Computer-Based Discovery in Federal Civil Litigation*

Kenneth J. Withers
Federal Judicial Center
Washington, DC

Discovery is changing in response to the pervasive use of computers. More and more cases involve e-mail, word-processed documents, spreadsheets, and records of Internet activity. In some cases, computer-based discovery can be routine and uneventful. The parties may agree simply to exchange computer disks of documents instead of paper. In many cases, however, computer-based discovery generates disputes over the scope of disclosure, form of production, privilege, and alleged spoliation. The costs associated with computer-based discovery procedures can be extraordinary. In many of the reported cases on electronic discovery, failure of the attorneys to understand their own clients’ computer systems, routines, capabilities, and limitations were at the heart of the problem. Early identification of potential discovery problems and early resolution of these matters may be the key to reducing costs and delay in cases involving computer-based discovery.

Part One of this Introduction briefly discusses some of the positive aspects of computer-based discovery. Part Two explores the unique problems of computer-based discovery, and offers some discovery management suggestions to attorneys. Part Three focuses on the judicial role in managing computer-based discovery and preventing or resolving some of the more common disputes. Finally, Appendix A provides a checklist of computer-based discovery considerations for a Rule 16(c) pretrial conference.

I. Potential Advantages of Computer-Based Discovery

A tremendous body of professional and academic literature is developing around the issue of computer-based disclosure, discovery, and evidence. Most of this literature is premised on the notion that computer-based discovery increases the cost and complexity of civil litigation. But no empirical research directly compares computer-based discovery to analogous conventional discovery, and there is a strong argument for the opposite premise, that the exchange of computer data, as opposed to paper, will reduce cost and delay. The costs of photocopying and transport can be reduced dramatically or eliminated altogether. The time involved in reviewing and organizing evidence can be reduced by using word-searching, sorting, and other forms of computer manipulation. The cost of using a litigation support system is reduced dramatically if the documents are in electronic form from the start and do not need to be scanned. Finally, electronic discovery leads logically to electronic evidence. It stands to reason that many of the media conversion costs associated with electronic courtroom presentations can be reduced or eliminated if the documents are in electronic form from the start.

* An earlier version of this article appears in the Federal Courts Law Review at www.fedjudge.org.
Computer-based discovery offers substantive advantages, as well. Evidence that would have been impossible or extremely difficult to obtain can now become part of the truth-seeking process. Drafts of documents that were routinely lost or destroyed in the conventional paper-based world are now retrievable. Nearly all of the modern panoply of computer-mediated communications, from e-mail messages to digital telephony to virtual conferences, are recorded and saved as digital “documents.” Vast amounts of data that would have been impossible to collect and manipulate in the conventional paper-based business world can be assembled, transmitted, manipulated, and analyzed by computer.

Judges are becoming more sophisticated about computer-based discovery and more willing to manage the process actively. As one computer forensics expert noted in a recent conference, the increased sophistication of judges in this field has “raised the bar” for attorneys appearing in computer-based discovery cases. When attorneys realize that they no longer can muddle, bluff, or stonewall their way through computer-based discovery, they will be forced to educate themselves and their clients, and may become more forthcoming and cooperative with their opponents.

II. Unique Problems of Computer-Based Discovery

Though computer-based discovery has many potential advantages, it can raise unique issues that normally do not occur or are less problematic in conventional, paper-based discovery. Among the most common difficulties are the preservation of data subject to discovery; the location and volume of data; e-mail as a novel medium; documents that have been deleted from the computers; backup tapes, archives, and legacy data; the conduct of on-site inspection; the form of production; and the need for expert assistance.

A. Preservation of data

In conventional paper-based discovery, the documentary sources of information have been, for all intents and purposes, physically stable. Attorneys seldom have cause to assume that paper or microfilm files are subject to imminent damage or destruction. Fire, flood, or corporate document destruction procedures occasionally result in the loss of potential evidence, but these have relatively rare occurrences. On the other hand, information stored in electronic form is easily changed, overwritten, or obliterated by everyday use of the computer, whether it is a single desktop PC (personal computer) or an enterprise-wide network. The simple acts of booting up a computer, opening a file, adding new data onto a hard disk, or running a routine maintenance program on a network can alter or destroy existing data, without the user’s knowledge.

At the outset of litigation involving computer-based discovery, attorneys on both sides have a heightened responsibility to inform their clients of the duty to preserve potential evidence. Counsel who may be seeking discovery of computer-based information should immediately notify opposing counsel of that fact and identify as clearly as possible the categories of information that may be sought later. Counsel who may be responding to
computer-based discovery may not want to wait for such notification, however. To avoid possible embarrassment and accusations of “negligent spoliation,” he or she should identify the computer-based information likely to be subject to discovery and take reasonable steps to secure the integrity of that data. In Procter & Gamble Co. v. Haugen, a defamation and unfair trade practices case, the plaintiff failed to segregate and preserve e-mail files that it knew would be subject to discovery. Ironically, the plaintiff had insisted early in the case that the defendant save all of its e-mail. Even though no specific preservation order was in place, the plaintiff was sanctioned $10,000 for its breach of discovery duties.

