New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

ALM

LITIGATION

Web address: http://www.nylj.com

TUESDAY, OCTOBER 10, 2006

In the Mirror Image?

Courts have allowed access to opponent's hard drive only in specific situations.



ART BY NEWSCOM/MICHELLE STEINBERG

BY ARTHUR S. LINKER

ACCESSING a "mirror image" of an opposing party's computer hard drive has become an increasingly popular aspect of litigants' discovery plans. Such access raises a number of unique discovery issues. As recent cases demonstrate, courts will only allow such access in a few very specific situations. This article will delineate the ground rules governing attempts to gain access to an opponent's hard drive.

Accessing Data

Data contained on a "hard drive," which is a storage device within a computer, consists of "bits" of information in binary form stored in defined locations (called "sectors") of the hard drive. The computer's operating system software (typically, Microsoft Windows) organizes the data by referencing these sectors to named "files," which are listed in a "directory" maintained by the operating system. When the data contained in a file is accessed through use of an application program (such as a word processor or a spreadsheet, database or e-mail program), a text document, spreadsheet or e-mail is displayed, which can be viewed, copied or printed.

Hard drives also contain data that has been left intact, in whole or in part, after files have been modified or "deleted," either in the ordinary course of business or to thwart discovery. Such deleted data "remains…in whole or in part until it is overwritten by ongoing usage or 'wiped' with a software program specifically designed to remove deleted data. Even after the data itself has been wiped, directory entries, pointers, or other metadata relating to the deleted data may remain on the computer."[1] Often, such "deleted" data, although not accessible using the computer's operating system, can be recovered by forensics experts, either directly from the hard drive, or preferably from a "mirror image" of the hard drive.

"A 'mirror image' is generally described as 'a forensic duplicate, which replicates bit for bit, sector for sector, all allocated and unallocated space…on a computer hard drive.'" *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668, *3 (D. Kan. March 24, 2006). Forensics experts use specialized software to capture all of the data on the hard drive without altering any of its contents.

Viewed as Document Request

While "electronic documents are no less subject to disclosure than paper records," *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317 (S.D.N.Y. 2003), the real issue is access, either onsite or through a mirror image, to an opponent's entire hard drive. Such access raises concerns regarding relevance, overbreadth, undue burden, privilege and privacy.

While access to a hard drive is sometimes considered to be a form of "inspection" of property, e.g., *Eugene J. Strasser, M.D., P.A. v. Bose Yalamanchi, M.D., P.A.*, 669 So.2d 1142 (Fla. App. 1996), courts usually view a request for such access as a document request, analogizing a hard drive to "an electronic filing

Arthur S. Linker *is a litigation partner with Katten Muchin Rosenman in New York.* **Evan Newman**, *a Katten summer associate, assisted in the preparation of this article.*

cabinet." *Menke v. Broward County School Board*, 916 So.2d 8, 10 (Fla. App. 2005). Courts thus ordinarily view requests for wholesale access to hard drives as improper, because, as explained in *Menke*, "we have never heard of a discovery request which would simply ask a party litigant to produce its business or personal filing cabinets for inspection by its adversary to see if they contain any information useful to the litigation. Requests for production ask *the party* to produce copies of the relevant information in those filing cabinets for the adversary." (emphasis in original) Id. Thus, Rule 34 contemplates that the responding party will search for and produce the relevant data; it "does not give requesting party the right to conduct the actual search." *Floeter v. City of Orlando*, 2006 WL 1000306, *3 (M.D. Fla. April 14, 2006) (quoting *In re Ford Motor Co.*, 345 F.3d 1315, 1317 (11th Cir. 2003)).

Strong Grounds

In light of the extremely intrusive nature of access to an adverse party's hard drive and overbreadth, privilege and burdensomeness concerns, a request for production of a "mirror image" will be denied absent strong grounds.[2] Courts require production of a "mirror image" only in certain well-defined circumstances. These include cases where the computer itself allegedly was used to commit the wrong that is the subject of the lawsuit, and those where there is evidence that computer files that should have been but were not produced improperly were deleted or destroyed.

