

# Electronic Discovery Disputes: Decisional Guidance

Kenneth J. Withers, Senior Judicial Education Attorney, Federal Judicial Center, Washington D.C.

*The opinions expressed in this article are those of the author and do not necessarily represent those of the Federal Judicial Center or any other agency of the United States Courts.*

Civil discovery is one area of law in which the digital revolution is felt keenly, and “electronic discovery” presents some significant challenges for judicial management. As lawyers grapple with new concepts and technologies, their missteps and miscommunications end up in front of judges as arcane and intractable discovery disputes. Some of these problems are just the old problems dressed up in 21st-century garb—the scope of discovery, protective orders, privilege, and spoliation. But many are unique to electronic discovery. To avoid these problems, courts need to apply a greater degree of pressure to counsel to communicate and cooperate in developing a discovery plan. But if those efforts fail, courts need to understand new concepts and new terminology to reach a fair and equitable result.

The federal courts have seen the problems of electronic discovery coalesce into a pattern of more-or-less predictable discovery disputes that can be grouped into some broad categories roughly following the chronology of the typical case.

## Electronic Data Preservation

At the outset of the litigation, one party or the other requests that the court issue a broad data preservation order, calling on the responding party to immediately halt all operations that can result in the destruction or alteration of computer data, including e-mail, word processing, databases, and financial information. The party requesting the data preservation order is expressing a real concern for the integrity of the truth-seeking process, since few opposing counsel are fully aware of their client’s routine computer operations and the potential for inadvertent (or intentional) destruction of relevant evidence. But a broad, blanket protective order can effectively unplug a computer network and put a computer-dependent company out of business. Twenty years ago, a document preservation order might inconvenience the back office of a company, but the assembly line and sales operation continued. In the information economy, the computer system functions not only as the back office, but also as the assembly line and sales operation.

If the court feels that any preservation order is necessary at all (which the requesting party bears the burden to demonstrate), the solution is a narrowly tailored data preservation order instructing the parties to take reasonable steps to preserve relevant data. The court is not in a position to draft the details of the order, and the requesting party seldom is, making *ex parte* orders a predictable prelude to disaster. Both parties must be involved. Only the requesting party can state, with particularity, what the scope of discovery will be, and only the responding party can state, with particularity, the nature of its data collection and its ability to preserve the relevant data. The court should use this opportunity to order the parties to meet and confer to develop a discovery plan, the first step of which is a mutually agreeable data preservation regimen. Until they meet and confer, the parties should be reminded of their ethical and legal obligations,

and the inherent authority of the court. See, e.g., *Prempro Product Liability MDL*, E.D. Ark No. 4:03-CV-1507 (Order dated November 17, 2003), available at <http://www.ark.uscourts.gov/mdl/index.cfm>; see also *Manual for Complex Litigation* (4th ed.), Sample Form 40.25 (Federal Judicial Center, 2004).

## Scope of Electronic Discovery

In all discovery, paper or electronic, the key to good management is narrowly defining the scope of discovery. Most good attorneys know this, but the prospect of electronic discovery is like a vision of a candy factory, and the legal press is full of articles and full-page advertisements for electronic discovery consultants telling attorneys to grab all they can get—all the e-mails, all the backup tapes, all the hard drives and laptops.

While the scope of discovery is not limited by media, it still must be defined by relevance to the subject matter of the dispute. The problem of scope becomes most apparent when the requesting party wants direct access to the responding party’s computer systems for the purpose of forensic analysis. Just because it is possible to recover deleted electronic files or residual data, that does not necessarily make deleted files or residual data relevant to the subject matter of the dispute. The requesting party must make some threshold showing that the request is, at the very least, reasonably calculated to lead to the discovery of admissible evidence. See, e.g., *Betha v. Comcast*, 218 F.R.D. 328 (D.D.C. 2003).

The flip side of the scope of discovery—defined by relevance to the matters in dispute—are limitations on the scope of discovery where the costs and burdens imposed on the responding party are undue. The Federal Rules of Civil Procedure and most state rules explicitly recognize logistical limits on scope. But some costs or business disruptions are to be expected in all litigation and are not the “undue burdens” that justify narrowing the scope, shifting costs, entering a protective order, or disallowing the requested discovery altogether.

In several recent cases, the distinction between a mere burden associated with litigation and an “undue” burden has been the accessibility of the requested data. See, e.g., *Zubulake v. UBS Warburg LLC* (“*Zubulake I*”), 217 F.R.D. 309 (S.D.N.Y. 2003) (Opinion and Order dated May 13, 2003). If the data requested are accessible to the responding party in the ordinary course of that party’s business or activities, cost shifting or other restrictions are probably not justified. However, if the requested data are inaccessible, discovery may be restricted. Examples of inaccessible data may include backup tapes (which are notoriously cumbersome and expensive to restore), data which have been deleted in the ordinary course of business, and “legacy data,” that is, data from outdated computers or in outdated formats that can no longer, or not without great expense, be restored and used.

