties for dealing with inadvertent disclosures. FRCP 16(f). Initial disclosures must identify and describe sources of e-discovery. FCRP 26(a). Under FRCP 26(f), parties must discuss issues relating to preservation and production of ESI, as well as the issue of inadvertent disclosures.

Safe Harbor Provisions. FRCP 37(f) provides a safe harbor for litigants who fail to preserve e-discovery due to normal business operations. The "safe harbor" provision is designed to excuse from sanctions the loss or destruction of "electronically stored information lost as a result of routine, good faith operation of an electronic information

Scafuri is a senior litigation associate at Bressler, Amery & Ross in Florham Park, where she maintains a complex litigation practice focusing on the defense of insurance companies in complex premium, coverage and bad-faith actions.

This article is reprinted with permission from the JUNE 16, 2008 issue of the New Jersey Law Journal. ©2008 ALM Properties, Inc. Further duplication without permission is prohibited. All rights reserved.

system." FRCP 37(f). The rule is designed to recognize that electronic systems, such as e-mail applications, must routinely overwrite or "autodelete" older information to allow for economical management of more recent data. The test is whether a "good faith operation" of the electronic system, a fact-sensitive inquiry, lost the ESI. The "safe harbor" provision, however, may fall short when a corporation is provided a litigation hold letter or other notice of ESI preservation and fails to disable the autodelete function of the e-mail system.

In addition, backup tapes may retain previously deleted information, and are fair game with respect to an e-discovery request. The question, however, becomes whether backup tapes are reasonably accessible, and, whether a corporate litigant should be subject to the expense of searching backup tapes.

Accessibility and Cost Shifting. FRCP 26(b) (2) (B) sets limits on the production of ESI and a fee shifting scheme for data determined to be "not reasonably accessible data." Thus, a party responding to e-discovery may argue that retrieval of backup tapes or other ESI is too costly to produce. The burden is placed on the litigant responding to the e-discovery request to show that the information is not reasonably accessible because of undue burden. Notably, even if such a showing is made, the court may still order the production. The question then becomes who is responsible for the cost associated with the retrieval of the ESI.

One of the series of *Zubulake* decisions provides insight into the distinction between costs associated with "accessible" and "inaccessible" data, creating an exception for a producing party to shift the cost of production to a requesting party in instances where the request for ESI primarily requests "inaccessible data." "Inaccessible data" is described as data that is stored in offline archival backup media, which typically requires sophisticated and complex restoration, and is typically utilized for disaster recovery. *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003).

Zubulake provides a seven-point test for determining when to shift the cost of production. The FRCP does not adopt the seven-point test in *Zubulake.* Instead, FRCP 26(b) (2) (B) simply provides that a producing party, on motion to the court, must show that the e-discovery requested is not reasonably accessible because of undue burden or cost.

From a practitioner's point of view, when faced with a party who maintains e-discovery is inaccessible, request to sample the inaccessible data, as opposed to a motion to compel. An inflexible position on an e-discovery request may be viewed by the court as unduly burdensome, or trigger potential cost-shifting. Thus, requesting a "sampling" of the data provides an efficient and cost-conscious solution to the problem. *See McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C.2001).

Spoliation and Sanctions. While FRCP 37(f) provides a "safe harbor" for routine, good-faith deletion of e-discovery, FRCP 37 also allows for sanctions where the producing party fails to provide e-discovery and is not protected under the "safe harbor" provision. Spoliation of evidence may result in entry of a judgment, and adverse inference or an award of attorneys' fees. Before sanctions can be levied, a court may make inquiry into whether the party alleging spoliation was *prejudiced* by the destruction of the ESI. *See Mosaid, supra.*

Further, the mere inference of wrongdoing can sway a jury to make a harmful finding against the party who failed to preserve e-discovery. Simply put, spoliation of e-discovery can potentially lead to millions of dollars in punitive damages.

Protecting the Institutional Client. Regardless of how sophisticated you believe your corporate client to be, explain ESI, e-discovery and spoliation. Many clients are simply unaware of the looming pitfalls in light of complex litigation and the 2006 amendments to the FRCP. Explain that a potential defendant has an obligation to preserve ESI before a lawsuit is even filed. When there is a suspicion of litigation, document retention is essential.

Institute a plan of action. Enlisting an individual or creating a department of competent employees within the company to take on the responsibility of collecting and preserving ESI is just good business. Information technology departments should also be given instructions on document retention. Make sure the team charged with the responsibility tracks the steps taken to preserve ESI. While it may be viewed as a costly undertaking, the initiative may save a potential corporate litigant millions of dollars. In addition, any plan of action should provide for maintaining a data map of all ESI, particularly for those corporate clients that conduct business internationally through many different offices, services and Internet providers.

Set up a time frame for maintaining ESI, and ensure that such a policy is adhered to uniformly and routinely. For example, holding computer backup tapes for too long can create unforeseen costs because of the time and expense required to search them when facing an e-discovery request in litigation. Therefore, preserve ESI to comply with laws and regulations for as long as necessary, but avoid infinite preservation.

Consider providing a "litigation hold form" at the inception of litigation. Emphasize that document destruction policies must be suspended once a duty to preserve ESI is recognized, whether it be in the form of an official hold letter or unofficially in the context of foreseeable litigation. A court will not fail to impose sanctions for spoliation that occurred when litigation was foreseeable.

Make sure the employees of your corporate client understand what a litigation hold letter is, as well as understand ESI retention policies. Even though your corporate client itself may comply in preserving ESI, to the extent your client's employees do not understand why preservation is critical, a court can still make a finding of spoliation against the corporation and impose sanctions. For example, the New Jersey District Court imposed a $1 million dollar fine where it concluded that the employees of a corporate litigant destroyed relevant documents despite the fact that the corporation itself took steps to notify its employees to preserve documents in accordance with the court's order. *See In re Prudential Insurance Company of America Sales Practice Litigation,* 169 F.R.D. 598 (D.N.J. 1997).

Reviewing these e-discovery issues now with your client will allow counsel to better reduce the risk of spoliation claims, as well as effectively manage e-discovery costs and protect your client's proprietary information in the setting of complex litigation. ■