In the recent case, *AutoNation, Inc. v. Hatfield*, 2006 WL 60547 (Fla. Cir. Ct. Jan. 4, 2006), for example, defendant was accused of stealing trade secrets in an attempt to gain a competitive advantage for his probable new employer. Because evidence demonstrated that he had improperly downloaded confidential proprietary information from plaintiff, he was required to produce for examination by a forensic computer expert a computer to which he had sent e-mails, to determine whether those e-mails had been forwarded and whether any other material belonging to plaintiff existed on the computer. Similarly, in *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 (D. Kan. March 24, 2006), an action for copyright infringement, plaintiffs claimed that defendants wrongfully copied digital embroidery designs and then sold the designs to at least one third party. Because the alleged infringement was claimed to have occurred through use of computers to download copyrighted material, the court found that computer evidence was particularly important, and ordered that all of defendants' computers be made available for mirror imaging, at plaintiffs' expense.

Likewise, in *Physicians Interactive v. Lathian Systems Inc.*, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003), plaintiff alleged that defendants hacked its Web site by sending "electronic robots" to steal its customer list, computer code and confidential data. Plaintiffs proffered evidence that defendants launched three "attacks" on its file servers to surreptitiously steal confidential data. The court granted plaintiff limited expedited discovery to enter the premises where the computers used in the alleged attacks were located and to obtain a "mirror image" of the computer equipment containing electronic data relating to the alleged attacks on plaintiff's file server. See also *Computer Associates International, Inc. v. Quest Software, Inc.*, 2003 WL 21277129, *1 (N.D. Ill. June 3, 2003) (defendants did not dispute having had possession of plaintiff's source code in copyright infringement and trade secret case, "making it likely that a thorough search of the drives will lead to the discovery of some relevant information").

In other cases, courts have required production of a "mirror image" where there was an unexplained failure to produce relevant documents, or evidence of improper deletion or destruction of computer files. Thus, in the recent case *Leviton Mfg. Co., Inc. v. Nicor, Inc.*, 2006 WL 1305036 (D. N.M. Jan. 6, 2006), e-mailed documents produced by other parties tended to show that defendant had not produced all responsive documents and he had not offered an excuse for not producing documents that existed. Also, although defendant contended that he had not retained e-mails because his only communications were through the equivalent of a "Hot Mail" account which precluded retention of e-mails, there was evidence that he in fact operated his own Web site to which e-mails were sent. The court therefore ordered defendant to make his computers available for inspection.

In *Etzion v. Etzion*, 7 Misc.3d 940, 943 (Sup. Ct. Nassau Cty. 2005), a matrimonial action, the court granted the wife's application to clone or copy the husband's hard drive based on his alleged history of past fraudulent conduct, stating that it was required to insure complete discovery where "it is suggested that some files may have been deleted or altered." In *Renda Marine, Inc. v. U.S.*, 58 Fed. Cl. 57 (Fed. Cl. 2003), plaintiff was granted access to defendant's hard drive where defendant admitted that it routinely deleted e-mails even after the lawsuit commenced. In *GTFM, Inc. v. Wal-Mart Stores, Inc.*, 2000 WL 335558 (S.D.N.Y. March 30, 2000), the court ordered defendant to make its computer facilities available for on-site inspection for the purpose of allowing plaintiff's expert to ascertain whether and how it was possible to extract information about the purchase of trademark-infringing goods, where defendant had misrepresented that its computer system did not maintain the relevant records.[3]

Mere Suspicion Is Insufficient

Absent "evidence of intentional deletion of data," courts usually deny requests for discovery of hard drives. *Menke*, 916 So.2d at 12 (access to hard drive denied because "no evidence of any destruction of evidence or thwarting of discovery").[4] "[A] party's suspicion that another party has failed to respond to document requests fully and completely does not justify compelled inspection of its computer systems." *Bethea v. Comcast*, 218 F.R.D. 328, 329-30 (D. D.C. 2003). In *Bethea*, an employment discrimination case, plaintiff found "incredulous" defendant's assertion that it had created no documents regarding plaintiff except for a single organizational chart, arguing that she "*just can't believe* that an organization of that magnitude could go through a reorganization and would not create one single document" and therefore seeking access to defendant's hard drives to determine whether there were additional documents that were not produced. (Emphasis in original). The court ruled, "plaintiff is speculating, and such conjecture does not warrant the compelled inspection of a computer system that contains voluminous information relating to many topics other than plaintiff's employment discrimination claim." Id. at 30.[5]

