

The New Frontier: **Discovery of Electronic Data**

By MEREDITH FEIN LICHTENBERG and ANN S. GINSBERG

The Federal Rules of Civil Procedure (“FRCP”) specifically provide for discovery of electronic media, and for on-site inspection of computer-stored and other electronic data. Nationwide, courts have held that electronic information is discoverable, limited only by the same constraints as “hard” document discovery – relevance, privilege and “undue burden” – and beyond that, counsel’s ingenuity and the court’s willingness to test the limits of the technological cutting edge.

Electronic media discovery (“EMD”) is important in any kind of case, from simple property damage cases to complex securities fraud litigations. Courts routinely mandate production of e-mail, computer diskettes, codebooks and software. Some go so far as to require production of information they find “likely” to be computerized, whether or not it is known to exist. Even data that never existed as a “hard” document may be discoverable. This article discusses tips for obtaining and protecting yourself against disclosure of EMD.

Electronic v. “Hard” Document Evidence

Production of electronically stored information raises some issues that are not present in the case of traditional “hard” document discovery.

Access. Whereas hard copies of correspondence are easily copied and sent to an opposing party, providing access to the computerized storage of a correspondence file may be more complex. Your company might seek to discover a computerized file in order to view, for example, unprinted drafts of letters, a computerized “activity log” indi-

cating when the letter was edited or unprinted “comments” that can be viewed only on the computer. Or, you might want production of a file in its computerized form if it contains millions of unsorted documents more easily searched on a computer than by hand. Courts generally require production of computerized files if they contain information not present in the hard copy.

Format. Under the FRCP, courts must consider whether straight duplication of a file will suffice to respond to a discovery request, or whether further measures need to be taken. A court might permit your company to physically inspect your adversary’s computer system to obtain information. Or, a court might require your opponent to create a computer program that translates raw data into a readable form for you.

Cost. The higher your adversary’s cost of complying with your EMD requests, the more courts scrutinize the material sought, and compare it to what could be produced in hard copy. Weighing the cost against how

“**Electronic information is discoverable**, limited only by the same constraints as “hard” copy discovery—relevance, privilege and “undue burden.”

current events

what’s in the news now

Courts Split On Scierter Standard: In a ruling which conflicts with interpretations by the S.E.C. and most other federal appeals courts, the Ninth Circuit decided that a complaint must state facts giving rise to a strong inference of “deliberately reckless or conscious misconduct” to maintain an action under the Private Securities Litigation Reform Act of 1995. The court also concluded that the mere existence of insider trading does not show the requisite fraudulent intent. *In re Silicon Graphics Inc. Securities Litigation.*

crucial the material is, courts may even require your company to pay for the EMD you seek.

Document Retention Policies and Spoliation. A company's document retention policies are often different for hard documents than for electronic data. Document retention is also a murkier issue when it comes to electronic data. For example, if one of your employees handwrites a draft of a letter, marks it up, and throws it away, the act of "destroying" the document is clear and the likelihood of retrieval is slim. On the other hand, computerized files may not be "destroyed" when they are "deleted" – the system might be configured to store backup files until it runs out of space, or may automatically purge old files regularly. If a document is automatically "destroyed" in this manner, it may be unclear who destroyed the document and what level of intent was involved.

Courts have started to focus on what constitutes sanctionable spoliation of evidence in the electronic realm. At least one court permitted a party to physically examine an adversary's computer system if the party could demonstrate a likelihood of retrieving purged information. Another court held that the necessity for a retrieval program or method for recovering electronic media is an "ordinary and foresee-

able risk" of litigation, indicating that a court-mandated retention policy regarding EMD may not be far behind.