To resolve misunderstandings and avoid disputes over scope, burdens, and costs, the parties should meet and confer early in

the case. Inviting the respective parties' technical people to the meet-and-confer session (perhaps under the cloak of an appropriate protective order, so the conference does not become a surprise deposition) can often eliminate the confusion and speed the process of developing a realistic discovery plan.

Several courts have adopted this approach as a local rule or standing order at the start of all civil litigation. See, e.g., United States District Court for the District of New Jersey, Local Rule 26.1, at <http://pacer.njd.uscourts.gov/njdc/rules/Rules-10-6-03.pdf>; see also United States District Court for the District of Kansas, Electronic Discovery Guidelines, at <http://pacer.njd.uscourts.gov/njdc/rules/Rules-10-6-03.pdf>.

### Cost Shifting in Electronic Discovery

When the parties cannot agree on limitations on the scope of discovery because of undue costs and burdens, one common mechanism for resolving the dispute is for the court to order that the proposed discovery go forward, conditioned on the requesting party assuming the additional discovery costs. This is a departure from the usual rule that parties pay their own costs in discovery. The court in *Zubulake* emphasized that a court can only do this if it finds that the burden on the responding party is "undue," i.e., that the data requested are inaccessible in the ordinary course of the responding party's activities. Once that threshold is met, the court can consider cost shifting, but must also consider other factors. Modifying a test from another recent federal case, *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421 (S.D.N.Y. 2002), the court in *Zubulake* formulated seven factors, in order of weight:

1. The extent to which the request is tailored to discover relevant data
2. The availability of those data from other sources
3. The total cost of production, relative to the amount in controversy
4. The total cost of production, relative to the resources available to each party
5. The relative ability and incentive for each party to control its own costs
6. The importance of the issues at stake in the litigation
7. The relative benefits to the parties in obtaining those data

### Privilege and Privilege Waiver

During discovery, a huge volume of electronic data will need to be reviewed for privilege, work product protection, trade secret, or other confidentiality considerations. To some extent, technology can ease the burden by helping counsel identify particular authors, recipients, or terms. But in the end, attorneys will need to manually review tens of thousands (if not millions) of e-mail messages, word-processing documents, and other files to make privilege determinations. Errors are inevitable. The inadvertent production of privileged information can carry enormous consequences, and usually both sides realize this. Before discovery starts, the parties can meet and confer on a mutually agreeable protocol for handling privilege claims and disputes.

These agreements can take two forms. One is the "call back" agreement, under which both parties agree that inadvertent pro-

duction of privileged information does not immediately constitute a waiver of privilege. If the producing party realizes its error within a reasonable time and requests return of the document or information, the receiving party must comply, but may challenge the privilege designation later. Likewise, if a receiving party identifies an obviously privileged item in the production, it has a duty to notify the other side and either return the item or tender it to the court for resolution of the privilege waiver question, if there is one.

The other form of agreement requires an even higher level of mutual trust and respect between counsel. It is called the "quick peek" approach and has the added benefit of reducing the overall scope and cost of discovery. Under the "quick peek" agreement, counsel are allowed to see each other's entire data collection before production and designate those items that they believe are responsive to the discovery requests. The producing party then reviews the presumably much smaller universe of files for privilege, and produces those that are responsive and not privileged, along with a privilege log. Such an arrangement usually requires a court order—the entire arrangement can be viewed as "privilege waiver" by third parties or in subsequent litigation, and a court order may serve to protect the privilege. However, a court is ill advised to unilaterally impose the "quick peek" approach on the parties, no matter how speedy and cost-effective it may be, because the arrangement requires such a high level of trust and cooperation between opposing counsel.

When the parties cannot agree on a privilege protection protocol, particularly when discovery involves the production of a computer itself and review of all the files on the computer's hard drive, many courts have resorted to the use of a neutral expert. In some cases, the neutral expert may be a Special Master under Fed. R. Civ. P. 53 or Fed. R. of Evid. 706. But if the parties and the court can agree on a neutral, and the neutral's role is objective or mechanical instead of adjudicatory, the neutral does not need to be appointed or supervised by the court. See, e.g., *Medtronic Sofamor Danek, Inc. v. Michelson*, 56 Fed. R. Serv. 3d 1159 (W.D. Tenn. 2003).

