

New Jersey Law Journal

VOL. CLXXII – NO. 4 – INDEX 309

APRIL 28, 2003

ESTABLISHED 1878

Complex Litigation

Discovery, Retention and Spoliation of E-evidence

Embedded data is not seen or heard, but it's there. And deleted data is often retrievable

By David M. Kohane

It has been estimated that the daily number of e-mails sent now exceeds 10 billion. It has also been estimated that at least one-third of all electronic data is never printed. With statistics like these, lawyers cannot afford to ignore electronically stored data as a potential source of evidence.

It is important to know the differences between electronic evidence and paper documentary evidence. It is also critical to understand how the discovery rules have been applied to electronic evidence and issues that can arise in the retention and spoliation of such evidence.

More Than Meets the Eye

Electronic data exists in many forms — some obvious and familiar, some not-so-obvious. Most computer users work with so-called active data, consisting of files created by familiar applications like WordPerfect, Word, Excel and the like. This data is organized and stored so as to be easily retrieved, processed and printed.

Computers also store data in less visible or accessible ways. Word processing programs, for example, may let users insert comments that show on the screen but that

The author is a partner in the litigation department at Cole Schotz Meisel Forman & Leonard of Hackensack.

are not normally printed. Programs often store data about the data, known as “meta-data” or “embedded data,” that reflects who accessed or edited the file at a particular time and what changes were made.

Internet usage can create a trail of Web sites the user visited. “Cookies” are data a Web server stores on the user’s hard drive that the Web server can retrieve to identify the user (and sometimes other information) when the user returns to the Web site. “Caches” are storage areas on a user’s disc that hold recently accessed information. Their function is to shorten the time to reload the image, but they can leave an imprint of the user’s Internet usage on the hard drive.

Many computer software products and systems automatically backup data at pre-programmed intervals. This data, known as archival data, file clones or replicant data, is created to avoid inadvertent data loss due to power outages, system freezes and the like.

Because the computer automatically backs up the data periodically, many versions of a particular document may be available without the user even knowing they exist.

It is now common knowledge that deleted data may be retrievable. When a computer deletes a file, it marks the file as available storage space — but the space may not actually be overwritten for some time, and fragments may remain even while other portions are overwritten. This residual data can often be retrieved.

E-mail deserves separate mention. E-mails are generally stored in database files — essentially buckets of data — rather than individual files, which makes the process of

retrieving e-mails somewhat different from individually saved files, and which may make the recovery of deleted e-mails more difficult.

Finally, many businesses back up data to magnetic tapes or offsite locations. Generally these backup files consist of snapshots of the entire system and are designed to be uploaded in their entirety in the event of system failure.

Electronic documents can also be stored in a variety of places. The most obvious is users’ and network hard drives. Electronic evidence may also be stored, however, on laptops, employees’ home computers (for employees who sometimes or always work at home), diskettes, backup magnetic tapes and the like.

At least as important as these technical differences between paper and electronic evidence are the different ways people treat electronic evidence — especially e-mails.

Users tend to use e-mails as an informal form of communication and “say” things they would never put on paper. The ease by which e-mails can be disseminated to third parties, furthermore, is both part of their value and part of their danger, as control over who has copies is lost.

The informality with which e-mails are composed often is mirrored in the haphazard way they are stored. Many large organizations that would never think of leaving to each employee how and when to store paper documents have no e-mail filing system.

Finally, the nature of computerized information and its storage can create special confidentiality and privilege concerns. One level of concern is that privileged electronic data and documents may be inter-

mingled with other documents.

In addition, a proprietary computer system or application may pose particular challenges in cases where the discovery might lead an adversary to seek access to a litigant's computer to search, for example, for replicant, residual or embedded data. See "Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?" 41 B.C. L. Rev. 327 (2000).

Discovery of Electronic Evidence

It is firmly established that electronic evidence is discoverable, subject to the same rules as other evidence. Rule 34 of the Federal Rules of Civil Procedure was amended in 1970 to include "data compilations" in the definition of "documents" subject to production, and New Jersey Court Rule 4:18 was modeled after that rule.

Initial mandatory disclosures under Rule 26(a) of the Federal Rules must, according to the 1993 Advisory Committee notes, disclose "computerized data and other electronically-recorded information." See *Kleiner v. Burns*, 48 Fed. R. Serv. 3d 644, 2000 WL 1909470 (D. Kan. 2000).