A recent case illustrates the limitations on the discovery of a "mirror image" that can be imposed by a court in order to ascertain whether relevant documents have been withheld and to prevent a party from pursuing an inappropriate "fishing expedition." In *Liturgical Publications, Inc. v. Karides*, 2006 WL 931892 (Wis. App. April 12, 2006), plaintiff alleged that defendants, former employees who resigned and began working for a competitor, misappropriated

computer information, programs and data. The court ordered the making of mirror images of defendants' personal and business computers under the supervision of a referee, but limited the inspection of the mirror images to a "hash value search, comparing hash values of materials on the defendants' computers to hash values on [plaintiff's] computers." Id. at *5. The court explained that "hash values" were "alphanumeric identifiers of files," id. at n.7, i.e., essentially digital fingerprints.

When the hash value search did not result in any matches, plaintiffs sought a second inspection of the mirror images with defined search parameters, including a search for specified words and evidence of various forms of computer activity. The court denied this additional request, finding that the request "essentially amounted to a fishing expedition" and would be unreasonable in light of the negative result of the "hash value" search. Id. at *6.

Protocol

An order for imaging of a hard drive that sets "no parameters or limitations" notwithstanding the presence of confidential and privileged information is improper. *Southern Diagnostic Associates v. Bencosme*, 833 So.2d 801, 803 (Fla. App. 2002). When courts grant access to a party's entire computer hard drive, they typically establish or approve a "protocol" to protect the party's privacy and any privileged documents. In *Playboy Enterprises, Inc. v. Welles*, (see endnote 3) an early case establishing such a protocol, the court appointed a neutral expert who would produce a mirror image of the defendant's hard drive. The expert would serve as an officer of the court and any "disclosure" to him of documents on the hard drive would not result in a waiver of the attorney-client privilege. Defendant's counsel would then review any recovered documents, produce those that were responsive and create a privilege log for any documents withheld on a claim of privilege. Defendant's counsel would be the sole custodian of and would retain the "mirror image" and copies of all retrieved documents. *Playboy*, 60 F.Supp.2d. at 1055.



Most cases have followed this or other similar protocols. In *Balboa*, for example, the court ordered the parties, with the assistance of their respective computer experts, to agree on a search protocol, whether one using key word searches and/or other search procedures, that would adequately protect confidential and irrelevant personal data. *Balboa Threadworks, Inc. v. Stucky*, 2006 WL 763668 at *5.

Who Bears the Expense?

As noted above, in some of the cases in which creation of a "mirror image" was ordered, the requesting party proposed to perform the imaging at its own expense. Generally, however, "the presumption is that the responding party must bear the expense of complying with discovery requests." *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978). Courts, however, have developed a fairly uniform set of factors that are employed when considering whether there are grounds to shift the cost of production to the requesting party. The factors include the extent to which the request is specifically tailored to discover relevant information; the availability of such information from other sources; the total cost of production, compared to the amount in controversy and to the resources available to each party; the relative ability of each party to control costs and its incentive to do so; the importance of the issues at stake; and the relative benefits to the parties of obtaining the information. *Zubulake*, 217 F.R.D. at 322. Presumably, these factors may apply in some cases so as to require a requesting party (which otherwise is unwilling to do so) to pay for all or some of the costs associated with imaging.

One court, however, in addressing the cost-shifting issue, held that a producing party's costs for hiring a computer consultant to image hard drives and to search for privileged communications contained in the images so that they could be removed prior to production should not be shifted to the requesting party, because they were "costs of…preventive measures undertaken before the actual disclosure of the information" and were "analogous to the review of documents for privileged information and should not be shifted to the requesting party." *Computer Associates*, 2003 WL 21277129 at *2.

In sum, litigants seeking access to a "mirror image" of an adversary's hard drive should be prepared to show either that the computer in question was used to commit the alleged wrong or that relevant documents that have not been produced existed and likely were deleted or destroyed. They should also be ready to propose a suitable protocol for imaging using the services of a nonparty expert to limit disclosure to relevant documents and to preserve any applicable attorney-client privilege.

•••••••••••••●●●•••••••••••••

1. "The Sedona Principles: Best Practices Recommendations & Principles for Addressing Electronic Document Production," Appendix A at 51 (The Sedona Conference 2004).

