LJN LAW JOURNAL NEWSLETTERS

The Corporate Counselor®

Volume 20, Number 3 • August 2005

ALM

Rule Changes for Electronic Discovery?

The Basics That You Need to Know

By Lawrence R. LaPorte and Michael A. Tomasulo

Technology has not only changed the way we live, but also the manner in which companies and their employees conduct business in the modern world. Today, companies both large and small utilize computer technology in every facet of their business. No longer just desktop tools, computers are now in our pockets or purses in the form of phones, palm pilots and blackberries. Simply put, computers are the dominant tool in today's business world.

Consider for a moment the daily activities at a typical corporation: E-mails are sent and received, files are generated, and information of all forms is stored on CD ROMs, hard drives, back-up tapes and the like — all with the click of a mouse. Today's world is paperless, and electronic document preparation and storage is fast, easy, and virtually unlimited. Accordingly, companies need to be aware that all electronically stored information is likely to be discovered in future litigation. As electronic records can be virtually permanent, the legal world has set its sights on discovering every written word and every record created. Because employees view e-mail less formally than typed letters, personal opinion — not always accurate and often provocative — invariably finds its way into e-mail communications. This reality is particularly true of communications between co-workers. Electronically stored information may have significant consequences for a company involved in litigation, and companies should therefore have reasonable policies for the creation, handling, storage and destruction of their electronic documents and communications.

Lawrence LaPorte and **Michael Tomasulo** are partners in the Los Angeles office of Jones Day, one of the world's largest law firms, where they both specialize in intellectual property matters. For more information, e-mail: llaporte@jonesday.com, or go to www.jonesday.com.

TARGET: E-MAIL

Lawyers are forever in search of an advantage, and a prime target has become electronic documents and communications. The proverbial "smoking gun" in litigation may be an informal e-mail message — sent, stored, and forgotten — and now sitting on an employee's hard drive or on a back up tape. Potentially damaging evidence is often created and deleted with little thought or effort. Such smoking gun evidence is colloquially referred to as "evidence mail" or "electronic truth serum," because juries perceive such communications, regardless of how cryptic or incomplete, as a person's true beliefs. In high stakes litigation, electronic documents have become known as the "star witness" or the "corporate equivalent of DNA evidence."

The failure to properly disclose electronic evidence can be an affront to the discovery required by our courts. Such discovery failures can cause significant, unfavorable results in litigation. For example, companies may be subject to an adverse inference instruction by the court to the jury for a failure to produce evidence. Specifically, a judge may instruct the jury that if they could find that a party could have produced e-mail evidence, but failed to, the jury is then permitted to infer that the evidence "would have been unfavorable" to that party. *See*, *MOSAID Tech. Inc. v. Samsung Elecs. Co.*, 348 F.Supp.2d 332, 334 (D.N.J. 2004) ("[Samsung] failed to produce virtually all technical and other e-mails in this case … If you find that [Samsung] could have produced these e-mails … you are permitted … to infer that the evidence would have been unfavorable to [Samsung]."). This spoliation inference jury instruction, as well as monetary sanctions, are "the least burdensome sanctions the Court can impose while still attempting to level what has become an uneven playing field." *Id.* at 340.

Parties may also be penalized via monetary sanctions, case dismissals, and

even incarceration of corporate employees for severe electronic discovery abuses. Monetary sanctions for non-compliance have reached millions of dollars, and are "particularly appropriate" for destruction of electronic information because "it is impossible to fashion a proportional evidentiary sanction that would accurately target the discovery violation" when there is no way to know what, if any, value the deletion of the data had to the opposing party's case. *See*, *U.S. v. Philip Morris USA Inc.,* 327 F.Supp.2d 21, 26 (D.D.C. 2004) (imposing sanction of $2,995,000 for company's failure to preserve e-mails of employees with responsibilities relevant to litigation issues in violation of discovery obligations). Monetary sanctions may be imposed regardless of whether the discovery abuses were intentional. In a case in New Jersey, *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598, 613-17 (D.N.J. 1997), the court determined that "substan-tial sanctions" of one million dollars were warranted for a party's "consistent pattern of failing to prevent unauthorized document destruction" even though no willful misconduct occurred.

Other instances of case dismissals or default judgments as sanctions for intentional discovery abuses have occurred. In *Metro. Opera Ass'n v. Local 100 Hotel Employees & Rest. Employees Int'l Union*, 212 F.R.D. 178, 210, 224 (S.D.N.Y. 2003), a New York district court granted a default judgment in favor of the plaintiffs as a sanction for the defendant's discovery abuses, including failure to produce e-mail, routinely deleting responsive documents from employee computers, and dismantling computers containing responsive material in willful disregard of discovery obligations. In Virginia, a recent high stakes patent action was dismissed in an effort to punish a party for destroying documents. *Rambus, Inc. v. Infineon* (E.D. Va. March 1, 2005).

For particularly egregious non-compliance of electronic discovery obligations, company executives that withhold or destroy documents can be prosecuted for obstruction of justice. *See*, *U.S. v. Lundwall*, 1 F.Supp.2d 249 (S.D.N.Y. 1998) (holding that former Texaco executives who allegedly withheld and destroyed documents sought in civil action for racial discrimination could be prosecuted for obstruction of justice). Furthermore, the obligations and penalties associated with electronic discovery are not simply a function of the litigation process. Under the new Sarbanes-Oxley Act [18 U.S.C §1520(a)(2) (2005)], executives may be subject to criminal penalties for violations of the SEC rules concerning retention of electronic audit records "which are created, sent, or received in connection with an audit … and contain conclusions, opinions, analyses, or financial data."