Both the federal and state rules grant the courts discretion to limit and condition disclosure demands and protect parties from "undue burden or expense." The federal rules explicitly authorize the court to weigh the likely burden or expense of the proposed discovery against its likely benefits. See Fed. R. Civ. P. 26(b).

Drawing on paper discovery precedents, the courts have found ample discretion in the rules to address electronic discovery issues, but not always sufficient guidance. Three principal questions are now at the forefront: (1) must electronic copies be produced in addition to paper copies? (2) who pays for the retrieval of hard-to-retrieve electronic evidence? and (3) how can the privilege be effectively protected in a large production of e-documents?

Electronic Plus Paper Production?

The time-honored document demand formulation seeks "any and all documents" relating to a particular matter. The typical request involves a lengthy definition of "document" that inevitably includes drafts and all nonidentical copies of a document.

Consider the implications of these formulations for electronic document discovery. A computer or network may have multiple versions of a document saved to disk. Embedded metadata showing who accessed a document when, or what additions and deletions were made, may make these versions separate documents subject to production.

Hard drives may contain residual data from deleted documents and replicant data automatically saved by the computer. A business' backup magnetic tapes may also contain responsive documents. In short, many more versions of a document may exist in electronic form than exist in paper, some of which the author may not even know about.

Good reason often exists for requiring production of documents in electronic as well as paper form. In addition to the fact that electronic versions of documents may contain information paper versions lack and may survive the discarding of the paper documents, computerized information is often more useful to the receiving party than paper documents. That is especially true in complex cases requiring analysis of large quantities of data.

For these reasons, courts often require production of electronic versions of information, even if paper copies of the same documents are available.

In *United States v. Davey*, 543 F.2d 996 (2d Cir. 1976), the Second U.S. Circuit Court of Appeals enforced an Internal Revenue Service summons for tapes containing financial information, even though defendant offered to produce the same information in paper form. The court held the taxpayer could not "give the IRS requested information in an inconvenient form with a view to immunizing itself from demands for other records containing the same relevant information in a more convenient form."

Similarly, in the antitrust case *National Union Electric Corp. v. Matsushita Elec. Indus. Co.*, 494 F. Supp. 1257 (E.D. Pa. 1980), after the plaintiff produced a printout of a large quantity of sales and production data, the court enforced the defendants' request that the same data be produced in electronic form. The court cited the 1970 Advisory Committee notes, which state that the responding party "may be required to use his devices to translate the data into usable

form."

The court concluded with an admonition to construe the federal rules to "secure the just, speedy and inexpensive determination of every action."

More recent case law has also tended to favor production in electronic form. In another antitrust case, *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 94 Civ. 2120, 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995), the court held:

[T]he rule is clear: production of information in 'hard copy' documentary form does not preclude a party from receiving that same information in computerized/electronic form.

The court also held that the producing party can be required to design a computer program to extract the data from its computerized business records, subject to the Court's discretion as to the allocation of the costs of designing such a computer program.

It bears emphasizing that trial courts have discretion over these issues. In *Williams v. Owens-Illinois Inc.*, 665 F.2d 918 (9th Cir. 1982), for example, the Ninth Circuit held that "while it is true that computer tapes are not per se non-discoverable," the district court did not abuse its discretion in refusing to order turnover of computer tapes where hard copies of the same information was produced.

Who Pays?

In the business litigation context — where the bottom line is money — who pays is the bottom line. The courts recognize that allocation of discovery costs can shift the playing field and skew settlement negotiations. The general rule, developed in the paper discovery era, is that the responding party presumptively bears the cost of retrieval and review for responsiveness and privilege and the requesting party pays copying costs.

This approach translates imperfectly into the electronic evidence context. The variety of ways electronic evidence is stored, the volume of electronic evidence, and the ease or difficulty of searching for responsive information and weeding out privileged material all conspire to drive up the cost of retrieval, review and production.

In resolving cost-allocation disputes, some courts have emphasized the custom-

ary rule that the producing party pays. Other decisions emphasize differences between paper and electronic records and have adopted balancing tests to resolve these issues.