These "neutral expert" protocols, many of which are based on the order entered in *Playboy Enterprises, Inc. v. Terri Welles*, 60 F. Supp. 2d 1050 (S.D. Cal. 1999), generally involve the following steps:

- (a) The neutral creates a "bitstream" or "mirror" copy of the computer hard drive, thereby preserving the integrity of the original.
- (b) Using computer forensics tools, the expert reviews the copy, restoring any deleted documents and recovering any residual data or fragments.
- (c) Using electronic discovery tools, the expert searches the files for those that fit preestablished criteria, such as those containing key words; those created, accessed or edited within key date ranges; those authored or received by key figures; or those bearing some other objective relationship to the issues in dispute.
- (d) The expert assembles the "responsive" files into a database or prints them out for the responding party's attorney, who reviews them for responsiveness to the specific discovery requests and for privilege.

**Electronic Discovery Disputes: Decisional Guidance, continued from page 5**

- (e) The resulting responsive and nonprivileged files are then produced for the requesting party.
- (f) If the parties cannot agree on the objective criteria for the expert to use to determine “responsiveness,” the court can order a protocol after consultation with the expert.

**Form of Production**

In conventional discovery, the form of production was seldom disputed. Paper was paper, and the parties produced paper. In electronic discovery, there are many choices of form for production. At one extreme, a party could produce hard-copy printouts of all the electronic files, but that would essentially hide the meta-data, embedded edits, and other nonapparent information. It would also be voluminous and cumbersome to handle, adding significant costs and delays to the discovery process. It may even be considered sharp practice. See, e.g., *In re Bristol-Myers Squibb Securities Litig.*, 205 F.R.D. 437 (D.N.J. 2002). At the other extreme, a party could produce all data in “native format,” streams of digital electrons on disks or tapes exactly as they might be found on the producing party’s computer, but without the word-processing, e-mail, or database software needed to make sense of them, and without any ability to organize and present the information in a coherent form.

The current standard in large-scale electronic discovery is to render most of the electronic files as electronic images, much as they would look on a screen or in paper form (i.e., “tif” or “pdf” images). These combine the advantages of electronic form (portability, ease of manipulation) and paper (ability to number pages, read, and print). However, some computer data cannot easily be rendered in paper or image form, nor can they be effectively produced in “native” format. Large-scale, enterprise-wide databases can only render relevant, nonprivileged information when they are “queried” using database software and a report is generated, which is a document or computer file created solely for the purposes of discovery, analogous to an interrogatory answer.

Most disputes over the form of production stem from a failure to communicate at the start of discovery what the requesting party wants and what the producing party can or intends to do. The requesting party receives paper or electronic files, and then discovers that for one reason or another, the form is inadequate or useless. The parties will then go to the court with cross-motions, one to compel production a second time in a more appropriate form, and one for a protective order preventing a second duplicative production. See, *McNally Tunneling Corp. v.*

*City of Evanston*, 2001 WL 1568879 (N.D. Ill. Dec. 10, 2001) (rejecting the motion to compel supplemental discovery in electronic form); cf. *In re Honeywell Int’l, Inc. Securities Litig.*, 2003 WL 22722961 (S.D.N.Y. Nov. 18, 2003).

**Electronic Spoliation**

The duty to preserve potentially relevant evidence depends on a number of factors, not all of which are obvious to the actors. It arises when litigation is reasonably anticipated, and encompasses documents and data that a reasonable person would know, at the time of destruction, to be relevant to the subject matter of the dispute. The duty, therefore, can attach to different data at different times. See, e.g., *Stevenson v. Union Pacific R. Co.*, 354 F.3d 739 (8th Cir. 2004). In a large organization, where the computer functions are decentralized and the daily computer operations are a mystery to the users, mistakes will occur. And the last person one can expect will have any knowledge of—let alone control over—the computer operations is outside litigation counsel. Therefore, most “spoliation” is the result of negligence or ignorance, rather than malicious acts to destroy evidence.

Then why is this called “spoliation,” which implies intent, and why are sanctions sometimes imposed, which demand findings of gross negligence or an otherwise culpable state of mind? Because in most of these cases, the loss of data is compounded by counsel’s failure to communicate the facts to opposing counsel and the court, or because counsel misrepresents the facts to the court, attempts to cover up for its failure, or engages in “purposeful sluggishness” (see, e.g., *Residential Funding v. DeGeorge*, 306 F.3d 99 (2d Cir. 2002)) in the hope that the problem will go away. The destruction of potential evidence might be due to negligence, but the subsequent cover-up is judged to be willful and grounds for severe sanctions.