Obtaining EMD

Notify Opposing Counsel To Preserve Electronic Evidence. When documents are stored electronically, it is important to notify your adversary to preserve electronic evidence as soon as litigation commences, or earlier if feasible. Otherwise, an adversary may destroy relevant evidence merely by continuing its regular policies, which may include overwriting data. An early letter, informing opposing counsel that you will seek electronic data, will put him or her on notice to take whatever steps are necessary to avoid spoliation of the evidence. Consider instructing your adversary to:

- Stop all rotation, alteration and/or destruction of electronic media that may affect relevant data, and refrain from altering, erasing or overwriting relevant data;
- Refrain from disposing of electronic media storage devices;
- Maintain an activity log to document substantive modifications to relevant electronic data or processing systems;
- Maintain a log for relevant electronic data, including backup, archive or disaster recovery. The log should include the names of people given access and the date, time and the nature of the activity performed.

Seek Pre-Discovery Information About the Adversary's Computer System. This information will help you craft the most useful discovery requests later. To get an overview of your adversary's computer system, consider asking for:

- Methods of information storage, including e-mail, and type of software used, including home and lap-top computers of key employees,
- Length of time information has been stored in this manner,
- Format, location and substance of information stored,
- Backup software and procedures,

“...it may be unclear who destroyed the document and what level of intent was involved.”

current events

what's in the news now

Disclosure of Board Disputes Not Required: The First Circuit recently held that a company was not required to disclose in its registration statement for an initial public offering the fact that members of its Board of Directors substantially disagreed about the strategic direction of the company. Although the Court found such disagreement to be material, it concluded that disclosure was not necessary to make other statements in the registration not misleading. *Cooperman v. Individual Inc.*

ABA Approves use of E-mail for Client Communications: Concluding that lawyers have a reasonable expectation of privacy when using e-mail, the American Bar Association has approved the use of unencrypted e-mail, including e-mail sent over the Internet, to send confidential client-related information. However, the Opinion advised that a lawyer seeking to communicate highly sensitive information should consult the client regarding its preferred method of transmission prior to using e-mail. *ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion 99-413 (March 10, 1999).*

- Methods of inputting, processing and outputting information,
- Which personnel have access to which files, and who is knowledgeable about storage and retrieval of data, and
- Status of and policies with respect to deleted files.

This information request can be part of a notice to take the deposition of the people most knowledgeable about the company's information systems or, if local rules permit, can be included in a letter to your opposing counsel. As part of your initial investigation, you might also consider requesting an inspection to survey computer-stored data, and consulting with an EMD expert in order to determine what to ask at inspections, what to ask at depositions, and how to analyze the responses you get.

Draft Enhanced Discovery Requests. By the time you are ready to draft discovery requests, you should be armed with as much information as possible about your adversary's computer systems. Discovery requests should describe the electronic information you seek as specifically as possible, to avoid objections on the ground of vagueness or undue burden. Moreover, as with hard document discovery, a party may move to compel production of wrongfully withheld electronic data. If you must move to compel, be prepared to identify to the court a specific method to obtain the requested information, based on the adversary's description of how the data is stored. Parties may also work out a protective order to ease concerns about disclosure of proprietary information or disruption of business operations.

Protecting Your Company

Companies with exten-

sive electronic databases and archives should develop defensive strategies and procedures to reduce exposure on a going-forward basis. Strategizing will require a thorough understanding of one's own electronic data, computer systems, and potential liabilities, similar to the methods used to obtain discovery from your adversary. Consult with your in-house information systems staff and consider hiring an expert to pinpoint vulnerabilities in your own system.

Develop A Comprehensive Document Retention Policy For Electronic Media.

Keep in mind that your document retention policy likely will be produced in any litigation and draft it accordingly. The policy should provide procedures to purge electronic media on a regular basis and to suspend purging if you are aware of or reasonably anticipate litigation. This will help your company to satisfy its duty to avoid spoliation of evidence. Emphasize accountability by making supervisors and managers responsible for their subordinates' compliance with the policy. All documents relating to this policy should be kept in a central location, at the offices of either the General Counsel or the manager of your company's information systems.

Develop an Electronic Media Policy.