A leading case representing the former view is *Brand Name Prescription Drugs Antitrust Litig.*, No. 94 C 897, MDL 997, 1995 WL 360526 (N.D. Ill. June 15, 1995). In that antitrust case, the court ordered CIBA-Geigy Corporation to retrieve, compile, format and search at least 30 million pages of e-data for responsive information — at an estimated cost of \$50,000 to \$70,000. The court reasoned, “if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk” over which the requesting party has no control.

Two recent cases have questioned this approach. In *McPeck v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), a Justice Department employee suing for retaliation on a sexual harassment claim sought backup tapes for the department computer system to search for deleted word processing files and e-mails of the persons he alleged retaliated. The tapes at issue were used only for disaster avoidance (system crashes), not as archives, and were retained haphazardly.

The court began by noting that it is “impossible to know in advance what is on these backup tapes.” The court held that restoring all backup tapes is not required in every case and rejected the proposition, relied on in *Brand Name Prescription Drugs*, that production of backup tapes is a “cost of doing business in the computer age.” Businesses have no choice but to computerize and to back up their data periodically. “What alternative is there?” the court asked. “Quill pens?”

The court’s solution invoked “the economic principle of ‘marginal utility.’” The court stated that “[T]he more likely it is that the backup tape contains information that is relevant to a claim or defense, the fairer it is that the government agency search at its own expense. The less likely it is, the more unjust it would be to make the agency search at its own expense.” The court went on to hold that the likelihood of finding the “needle in the haystack” should not be the only criteria. The court also cited the magnitude of the cost as a proper consideration, so as to avoid giving the requesting party “a

gigantic club with which to beat his opponent into settlement.”

The court ordered a test run — restoration of a small portion of the tapes to see what might be found to test the evidentiary value of backup tapes’ contents. The court deferred decision on who would pay the cost of the test run. (Predictably, the recently-issued sequel to *McPeck*, 212 F.R.D. 33 (D.D.C. 2003), reports complete disagreement between the parties on what the test run showed. In *McPeck II*, the court ultimately ordered that plaintiffs’ requests be substantially narrowed, but no resolution of the cost allocation issue is reported.)

In *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002), black concert promoters alleged that other promoters and booking agencies unlawfully discriminated and committed antitrust violations by colluding to freeze them out of promotion of white bands. The plaintiff sought documents concerning the selection of concert promoters and the bidding processes relating to concert promotions.

The court noted that “the burden to each defendant depends upon the specific structure of its e-mail retention and on the related means for retrieving and producing responsive e-mails.” The court questioned the line of cases, represented by *Brand Name Prescription Drug* and others, that presumed that the producing party should bear the cost because that party chose the storage method. The court noted that while paper records are generally retained because they are expected to be useful, electronic data may be retained simply because the cost of retaining it is so small.

Then, like the court in *McPeck*, the court noted that backup data, unlike paper records, are often created not as accessible archives, but “for wholesale, emergency uploading onto a computer system,” so “the organization of the data mirrors the computer’s structure, not the human records management structure.” (quoting “Computer-Based Discovery in Federal Civil Litigation,” SF97 ALI-ABA 1079, 1085 (2001)).

For these reasons, the court concluded, it “is not enough to say that because a party retained electronic information, it should necessarily bear the cost of producing it.”

The *Rowe* court adopted an eight-factor balancing test to determine whether the cost of discovery should be shifted to the

requesting party: (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data; (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party.

Applying these factors, the court shifted the cost of production to the plaintiffs, with the cost of review for privileged or confidential material remaining with the defendants.

Protecting Attorney-Client Privilege And Work-Product Immunity

Production of computerized records often entails delivery of large quantities of data to an adversary. In traditional document production, the producing party’s counsel reviews the responsive documents for privileged items.

When electronic storage of documents is at issue, however, entire hard drives or storage tapes containing disparate and unrelated information may be reviewed or downloaded for search, retrieval and even reconstruction so a complete review of these documents for privilege may be time consuming and inefficient. The courts and counsel have sought creative approaches to protecting the privilege.

One approach is to have the requesting party’s counsel review all retrieved e-mails for responsiveness and then have the responding party’s counsel review the selected items for privilege, stipulating that the disclosure of potentially privileged documents to the requesting party would not constitute a waiver of the privilege.