**Conclusion**

Far from being a drain on judicial resources, the sort of hands-on judicial management that has been proposed in this article reduces the number of discovery disputes that end up before the judge, speeds settlement for those cases that settle, and speeds trial for those cases that get tried. Meanwhile, a body of caselaw is developing to address electronic discovery disputes as they arise. However, we are “living in interesting times,” as the ancient curse foretold, and everyone—judges, counsel, and parties—occasionally finds themselves on uncharted waters in the sea of electronic discovery.

# Is Digital Different?

*In litigation involving the breakup of a medical practice, one party requests access to the other's hard drive. The hard drive in question also contains confidential patient records.*

*A national company accuses an employee's union of organizing a "sick-out," and requests access to the hard drives of defendants' home PCs.*

Today, most documents are in digital form. "Electronic (or digital) documents" refers to any information created, stored, or best used with computer technology of any sort, including business applications, such as word processing, databases, and spreadsheets; Internet applications, such as e-mail; devices attached to or peripheral to computers, such as printers, fax machines, pagers, and wireless telephones; and media used to store computer data, such as disks, tapes, CDs, and the like.

According to a study by the University of California at Berkeley, 93 percent of all information created in 1999 was generated in digital form. There are significant differences, however, between conventional documents and electronic documents.

## Differences in Degree

The volume, number of locations, and data volatility of electronic documents are significantly greater than that of conventional documents. One paper document originating from a corporate computer network and shared with other employees who commented on it may result in well over 1,000 copies or versions of that document in the system. A small company with 100 employees sending or receiving the industry average of 25 e-mail messages a day produces 625,000 e-mail messages a year, generally unorganized and full of embarrassing, inappropriate, and irrelevant comments. Document search locations include not only computer hard drives, but also network servers, backup tapes, and e-mail servers; outside computers, servers, and backup tapes; laptop and home computers; and palm pilots and other portable devices. Electronic documents are easily damaged or altered. Computer systems automatically recycle and reuse memory space, overwrite backups, change file locations, and otherwise maintain themselves automatically—with the effect of altering or destroying computer data without any human intent, intervention, or even knowledge. And every electronic document can look like an original.

## Differences in Kind

One difference in kind between digital discovery and conventional paper discovery is that digital transactions (creation of an electronic airline ticket, for example) often create no permanent document in electronic or any other form. There are only integrated databases containing bits and pieces of millions of transactions. After a customer has printed out an e-ticket and moved to a different screen, the e-ticket "disappears."

In addition, unlike conventional documents, electronic documents contain nontraditional types of data, including metadata, system data, and "deleted" data. Metadata refers to the informa-

*A company CEO with no protocol for preserving data during litigation is personally sanctioned by the court for failure to take reasonable measures to preserve data.*

*A small family business is asked to produce relevant e-mail messages, although many messages are believed to have been deleted.*

tion embedded in an electronic file about that file, such as the date of creation, author, source, history, etc. System data refers to computer records regarding the computer's use, such as when a user logged on or off, the Web sites visited, passwords used, and documents printed or faxed. "Deleted" data is not really deleted at all. The computer has merely been told to ignore the "deleted" information and that the physical space that the data takes up on the hard drive is available for overwriting when the space is needed. The possibility that a deleted file can be restored or retrieved presents a temptation to engage in electronic discovery on a much broader scale than is usually contemplated in conventional paper discovery.

## Differences in Costs

Cost differences are often thought to include differences in the allocation of costs as well as the amount of costs. In conventional "big document" cases, for example, when responding parties simply make boxes of documents available for the requesting party to review, the costs of searching through the boxes typically fall on the requesting parties. On the other hand, the cost to the responding parties of locating, reviewing, and preparing vast digital files for production is perceived to be much greater than in conventional discovery proceedings.

One reported case, for example, involved the restoration of 93 backup tapes. The process was estimated to cost \$6.2 million before attorney review of the resulting files for relevance or privilege objections. Complete restoration of 200 backup tapes of one of the defendants in another prominent reported decision was estimated to cost \$9.75 million, while restoration of eight randomly selected tapes, to see if any relevant evidence appeared on them, could be done for \$400,000.

The high costs of electronic discovery frequently include the costs of experts. Systems experts know the computers, software, and files at issue in the case. Outside experts are often brought in to conduct electronic discovery. Their role is to take the data collections, convert them into indexed and reviewable files, and ready them for production. Forensic examiners, the most expensive of all, may be brought in to search for deleted documents, missing e-mail, and system data.

On the other hand, electronic discovery can also greatly reduce the costs of discovery and facilitate the pretrial preparation process. Properly managed, electronic discovery allows a party to organize, identify, index, and even authenticate documents in a fraction of the time and at a fraction of the cost of paper discovery while virtually eliminating costs of copying and transport.

From Ken Withers's presentation to the National Workshop for U.S. Magistrate Judges (2002) available at [www.kenwithers.com](http://www.kenwithers.com).