2. See, e.g., *BG Real Estate Services, Inc. v. American Equity Ins. Co.*, 2005 WL 1309048, *5 (E.D. La. May 18, 2005) ("request for the entire 'computer hard drive'…is overly broad and seeks much that is irrelevant and not likely to lead to the discovery of admissible evidence"); *Galvin v. Gillette Co.*, 19 Mass.L.Rptr. 380, 2005 WL 1476895, *4 (Mass. Super. May 19, 2005) (state official's request to have access to and search "hard drives (of all computers of Gillette and Gillette personnel)" denied as "nearly impossible to comply with"); *Dikeman v. Mary A. Stearns, P.C.*, 560 S.E.2d 115, 117 (Ga. App. 2002) (request to produce full and complete copy of hard drive denied because "overbroad, oppressive, and annoying and to require undue burden and expense").

3. See also *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 641 (S.D. Ind. 2000) ("mirror image" ordered to permit plaintiff at its own expense to attempt to recover deleted files, based on showing of "some troubling discrepancies with respect to defendant's document production"); *Playboy Enterprises, Inc. v. Welles*, 60 F.Supp.2d 1050 (S.D. Cal. 1999) ("mirror image" ordered to attempt to recover deleted files where defendant produced very few e-mails or hard copies of computer files and admitted that it was her custom and practice to delete e-mails); *Alexander v. F.B.I.*, 186 F.R.D. 78, 96 (D. D.C. 1998) (discovery of nonparty witness' hard drive granted where his conduct in deleting files prior to receiving subpoena was "highly unusual and suspect" in light of pending government investigation).

4. See also *Floeter*, 2006 WL 1000306 at *3 (denied where no showing that plaintiff requested information contained on hard drive that defendant failed to produce); *Williams v. Mass. Mutual Life Ins. Co.*, 226 F.R.D. 144, 146 (D. Mass. 2005) (denied where plaintiff "provided no reliable or competent information to show that [d]efendants' representation [regarding completeness of production]…are misleading or substantively inaccurate"); *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 169 (S.D.N.Y. 2004) ("widespread destruction or withholding of relevant information" not shown); *Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc.*, 2003 WL 1809465 (N.D. Ill. April 4, 2003) (denied where there was no evidence of withholding of or tampering with evidence).

5. See also *McCurdy Group, LLC v. American Biomedical Group, Inc.*, 9 Fed.Appx. 822, 831 (10th Cir. 2001) (mere skepticism that adverse party produced all relevant and nonprivileged documents from hard drives was insufficient to warrant "drastic discovery measure" of physical inspection of hard drives); *Fennell v. First Step Designs, Ltd.*, 83 F.3d 526, 533 (1st Cir. 1996) ("mere speculation" that document was fabricated after its ostensible date was insufficient to require forensic examination of hard drive to attempt to determine creation date of file).

This article is reprinted with permission from the October 10, 2006 edition of the NEW YORK LAW JOURNAL. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit **almreprints.com**. #070-10-06-0040

New York Law Journal

A NEW YORK LAW JOURNAL SPECIAL SECTION

INVESTIGATIONS & COMPUTER FORENSICS

Tuesday, May 30, 2006

ALM

Government Investigators Focus In on E-Mail

With requests for not only full, but fast, subpoena compliance, corporate entities face significant challenges to which the key is preparation.

BY SCOTT A. RESNIK

E-MAIL HAS TRANSFORMED the way the world communicates and does business. It also has become a highly sought-after form of evidence in white-collar criminal and regulatory investigations.

As an increasing percentage of business communication is entrusted to e-mail, conversations that once passed and vanished over telephone lines or on readily discarded fax pages, now lay preserved for years—often unbeknownst to their creator—electronically chiseled into a server, hard drive or back-up tape. A stored e-mail has the potential to provide an investigator with a trove of information, from the text of a past conversation, to the substance of attached files, to a catalogue of recipients and copied parties. For the government investigator, stored e-mails have the ability to narrate past crimes or regulatory violations and identify co-conspirators through frozen-in-time communications with a clarity and ease that was unimaginable a short time ago.

It took law enforcement and regulatory agencies a while to appreciate the bounty offered by this electronic document trail and harness the human and technological resources needed to tap into this information source. But with increased staffing and the tools of computer forensics, the days when a government investigator could be dissuaded by skilled counsel from putting a company through the rigors of collecting e-mails in response to a subpoena are gone for good. In fact the pendulum has swung in the opposite direction.