The *Rowe* court took that approach, which places the burden of initially reviewing large quantities of documents on the requesting party. The court had an expert create “mirror images” of the hard drives and backup tapes at issue, retrieve the e-mails and present them to plaintiff’s counsel on an “attorneys eyes only” basis for review, after which defendants’ counsel would review the selected documents for privilege.

The requesting party was required to bear the cost of this procedure — except

that the responding party was given the option of conducting the privilege review before the documents were culled for responsiveness at their own expense.

The court in *Playboy Enterprises, Inc. v. Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999), implemented a similar procedure but had the producing party conduct the initial privilege review.

To retrieve deleted e-mails from defendant's hard drive while protecting the privilege, the court had a court-appointed expert create a mirror image of the defendant's hard drive. Defendant's counsel would then print and review any recovered documents and produce any nonprivileged, responsive documents and a privilege log. Without detailed analysis, the court ordered the requesting party (the plaintiff) to pay the cost of the electronic information recovery.

Preservation and Spoliation of Electronic Evidence

The differences between paper and electronic data also require special attention to another issue — preservation and spoliation. The Enron/Arthur Anderson debate has put spoliation issues under a spotlight. The truth, however, is that inadvertent spoliation of electronic evidence may be a larger problem than willful destruction.

Because even negligent destruction of evidence can lead to adverse consequences, lawyers are well-advised to work with clients in forming document retention policies and, when disputes arise, in preserving potentially probative and discoverable evidence.

Leaving aside criminal conduct, case law has made it clear that the parties have an obligation to retain documents "relevant to pending, imminent or reasonably foreseeable litigation." See *Shamis v. Ambassador Factors Corp.*, 34 F. Supp. 2d 879 (S.D. N.Y. 1999). This duty may require affirmative action; even a company's blindness to document destruction may result in sanctions.

Sanctions for failure to preserve evidence, both willful and negligent, can be imposed under the discovery rules and the court's inherent powers, and range from monetary sanctions to adverse inference instructions to dismissal/default. The courts tailor the severity of the sanctions to the

gravity of the offense and the prejudice to the other party.

Perhaps the best-known sanction for spoliation of relevant documents is an adverse inference or similar species of instruction to the jury. As the New Jersey Supreme Court stated in *Rosenblit v. Zimmerman*, 166 N.J. 391 (2001), when a litigant hides or destroys relevant evidence, a presumption may be made that "the evidence the spoliator destroyed or otherwise concealed would have been unfavorable to him or her."

Both adverse inferences and monetary sanctions were brought to bear in *In re Prudential Ins. Co. of Am. Sales Practices Litig.*, 169 F.R.D. 598 (D.N.J. 1997). In that class action alleging deceptive insurance sales schemes, the court had ordered that all parties "preserve all documents and other records containing information potentially relevant to the subject matter of this litigation." Although there was no evidence of willful destruction at the management level, individuals at some field offices were found to be destroying documents.

The court found that management failed to disseminate the preservation order or take other steps to encourage preservation of relevant documents. The court noted that "[W]hile there is no proof that Prudential, through its employees, engaged in conduct intended to thwart discovery through the purposeful destruction of documents, its haphazard and uncoordinated approach to document retention indisputably denies its party opponents potential evidence to establish facts in dispute."

The court emphasized that senior management could not blame the field offices for the failure of preservation. "The obligation to preserve documents that are potentially discoverable materials," the court held, "is an affirmative one that rests squarely on the shoulders of senior corporate officers."

The bar and its clients should note the sanctions for the company's negligent failure to comply with the preservation order. As for permanently lost records, the court drew an adverse inference that the materials were relevant and would establish liability. The court then ordered Prudential to disseminate the preservation order immediately, to propose a written document preservation policy, to establish a hotline to facilitate document destruction reports and a certification process for field managers

— and to pay a \$1 million fine.

Spoliation concerns can be especially thorny in the electronic evidence context. Recall that archival, residual and backup data may be stored without the user's knowledge on a hard drive or backup tapes — and may also be erased, overwritten or destroyed without the user's knowledge in the ordinary course of business or the ordinary course of the computer's operations. Must a litigant, or potential litigant, take extraordinary steps to preserve such evidence whenever a dispute is brewing?

There is a dearth of authority to date on whether sanctionable spoliation occurs absent such steps. The courts have, however, begun to address this problem in case-by-case preservation orders.

