

“DIGITAL DISCOVERY: PROTECTING THE PROFESSIONAL CLIENT IN THE INFORMATION AGE”

by Lee H. Ayres

1. Introduction.

The professional world is a vastly different place from what it was just twenty years ago. While personal computers were a rarity then and e-mail did not exist, estimates are that today more than 90% of records are created and up to 70% of records may be stored in digital form.¹ When looked at in concrete terms, the numbers are even more startling. With professionals sending and receiving an average of thirty e-mails per day,² a business of 100 will log almost one million e-mails per year. All told, in 2001 businesses in North America generated approximately 2.5 trillion e-mail messages.³

This sea change, brought on by the advent of information technology in the professional world, has resulted in a corresponding ripple effect in the world of discovery. Because professionals often play lead roles in the discovery process -- whether it be as lawyers advising clients on best discovery practices, as corporate directors and officers adopting and implementing document retention and production policies, etc. -- lawyers who represent professionals are well advised to take note of discovery's changing face. While the scope and length of this forum do not permit a complete, in-depth analysis of the issues, this article discusses general discovery duties and the risks professionals can face when unmindful of these duties, and offers some recommendations for the lawyer representing the professional client in navigating the rough waters of digital discovery.

2. Discovery Duties: Generally.

Rules 26 through 37 of the Federal Rules of Civil Procedure form the cornerstone of parties' discovery duties in federal litigation. In broad terms, those duties can be classified as obligations to preserve and produce.

a. Duty to Preserve.

The duty to preserve embraces any and all relevant evidence over which a party has control and would reasonably know or could reasonably foresee is material to potential future litigation.⁴ While the duty to preserve does not obligate a party to retain every document or tangible item that is in its possession when a complaint has been filed,⁵ a party is subject to a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.⁶ Pursuant to such a duty, a party may adopt a document retention and destruction policy designed to ease the burden of storing and maintaining accumulated documents. A party cannot, however, blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy.

b. Duty to Produce.

The duty to produce discoverable information may attach to any document regarding a matter that is not privileged and is relevant to the claim or defense of any party.⁷ To be sure, matters entirely without bearing (either as direct evidence or as may lead to evidence) are not within the scope of a party's duty to produce.⁸ Nonetheless, to the extent that documents develop useful information, they function successfully as instruments of discovery, to which a duty of production may attach.

The Federal Rules of Civil Procedure make clear that digital data is subject to these same discovery duties of preservation and production; and, they provide for the imposition of sanctions for failure properly to preserve or produce such data. Rules 26(a)(1)(B) and 34(a) call for the inspection, copying, and disclosure of all "data compilations" that a party may use to support its claims or defenses. Parties and their lawyers engaging in misconduct during such discovery may be subject to the imposition of sanctions pursuant to Rules 26(g) and 37(c) or the court's inherent sanctioning power.⁹

3. Risks for Professionals.

_____Recent cases describe the risks run by professionals who fail to educate themselves as how to properly conduct the discovery of digital documents.

Arguably, those professionals who bear the weightiest risks attendant to the

burdens of digital discovery are lawyers themselves. In Metropolitan Opera Association, Inc. v. Local 100, the federal district court for the Southern District of New York awarded sanctions in the form of attorney's fees against the defendant and its counsel for failing to comply with discovery rules, specifically failing to search for, preserve, or produce digital documents.¹⁰ As the court stated:

“[C]ounsel (1) never gave adequate instructions to their clients about the clients' overall discovery obligations, what constitutes a 'document'...; (2) knew the Union to have no document retention or filing systems and yet never implemented a systematic procedure for document production or for retention of documents, including electronic documents; (3) delegated document production to a layperson who...did not even understand himself...that a document included a draft or other non-identical copy, a computer file and an e-mail; (4) never went back to the layperson designated to assure that he had 'establish[ed] a coherent and effective system to faithfully and effectively respond to discovery requests,'...and (5) failed to take any action to remedy the situation or supplement the demonstrably false responses, failed to ask important witnesses for documents until the night before their depositions and, instead, made repeated, baseless representations that all documents had been produced.”¹¹

In Sheppard v. River Valley Fitness One, the federal district court for New Hampshire fined the defendant fitness club's attorney for his failure to turn over requested paper documents and digital communications.¹² As the court noted, though the attorney's obstructive behavior reflected a lack of diligence rather than an intentional effort to abuse the discovery process, the failure to produce the requested computer records and to retain relevant drafts and other documents unfairly prejudiced the plaintiffs and thus merited sanctions.¹³