The opening salvo of a white-collar criminal or regulatory investigation will likely be a corporate subpoena featuring a request for relevant e-mails. A company's ability to gather, to the government's satisfaction, relevant e-mail will impact dramatically on the government's view of whether the company is cooperating with, or hindering, the investigation. The consequences of such a determination can, obviously, be dire.

While there is nothing new in the observation that shoddy subpoena compliance is a sure way to run afoul of government investigators, e-mail compliance poses additional pitfalls for the unprepared. With heightened investigatory focus on electronic evidence, prosecutors and regulators are insisting on e-mail compliance on expedited time schedules from subpoenaed companies. Compliance must not only be full, but fast.

The challenge this poses to corporate entities with thousands of individuals and a panoply of e-mail accounts, hard drives, servers, back-up tapes, PDAs and laptops, is significant. A subpoenaed company acting in good faith to comply and cooperate with the government can still suffer dramatic consequences if it cannot adequately harness its e-mail systems to make complete and timely productions.

Indeed, in-house counsel who wait until a subpoena arrives to begin familiarizing themselves with the strengths and weaknesses of their e-mail systems, place themselves and their company at a distinct disadvantage. And as the emerging legal landscape warns, the consequences can be significant.



ART BY ISTOCK

The Compliance Environment

The challenge of electronic evidence compliance begins with the heightened expectations of investigating agencies. Most regulators and prosecutors are far removed from the technological challenges facing modern companies.

Government investigators often take a broad-brush approach to demands for electronic discovery. The prevailing mind-set remains that electronic communications are easy for a corporation to preserve and produce. Further, law enforcement's concern that electronic information remains susceptible to destruction or tampering reinforces their instinct to insist on prompt production.

Corporate counsel faced with grand jury or regulatory subpoenas for electronic communications in this environment must be prepared to act quickly and comprehensively. A

Scott A. Resnik *is a litigation partner in the New York office of Katten Muchin Rosenman, and a member of the firm's white collar criminal and civil litigation group.*



company's opportunity to cooperate with the authorities and negotiate a favorable resolution of the investigation will be heavily influenced by its ability to comply fully and expeditiously with the government's subpoena. This is especially so in the securities industry, where the Securities and Exchange Commission requires broker-dealers to preserve business-related e-mails for three years, and to keep two years' worth of stored e-mails available for "prompt" production to the Commission if requested.[1]

Anticipate and Prepare

In such an atmosphere of heightened compliance expectations, corporate counsel cannot, as already noted, wait for the arrival of a regulatory subpoena to begin familiarizing themselves with the capabilities of their firm's electronic document retention and retrieval capabilities.

Counsel best positioned to handle the crisis of an investigation are those who have already established a working relationship with their company's information technology department and are knowledgeable of data storage policies and procedures. Armed with this information, counsel can effectively interface with the regulator or prosecutor and negotiate meaningful limitations to the scope of the subpoena and adjustments to the time frame of compliance. It will also enable counsel to make appropriate representations to regulators concerning the company's compliance with applicable industry regulations on the storage of electronic communications.

Conversely, if counsel is unfamiliar with e-mail retention policies and recovery capabilities, initial negotiations with the investigators can be counter-productive. Setting deadlines that cannot be met, or unintentionally misrepresenting what can be produced, will quickly sour relations with the investigating agency and often doom any attempts at cooperation.

A company's obligation to preserve potentially relevant e-mails likewise does not necessarily require the arrival of a subpoena to be triggered. While the receipt of a criminal or regulatory subpoena clearly places a duty upon a company to preserve responsive documents and halt any regular destruction procedures, companies are well advised to begin preservation efforts when an investigation becomes reasonably foreseeable.

In *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003), the district court, addressing the preservation of electronic evidence in the context of an employment discrimination case, held that "the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant in future litigation." Accordingly, "once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." Id. at 218.

Zubulake's forward-looking preservation rule would likely apply with equal force in the context of an anticipated government investigation. Prudent corporate counsel, post-*Zubulake*, therefore, should begin preserving electronic evidence once a criminal or regulatory investigation becomes reasonably foreseeable.

A failure to preserve electronic communications in the face of a foreseeable investigation invites great risk. An intentional failure to preserve such evidence can lead to criminal prosecution for obstruction of justice.[2] Even an unintentional failure to halt the destruction of relevant electronic evidence can result in sanctions.