In *In re Mercedes-Benz Anti-Trust Litigation*, No. 99-4311 (D.N.J.), the court ordered preservation of potentially relevant evidence but struck the balance in favor of continuing normal business operations, with a proviso: "Subject to further Order of the Court, parties may continue routine erasures of computerized data pursuant to existing programs, but they shall immediately notify opposing counsel about such programs, and preserve any printouts of such data." (Feb. 16, 2001 Order). A Southern District of New York case took a similar approach in *In re Rezulin Products Liability Litigation*, 2000 WL 1530005 (S.D.N.Y. Oct. 16, 2000).

Other courts have struck a different balance and required automatic deletions to be suspended. In *In re: Propulsid Products Liability Litigation*, MDL No. 1355 (E.D. La.), the court entered an order suspending automatic deletion of discoverable information and requiring the defendant to secure any hard drives that might contain relevant information or create mirror images thereof; to preserve all electronic archival material; and to retain current or legacy software or hardware needed to process active or backup data.

In cases of any complexity or that may otherwise involve computerized evidence, lawyers must now plan electronic discovery at least as carefully as traditional paper discovery. The variety of potential sources and locations for electronic evidence, the frequency with which electronic evidence is automatically destroyed, and the potential expense and time sometimes involved in retrieving, reconstructing and reviewing electronic evidence all require early plan-

ning.

Communicate with the client and adversary early — perhaps before a lawsuit begins — about electronic evidence issues. Preservation issues should be at the top of that list, since probative evidence can be destroyed without human intervention. A court is much more likely to be forgiving of an inadvertent destruction of electronic evidence resulting from an ongoing, consistently applied document retention policy than a haphazard policy that is left to employees' discretion — or worse, is adopted after a dispute erupts.

Focus discovery demands on computer evidence issues. Ask for computerized evidence specifically and explore with appropriate witnesses, including your client's and the adversary's personnel, what computerized evidence may exist. Unless your pre-law degree was in computer science, expert advice may be needed to help navigate discovery.

Be Careful What You Ask For

You improve your chances of avoiding substantial costs of retrieving an adversary's electronic data if you can persuade the court that your discovery requests are narrowly tailored to uncovering evidence likely to be found in computerized form. It is always tempting to leave no stone unturned, but if you press such a request, you're more likely to find your client paying the costs of turning the stones.

And don't forget the rules of evidence.

The usual hearsay and authentication rules apply to electronic evidence. As proponent of an e-mail, make sure you can establish that it is what it purports to be.

A New Jersey district court case, *In re Bristol-Myers Squibb Securities Litigation*, 205 F.R.D. 437 (D.N.J. 2002), holds a final lesson for anyone practicing complex litigation.

In that class action suit, the defendants estimated that the response to the plaintiffs' document demand would comprise 500,000 copies, and the plaintiffs agreed to pay 10 cents per page for copies of the entire production.

The production actually amounted to 3 million pages of documents in paper form, and the plaintiffs cried foul. Then the plaintiffs learned that the defendants had made the production by "blowing back" the documents — scanning them into computer disc while printing them in paper form.

The defendants agreed to the plaintiffs' request to produce the computerized information, but only if the plaintiffs paid half the cost of scanning in addition to the cost of paper reproduction.

The court rejected the plaintiffs' contention that the defendants had dumped documents to drive up their copying costs, but also took the defendants to task for failing to disclose in initial disclosures that some of the documents were already computerized, and reduced the plaintiffs' copying bill accordingly.

Also, the court rejected what it viewed as the defendants' effort at a double-recovery — to collect for paper copying and for duplicating the electronic files — and required the plaintiffs to pay only the cost of replicating the diskettes plus the hard copies.

Finally, referring to the requirement under Rule 26 of the Federal Rules of Civil Procedure to meet and confer to develop a proposed discovery plan at the beginning of the case, the court closed with this sage advice:

In the electronic age, this *meet and confer* [original emphasis] should include a discussion on whether each side possesses information in electronic form, whether they intend to produce such material, whether each other's software is compatible, whether there exists any privilege issue requiring redaction, and how to allocate costs involved with each of the foregoing.

As the eve of electronic case filing (ECF) is upon us, in this and most other Districts, the production of electronic information should be at the forefront of any discussion of issues involving discovery and trial, including the fair and economical allocation of costs.

That is a message all practitioners should heed. ■