Lawyers are not the only professionals who may bear the risks of personal liability for failing to properly conduct discovery of digital data. In Danis v. USN Communications, Inc., the federal district court for the Northern District of Illinois levied a \$10,000 personal fine on the defendant's chief executive officer for failing to take reasonable steps to preserve documents and electronic information regularly created and received by the defendant corporation.¹⁴ The underlying case was a class action involving two groups of purchasers of common stock issued by the defendant

corporation, USN Communications, Inc.¹⁵ Prior to the commencement of litigation, USN had no formal retention policy covering the many categories of documents and electronic information in USN's possession.¹⁶ Though USN routinely created back-up tapes, copies were maintained only for a period of about thirty days, after which time the copies were reused.¹⁷ Three months prior to the commencement of litigation, USN enacted policies 1) for "preserving company assets and retrieving key records in anticipation of upcoming office closures and layoffs" and 2) for purging computer drives of terminated employees in response to security concerns.¹⁸ Both of these policies involved the deletion of digital data. Despite an order from the board of directors to the chief executive officer, J. Thomas Elliott, to take steps to preserve potentially relevant documents, no affirmative steps were ever taken to ensure that relevant documents were not destroyed. In granting sanctions against Mr. Elliott personally, the court noted:

The duty to preserve documents in the face of pending litigation is not a passive obligation. Rather, it must be discharged actively.... 'When senior management fails to establish and distribute a comprehensive document retention policy, it cannot shield itself from responsibility because of field office actions. The obligation to preserve documents that are potentially discoverable materials...rests squarely on the shoulders of senior corporate officers.'¹⁹

By imposing sanctions on Mr. Elliott personally, the court made it known not only that senior management bears personal responsibility for conducting the discovery of digital data, but also that any transgression of this responsibility could be met by the assessment of personal liability.

4. Protecting the Professional Client: An Introduction to Digital Discovery.

a. What to Look For.

Before a lawyer can advise a professional client as to the client's digital discovery duties, the lawyer must first understand what is meant by a digital "document." Digital documents may include:

- Electronic Records (e.g. customer lists, financial records, purchase and sales reports, and personnel files).
- Original Electronic Documents (e.g. letters, memoranda, invoices, and design specifications created electronically).
- Electronic Communications (e.g. e-mail messages, voice-mail messages, instant messaging communications, chat room communications, spontaneous conferencing recordings, streaming video recordings, and PDAs/wireless phone recordings).
- Computer Programs (evidencing a particular process, incorporating specific information, or demonstrating the use of proprietary methodologies).
- Computer Operations Logs (containing detailed usage information).²⁰

Because of the data embedded in computer files -- such as names of authors of a document, draft versions of a document, “bcc” recipients, and “read/unread” annotations -- digital data can constitute a goldmine of invaluable discovery over and above the data contained in analogous paper documents.²¹

b. Where to Look.

Digital documents do not reside solely on the hard drives of the computers in a client’s office or on a client’s computer server. Locations of additional digital data may include:

- Hard drives in homes of client’s employees.
- Portable drives in client’s office or homes of client’s employees.
- Lap-tops of client’s employees.
- Handheld computer devices (e.g. Palm Pilots)

- Diskettes in client's office or homes of client's employees.
- On- and off-site back-up files.²²

In addition to physical locations, digital data may reside at varying levels of digital accessibility. The federal district court for the Southern District of New York recently enumerated five categories of digital data:

- Active, online data: Data used in the very active stages of an electronic record's life, when it is being created or received and processed. (e.g. hard drives)
- Near-line data: Data normally accessed through a robotic storage device that houses removable media. (e.g. optical disks)
- Offline storage/archives data: Data on removable media stored in a shelf or rack; lacks the coordinated control of an intelligent disk subsystem. (e.g. JBOD ["Just a Bunch of Disks"])
- Backup tape data: Data stored on tapes typically employing some sort of data compression, permitting more data to be stored on each tape; makes restoration more time-consuming and expensive.
- Erased, fragmented or damaged data: Data "erased" from a system; often exists in fragmented clusters until written over by newly created files; accessible only after significant processing.²³

_____c. Preserving Digital Documents.

In Zubulake, the district court provided some helpful recommendations as to how a lawyer and his client can comply with their obligations to preserve digital materials.

- Know the character and extent of the client's computer system. Where are digital documents located? Digital documents typically leave an electronic footprint in every location of access. By

accounting only for the versions of digital documents residing on the hard drives of the computers in a client's office and on a client's central computer server, the lawyer and client may fail to cover a potentially expansive range of discoverable digital data.²⁴

- Learn about the client's digital document retention policy. How are retained digital documents stored? How are documents intended for destruction destroyed? Because a document retention policy is only as effective as its ability to eliminate all copies of a document intended for destruction, a policy's failure to account for locations of additional digital data may thwart the very purpose of the policy. Consider extending the professional client's document retention policy to cover all copies of electronic files, including, e.g. archival e-mail, back-ups of hard drives, and network files.²⁵
- Avoid a digital document retention policy that is not grounded in legitimate business objectives or would call for the selective purging of information. Such policies will likely be viewed skeptically by a court if challenged in litigation.²⁶
- Ensure that the digital document destruction policy can be suspended easily should litigation arise. Even a policy entered into in the utmost of good faith may spell trouble for the professional client if destruction cannot be halted to preserve key documents for impending litigation.

d. Producing Digital Documents.