Illustrative is *MOSAID Tech. Inc. v. Samsung Elecs. Co.*, 348 F. Supp. 2d 332, 337-38 (D.N.J. 2004), where the court concluded that even in the absence of bad faith, a company's failure to put a litigation hold on e-mail, which resulted in the prejudicial destruction of relevant technical e-mail, warranted an adverse inference instruction and monetary sanctions.[3]

With increased staffing and the tools of computer forensics, the days when a government investigator could be dissuaded by skilled counsel from putting a company through the rigors of collecting e-mails in response to a subpoena are gone for good.

This refusal to require bad faith as a prerequisite to imposing sanctions provides convincing evidence that courts are joining with investigators in growing increasingly intolerant of companies that do not adequately preserve and produce electronic communications. In appropriate cases, it is not uncommon for courts to enter orders requiring the preservation of potentially relevant electronic evidence. When parties fail to abide by such orders, the consequences are predictably dire.[4]

Can You Assure Full Compliance?

Similarly, to promote accountability in electronic document productions, the SEC often seeks an assurance of full compliance from the respondent company. In addition, it is standard for the SEC to require a company, as part of any settlement agreement, to certify in writing, under penalty of perjury, that it has produced all required documents.[5]

To be in a position to satisfy either of these obligations, counsel must ensure that their client's retention and collection efforts are thorough and well-documented. Pre-investigation efforts by counsel to ensure that the right personnel are involved with compliance, and that procedures are in place to both avoid the destruction of relevant e-mails and to ensure the full recovery of stored messages, will pay dividends when the time for assurances or certification comes.

The SEC has imposed some jaw-dropping fines in resolving investigations of corporate wrongdoing where corporate assurances of complete electronic discovery compliance were later revealed to have been inaccurate.

In *SEC v. Deutsche Bank Securities Inc.*, Litigation Release No. 18854 (Aug. 26, 2004), the SEC imposed a $7.5 million fine on Deutsche Bank (DB) (in addition to the $50 million fine to resolve the underlying investigation into research analyst conflicts of interest) for failing to "timely produce all e-mail during the investigation." DB's trouble began after it had made assurances to the SEC that its production of requested e-mail was complete.

Over the course of the next year, however, DB discovered and produced an additional 227,000 e-mails, more than tripling its original "complete" production. Id. The SEC blamed this compliance failure with delaying the completion of the investigation for over a year and fined DB accordingly. Id.

Similarly, in *In the Matter of JPMorgan Securities, Inc.*, Admin. Proc. File No. 3-11828 (Feb. 15, 2005), during an investigation of stock analyst misconduct, JPMorgan made repeated representations that all relevant e-mail requested by the Commission had been produced. Subsequently, in response to further requests by the SEC, JPMorgan revealed that it had been unable to locate and restore certain backup tapes containing responsive e-mail. For this failure, which was disclosed months into the investigation, JPMorgan agreed to settle with the SEC, NYSE and NASD for $2.1 million in fines. Id.[6]

The consequences of making a knowingly false certification of compliance to a court were starkly spelled out in *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, Case No. 502003-CA-005045, 2005 WL 679071 at *1-*5 (Fla. Cir. Ct. March 1, 2005). The Florida state court gave the jury a detailed adverse inference charge after Morgan Stanley was discovered to have made a knowingly false certification that it had complied with a court order requiring the complete production of e-mail evidence.

Morgan Stanley had submitted the certification knowing that it had failed to search or produce over 2,000 backup tapes and had continued to delete e-mails on a 12-month schedule in violation of the SEC rule that e-mails be maintained for three years. The jury verdict against Morgan Stanley awarded over $604 million in compensatory damages and $850 million in punitive damages.

To make matters worse for Morgan Stanley, the revelation of its e-mail retention policies attracted the attention of the SEC. In February 2006, MS agreed to settle with the SEC for a record $15 million in fines as a result of its failure to properly maintain its e-mail records in accordance with SEC regulations.[7]

Timing Is Everything

Timing is the other critical factor in compliance with requests for electronic discovery.

Even for the respondent company that can efficiently retrieve requested e-mails, time remains a valuable commodity. This is because one of coun-

sel's primary responsibilities in subpoena compliance is to preserve privilege. And to review a sizeable collection of responsive e-mails for privilege is going to take a significant amount of time.