Proposed Changes

The nature of electronic documents and their creation, storage and automated destruction warrant separate discovery rules in litigation for electronically stored data. Unlike words on a piece of paper, electronic information is dynamic. Technology allows computers to automatically create information without the operator's direction or awareness. Electronic data may also be incomprehensible when separated from the system that created it. Additionally, electronically stored information, although "deleted," may still continue to exist in forms difficult to locate, retrieve or search. These uniquely electronic differences from a paper trail lead to increased uncertainty as to how to treat electronically stored information under the current discovery rules.

In response to the rapidly increasing amount of electronic discovery, the federal judiciary disseminated a proposed set of rules to govern electronic discovery. *See*, Lee H. Rosenthal, *Report of the Civil Rules Advisory Committee* (Aug. 3, 2004) (www.uscourts.gov/rules/comment2005/CVAug04.pdf).

If adopted, the proposed set of rules would amend the Federal Rules of Civil Procedure in seven distinct ways. The first four propositions are not dramatic, nor are they expected to be particularly controversial. They are, however, intended to set common expectations and understanding regarding the role of electronic discovery. The first four Rule changes are:

1. "Updating" the language in Rule 34 to reflect the changes in technology that have caused some of the language to become outdated;
2. Providing for attention to electronic discovery issues at the outset of litigation;
3. Creating a procedure whereby issues regarding the form of production and preservation of electronically stored information are addressed early in the discovery process; and
4. Applying Rule 33 for interrogatory responses to electronically stored information as well as business records.

The final three propositions for change merit additional discussion.

The fifth proposed change, recognizing the sheer volume and unique character of electronic information, would provide a general procedural mechanism for return of inadvertently produced privileged materials and a process for challenging privilege claims. The proposal would essentially codify emerging "best practices" that would benefit all parties involved in litigation.

The sixth proposed modification is to Rule 26(b)(2), and it applies a two-tier structure. The first tier: A party must provide discovery of relevant, reasonably accessible electronically-stored information without a court

order, but a party need not review or provide discovery of electronically-stored information that it identifies as not "reasonably accessible." The second tier: If the requesting party moves for discovery of purportedly inaccessible information, the responding party must show that the information sought is truly not reasonably accessible. The court would then balance the burden or expense of the proposed discovery against its likely benefit.

The seventh proposed change is to Rule 37 and would provide a "safe harbor," under specified circumstances, to a party that fails to provide electronically stored information. The proposal would protect a party from sanctions for failing to provide electronically stored data that was lost as a result of the automated or routine operations of the computer system. This proposition is the most controversial and least settled proposal. As currently framed, the proposed change does not define the scope of a party's duty to preserve electronically stored information.

Preservation obligations for electronic data are, in principle, the same as in the paper world, and the traditional duty to preserve evidence extends to electronically stored information when a company is faced with the prospect of litigation. Generally speaking, a party has an obligation to take "reasonable steps" to preserve information that it "knew or should have known" would be relevant to litigation on the horizon. While the preservation obligations remain the same, unique challenges arise in storing electronic data. For instance, electronically stored information is not easily visualized. Thus, it may be difficult to track down all potentially relevant materials. Moreover, the compression of data may magnify the consequences of error.

In order to properly comply with preservation obligations, the litigant must be in "possession, custody, or control" of the discoverable information. Litigants must first ask themselves: "Who has or where is the electronically-stored evidence relating to this case?" Once this question has been answered, the litigant must look at the various ways electronic data may have been stored and what, if any, potential challenges exist. For example, backup tapes, also commonly referred to as "data dumps," are utilized to preserve information in case of a system failure. Backup tapes store a vast amount of potentially discoverable information. This information, however, is often automatically recycled, thus destroying potentially relevant evidence. Suspension of a recycling program may cost companies large sums of money. Moreover, it may be expensive to restore and produce data stored on a backup tape. Federal and state courts have issued conflicting opinions on whether information stored on backup tapes are "accessible" or "inaccessible" for discovery purposes and what party should bear the cost of restoring the stored data. *See*, *Toshiba Am. Elec. Components, Inc. v. Super. Crt.,* 124 Cal. App. 4th 762, 773 (2004) (shifting reasonable expense to requesting party for recovery of usable information on backup tapes); *Zubalake v. UBS Warburg LLC,* 217 F.R.D. 309 (S.D.N.Y. 2003) (applying a discretionary cost-shifting to requesting party for recovery of inaccessible data on backup tapes). Considering the uncertainty in this area of law, companies are advised to tread cautiously when using backup tapes as they may present significant consequences once litigation ensues.

Retention Policy a Must

Based on the proposed changes to the discovery rules and the challenges electronic discovery presents, it is integral that businesses institute a retention policy so that relevant information will be preserved and retrievable if the company eventually finds itself involved in litigation. A company should consider its regulatory and business needs when creating a retention policy. For example, what information is the organization required to maintain for regulatory or other legal purposes? What data is necessary to maintain the core business? How much control over technology use will the organization's culture tolerate?

Businesses should be realistic, and construct a rational and enforceable retention policy. It is advisable that companies implement a policy that strongly discourages creating or accessing inappropriate materials, and one that deletes electronic materials as scheduled. Moreover, organizations should be proactive: limit files or isolate servers containing privileged or trade secret data; designate a knowledgeable and effective technical witness to suggest and defend protocols; preserve responsive data in technologically appropriate formats; and adhere to federal and state guidelines that require companies to preserve specific data for prescribed periods of time.

In summary, protecting the client in electronic discovery is an art. The twin keys required for success are to "be prepared" and "be proactive" prior to any hint of litigation.