Similarly, published authorities have made recommendations for the proper production of the electronic data.

- Identify potentially relevant "key" actors and the potentially relevant universe of documents with respect to each "key" actor.²⁷
- Take precautions to ensure that searches of "key" persons' digital documents will not alter the documents themselves. Embedded

data such as “last-viewed” information can be altered simply by opening a digital document. Consider producing a “snap-shot” of digital documents on an optical disk.

- Search each “key” person’s office computer hard drive, lap-top computer, home computer, handheld computer devices (e.g. Palm Pilots), and network files.²⁸
- Produce any individually “backed-up” data, such as floppy disks.²⁹

Notably, adherence to the above recommendations would have offered each of the parties in Metropolitan Opera, Sheppard, and Danis a far better argument to avoid sanctions for their conduct of digital discovery.

5. Conclusion.

The information age has created a host of new risks for the lawyer and the professional client conducting discovery. Courts have become less hesitant in imposing sanctions against parties and their attorneys, who have scorned these risks by failing to educate themselves as to digital discovery. The risks of digital discovery, however, can be lessened by the careful attention to the client’s computer system and the restructuring of its existing document policies.

Lee H. Ayres

COOK, YANCEY, KING & GALLOWAY
333 Texas Street, Suite 1700
Shreveport, LA 71101
Telephone: (318) 221-6277
Facsimile: (318) 227-7850
E-Mail: ayres@cykg.com
Web: www.cykg.com

ENDNOTES

1. The Sedona Conference, The Second Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 3-5, at <http://www.thesedonaconference.org/miscFiles/SedonaPrinciples200401>.
2. Whitney Adams, A Guide Through the Minefield of Electronic Discovery for the Experienced Trial Lawyer, 2, at http://www.crickettechnologies.com/case_studies/crickettechnologiesarticle.pdf.
3. Michael P. Zweig and Mark J. Goldberg, “Electronic Discovery: A Brave New World,” *WALL STREET LAWYER* (2003).
4. See China Ocean Shipping Co. v. Simone Metals, Inc., 1999 WL 966443 (N.D. Ill. Sept. 30, 1999).
5. 7 MOORE’S FEDERAL PRACTICE § 37.120 (3d ed. 1999).
6. In re Agent Orange Prod. Liability Litig., 506 F. Supp. 750 (E.D.N.Y. 1980).
7. Fed. R. Civ. Proc. 26(b).
8. See, e.g., Lewis v. United Air Lines Transp. Corp., 27 F. Supp. 946 (D. Conn. 1939).
9. The Advisory Comments to Rule 26(g) emphasize that lawyers have an affirmative duty to engage in pretrial discovery responsibly and encourage sanctions for abuse; and, Rule 37 encourages additional sanctions for parties that abuse the discovery process. The courts’ inherent powers to manage their own affairs have been recognized as grounds for the imposition of sanctions. See, e.g., Residential Funding Corp. v. DeGeorge Fin. Corp., 306 F.3d 99, 106 (2d Cir. 2002). (“Whether exercising its inherent power, or acting pursuant to Rule 37, a district court has wide discretion in sanctioning a party for discovery abuses.”).
10. 212 F.R.D. 178 (S.D.N.Y. 2003).
11. Id. at 222.
12. 203 F.R.D. 56 (D.N.H. 2001).
13. Id.
14. 53 Fed. R. Serv. 3d 828 (N.D. Ill. 2000).
15. Id. at *2.

16. Id. at *11.
17. Id.
18. Id. at *11-12.
19. Id. at *32, quoting In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 615 (D.N.J. 1997).
20. Adam Cohen & David Lender, *ELECTRONIC DISCOVERY: LAW AND PRACTICE* (2004); Zweig and Goldberg, “Electronic Discovery: A Brave New World”; D. Chad McCoy, “Emerging Technology Creates New Legal Risks for Clients,” *E-BUSINESS LAW BULLETIN* (June 2003).
21. Cohen & Lender, *ELECTRONIC DISCOVERY: LAW AND PRACTICE*, § 1-67; Zweig and Goldberg, “Electronic Discovery: A Brave New World.”
22. Cohen & Lender, *ELECTRONIC DISCOVERY: LAW AND PRACTICE*, § 1-10.
23. Zubulake v. UBS Warburg, LLC, 217 F.R.D. 309, 318-20 (S.D.N.Y. 2003).
24. Id.
25. Id.
26. Id.
27. Carey Meyer & Kari Wraspir, “E-Discovery: Preparing Clients for (and Protecting them Against) Discovery in the Electronic Information Age,” 26 *WM. MITCHELL L. REV.* 939 (2000).
28. Cohen & Lender, *ELECTRONIC DISCOVERY: LAW AND PRACTICE*, 1-10.
29. Id.