This reality creates an inherent tension with the government investigator whose instinct is to demand expeditious production. It further emphasizes why the data collection process must be swift. Time lost in retrieving responsive documents will further erode counsel's time to review the data collection to ensure that privileged documents are not disclosed to the government. Even inadvertent disclosure of privileged documents may result in a waiver of the attorney-client privilege.[8]

One strategy for reducing delay frequently advocated by the government is for the respondent company to produce the requested e-mail without attorney review, but with an agreement that the government will not assert waiver if the production contains attorney-client communications or attorney work product. This strategy is fraught with danger for the respondent company. In addition to divulging the substance of critical communications, such an approach can have unintended consequences on the attorney-client privilege in subsequent litigation.[9]

In the context of private-party civil litigation, sanctions are rarely imposed for mere delay in producing electronic discovery.[10] In the realm of regulatory investigations, however, there is evidence of a countervailing trend.

In a recent action, the SEC imposed a $2.5 million fine on broker Merrill Lynch for "failure to furnish promptly to representatives of the Commission…electronic mail communications" as required under §17(a) of the Exchange Act and enabling regulations. *In the Matter of Merrill Lynch, Pierce, Fenner & Smith, Inc*., Admin. Proc. 3-12236 (March 13, 2006). The case is noteworthy because the SEC release does not identify any substantive wrongdoing on the part of Merrill Lynch (ML) nor any failure to produce critical e-mails. The sanction is based solely on the firm's slow compliance response and inadvertent short-comings in its e-mail capture system. Because of this, it is worth a closer look.

From October 2003 through February 2005, the SEC requested that ML produce e-mails in connection with a series of separate investigations. On Oct. 17, 2003, the SEC requested the production of e-mails from six ML employees. Id. at 2. It took ML seven months to produce the requested e-mails. Id.

Also in October 2003, the Commission issued a request in another investigation for the e-mails of five ML employees. ML took two months to begin making its production and completed delivery of the requested e-mails five and one-half months from receipt of the Commission's request. Id. at 3.

In two other investigations in August and September 2004, it took ML over five months to produce requested e-mails. Id. Further aggravating the situation from the SEC's perspective were ML's representations that its e-mail systems were sufficient to retain e-mail and produce it to regulators upon demand. Id.

It was subsequently discovered that ML's e-mail systems were not capturing (a) e-mails that were not in a user's mailbox at the time of the next scheduled tape back-up; (b) e-mail that had been moved from a user's mailbox to a personal folder or shared drive outside the e-mail system or moved to another medium such as a floppy disk, a hard drive, or a USB (universal serial bus) device; (c) e-mail that had been "hard-deleted" prior to the next scheduled tape back-up; and (d) "bcc" recipients on certain e-mail messages. Id.

Based on these technological shortcomings and its slow compliance response, the Commission took the position that ML was in violation of its document retention obligations under the Exchange Act. The settlement not only required ML to pay a fine of $2.5 million, but also to hire at its own expense an independent consultant to review ML's e-mail retention policies and procedures. Id. at 5-7.

Time lost in retrieving responsive documents will further erode counsel's time to review the data collection to ensure that privileged documents are not disclosed to the government.

The *Merrill Lynch* decision demonstrates the potential of electronic discovery to become the "tail that wags the dog" in regulatory investigations.[11] Even in the absence of substantive wrongdoing, a corporation remains vulnerable to dramatic fines if it fails to meet the regulator's timetable for compliance.

The decision makes clear that from the Commission's perspective, five months to produce e-mail was too long. Observers, though, are left to speculate on what time frame, given these circumstances, would have been acceptable. Nonetheless, the decision puts companies on notice that those who fail to act expeditiously in complying with requests for electronic communications, do so at their own risk.

Conclusion

The challenges of responding to an investigator's request for corporate e-mail are many but they are not insurmountable. The key is preparation.

Companies must establish and continually review their electronic document retention and production policies to ensure that once an investigation becomes foreseeable, responsive documents are preserved and can be timely collected. Counsel should be knowledgeable of their clients' technological capabilities and establish working relationships with their IT staff.

If faced with the same requests for e-mail as confronted in *Merrill Lynch*, would your company be able to produce the information in under five months? Can your e-mail system capture "bcc" recipients? If you do not know the answer to these questions, the time to figure it out is now. Not when an SEC subpoena arrives.