By the time you are ready to draft discovery requests, you should be armed with as much information as possible about your adversary's computer systems.

current events

what's in the news now

Former Executive May Have To Repay Stock Option Profits: A former IBM executive who left the company to join a rival may be forced to repay to IBM the profits he received by exercising company-granted stock options as the options were not "wages." The U.S. District Court for the Southern District of New York noted that the executive could keep the profits if he could demonstrate that he was constructively discharged. *International Business Machines v. Martson*.

Attorney-Client Privilege Does Not Shield Conversation With Investment Banker: The IRS was entitled to enforce a subpoena against an investment banker who had explained a proposed investment to the lawyer for the company being audited, the U.S. Court of Appeals for the Second Circuit held. The court noted that the attorney-client privilege would not shield the investment banker's conversations with the lawyer as the investment banker did not play a "translator" role analogous to that of an accountant in previous cases upholding the privilege. *United States v. Ackert*.

“The policy should provide procedures to purge electronic media on a regular basis”

warning those who use your computer systems of the consequences of transmitting and disseminating improper and inappropriate electronic media in the office, you protect yourself against damaging evidence before it is created. Consider including the following guidelines in your policy:

- The Company's e-mail and computer systems are not private and may be monitored without prior notice;
- All e-mail and computer systems are to be used solely for business purposes;
- Unauthorized installation of personal or encryption software is prohibited;
- The Company prohibits the use of e-mail for the transmission, dissemination or solicitation of the following:
 - Proprietary data, trade secrets or other confidential information in violation of Company policy or proprietary agreements;
 - Sexually suggestive, discriminatory or otherwise inappropriate material;
 - Information used to usurp business opportunities, solicit money for personal gain or for job searches outside of this Company;
 - Chain letters, gambling or engaging in any other activity in violation of local, state or federal law;
- Any computer user who engages in conduct determined to be in violation of this policy

shall be subject to corrective and/or disciplinary action, which may include discharge.

Once you have a written policy, set up mandatory periodic training for all computer users, all of whom should submit a signed acknowledgment stating that they have read the policy, been trained in it, and agree to abide by it.

Conclusion

The process of defending against EMD in litigation and preparing prophylactic defensive strategies is undoubtedly time-consuming and expensive. But a company prepared with this knowledge has a defensive strategy already in place before the next lawsuit commences. ■

Meredith Fein Lichtenberg and **Ann S. Ginsberg** are with the New York office of Anderson Kill & Olick, P.C.

AKO Commercial Litigation Advisor is published quarterly by Anderson Kill & Olick, P.C. The Firm has offices in New York, Washington, Chicago, Philadelphia, and Newark. The newsletter informs clients, friends, and fellow professionals of developments in commercial litigation. The newsletter is available free of charge to interested parties. The articles appearing in **AKO Commercial Litigation Advisor** do not constitute legal advice or opinion. Such advice and opinion are provided by the Firm only upon engagement with respect to specific factual situations.

For more information, contact Co-Editors **Jordan W. Siev, Esq.**, (212) 278-1542, jsiev@andersonkill.com; **Ann S. Ginsberg, Esq.**, (212) 278-1512, aginsberg@andersonkill.com; or **Mark L. Weyman, Chair, Commercial Litigation Department**, (212) 278-1852, mweyman@andersonkill.com. Rich Mansfield, Publisher, PRI (732) 548-4609. Copyright © Anderson Kill & Olick, P.C., 2001. All rights reserved.

AKO corner

notable decisions

Viagra Claims Against Oxford May Proceed: Oxford Health Plans. motion to dismiss claims brought by individuals seeking insurance coverage for their medically-necessary Viagra prescriptions has been denied. Oxford argued that the plaintiffs had not exhausted Oxford's administrative appeal remedies. Noting that Oxford had not even assured that the plaintiffs knew about the appeal procedures, District Judge Dearie agreed with AKO's clients. contention that further efforts by the plaintiffs to overturn Oxford's decision would have been futile, and termed Oxford's position "offen[sive to] notions of fairness and common sense." *Sibley-Schreiber v. Oxford Health Plans (NY) Inc.*