1. Rule 17a-4(b)(4), promulgated pursuant to §17(a) of the Exchange Act, requires broker-dealers to "preserve for a period of not less than three years, the first two years in an easily accessible place…[o]riginals of all communications received and copies of all communications sent…(including inter-office memoranda and communications) relating to its business as such…." 17 C.F.R. 240.17a-4(b)(4). E-mail communication falls within this rule. See *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 308, 314 (S.D.N.Y. 2003). Further, Rule 17a-4(j) requires broker-dealers, upon request of the SEC, to "furnish promptly" any records required to be preserved by §17(a) of the Exchange Act. 17 C.F.R. 240.17a-4(j).

2. See, e.g., 18 U.S.C. §1512(c)(1) ("Whoever corruptly alters, destroys, mutilates, or conceals a record, document, or other object, or attempts to do so, with the intent to impair the object's integrity or availability for use in an official proceeding [commits a federal crime]"); 18 U.S.C. §1519 ("Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record…with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States…[commits a federal crime]").

3. See also *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002) (holding that negligent destruction of potentially relevant electronic data can be an appropriate basis for discovery sanctions); *Telecom Int'l Am., Ltd. v. AT&T Corp.*, 189 F.R.D. 76, 82 (S.D.N.Y. 1999) (holding that defendant's destruction of documents, even though not committed in bad faith, demonstrated an "indifference to…discovery obligations" that required the imposition of appropriate sanctions).

4. See *United States v. Philip Morris USA Inc*., 327 F. Supp. 2d 21, 24-6 (D.D.C. 2004) (imposing $2.75 million sanction, ordering party to pay costs related to spoliation and prohibiting party from calling certain witnesses where party did not put in place a litigation hold and permitted routine destruction of relevant e-mail for two years after the court entered a document-retention order).

5. See John Savarese and Carol Miller, "Effective Strategies for Defending Investigations, Sept. 14, 2005," in "Coping With Broker/Dealer Regulation & Enforcement 2005" at 266 (PLI 2005).

6. See also *In Matter of UBS Securities LLC*, Admin. Proc. File No. 3-11980 (July 13, 2005) (for failure to produce relevant e-mail for each individual identified in investigation, UBS agreed to pay $70,000 in fines to SEC, NYSE and NASD).

7. See Bruce Kelly, "E-mail Troubles Continue to Haunt Broker-Dealers, Morgan Stanley to Pay $15 Million Fine," Investment News, Feb. 20, 2006, at 33.

8. See *Genetech, Inc. v. U.S. Int'l Trade Comm'n*, 122 F.3d 1409, 1417 (Fed. Cir. 1997) (holding party's waiver of attorney-client privilege with regards to documents it inadvertently disclosed during patent infringement litigation was general waiver that could be asserted in administrative proceeding before the International Trade Commission); *F.D.I.C. v. Singh*, 140 F.R.D. 252, 253 (D. Me. 1992) (holding inadvertent production of memorandum containing privileged communications constituted waiver of attorney-client privilege).

9. See *In re Columbia/HCA Healthcare Corp. Billing Practices Litig.*, 293 F.3d 289, 302 (6th Cir. 2002) (holding party could not selectively waive attorney-client privilege by providing otherwise privileged documents to government agencies during an investigation but continue to assert privilege as to private litigants).

10. See Shira A. Scheindlin and Kanchana Wangkeo, "Electronic Discovery Sanctions in the Twenty-First Century," 11 Michigan Telecomm. and Tech. L. Rev. 71, 76 (2004) ("The sanctioned behavior most often involved the non-production, i.e., destruction of electronic documents (84%), rather than a delay in production (16%). When parties were sanctioned for delay, the late production was sometimes coupled with some form of deception or misrepresentation to the court, such as the fabrication of evidence or falsely claiming that documents did not exist (43%)").

11. See Terry Weiss, "Summary of Selected Programs From SIA Compliance & Legal Division's 2006 Annual Seminar," Mondaq Bus. Briefing, April 3, 2006 ("The failure to retain and produce electronic data when required to do so has become an independent source of potential liability regardless of any underlying wrongdoing, panel members cautioned…'The tail is now wagging the dog,' the panel warned").

This article is reprinted with permission from the May 30, 2006 edition of the NEW YORK LAW JOURNAL. © 2006 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit **almreprints.com**. #070-10-06-0041