Early in the case, the parties should meet and try to agree on the steps each will take to segregate and preserve relevant data, to avoid later accusations of spoliation. At the Rule 16 pretrial conference, the judge can issue a preservation order in line with the agreement.

B. Location and volume of data

In the days of conventional paper-based discovery, most organizations had centrally-located files or a limited number of physical file locations. In the PC-based world, each employee may have a desktop computer, plus disks or other removable data storage media, a laptop computer, a home computer, and a hand-held personal organizer, all containing potentially relevant data. Larger organizations will have network servers connecting and storing data for many PCs, plus backup and archival data storage (discussed below). Offsite and even offshore data storage facilities, Internet service providers, and other third parties may also hold data subject to discovery. The cost and complication of conducting discovery in a modern, distributed business computing environment can be enormous.

In paper-based record-keeping systems, outdated records, papers with no business significance, and superfluous copies are destroyed routinely. Records managers maintain paper files in “business-record order.” In computerized business environments, equivalent electronic records management systems seldom exist. Copies of documents are made routinely, distributed widely, and seldom purged when outdated. Potentially discoverable records are stored according to computer logic, as opposed to “business-record” logic, and can be difficult to locate and untangle from irrelevant and privileged records.

The combination of multiple locations, tremendous volume, and arcane or non-existent records management practices is potentially explosive for defending counsel. In Linnen v. A.H. Robins Co., the defendant faced sanctions in the form of costs and a spoliation inference stemming from counsel’s failure to completely investigate stored computer backup tapes, while representing to the court that all relevant computer files had been produced. Linnen was one of the various state product liability actions stemming from the marketing and distribution a diet drug combination popularly known as “Phen-fen,” which was linked with primary pulmonary hypertension. After counsel for defendant Wyeth-Ayerst Laboratories denied the existence of e-mail backup tapes early in
discovery, deposition testimony of Wyeth staff revealed that nearly 1,000 backup tapes had been set aside for unrelated litigation. But by the time of the disclosure, tapes covering a relevant four-month period had been destroyed in the routine course of business.

The attorneys have an obligation to investigate their clients’ information management system thoroughly to locate potentially relevant and discoverable material, no matter how technically opaque that information system appear. Such an investigation goes well beyond simply asking the client for the relevant files and trusting that the client itself has a complete understanding of its own information technology infrastructure.

**C. E-mail as a unique phenomenon**

Electronic mail does not have a counterpart in the conventional paper-based world. Several characteristics make e-mail particularly problematic. One is the sheer volume, which can be staggering, even for a small company or individual. Another is the lack of a coherent filing system, as e-mail systems are seldom designed for file management and retrieval. Relevant business-related e-mail messages will be found side by side with irrelevant and often very private personal e-mail messages. Perhaps the most important characteristic of e-mail is the nature of the medium itself, which commentators in both the popular press and the legal literature have noted is informal, breezy, and riddled with slang, jargon, and jokes, even in the strictest business environments. These factors combine to make retrieval of e-mail messages by topic difficult, even with computer-based word-searching, and screening for relevance and privilege costly and time-consuming. But these characteristics of e-mail also make it a most attractive target for discovery.

Conventional document-intensive discovery may present problems of volume and density, but generally the organizational system of paper files, where one exists, can be understood without any special technical skill or knowledge. In computer-based discovery, the e-mail system may initially appear as an unfathomable “black box.” The attorneys should develop a clear understanding of their own clients’ e-mail systems, particularly the nature and extent of backup and archival files. They should also develop an understanding of the methods available to search for relevant e-mail messages and an idea of the numbers of messages that are likely to result from such a search. At the start of discovery, counsel should meet and confer about the scope of anticipated e-mail discovery. While the requesting party may want a broad scope to discovery, the realities of budget and time constraints may dictate a narrower search. Both sides should try to agree on an e-mail search protocol, including the sources, key words, names, and date ranges to be searched to avoid disputes over the adequacy of production later.

The question of screening e-mail messages for attorney-client communication privilege, attorney work-product protection, or other privileges before production deserves special attention and may call for some creative negotiation. Large volumes of assorted, undifferentiated text files are difficult to screen for privilege. Computer search techniques may be used to roughly identify messages addressed to or authored by legal
personnel, but the results of such searches will be far from precise. Manual review of the messages by people is time consuming and costly, as well as stupefyingly dull. While the seriousness of the consequences vary among the federal circuits, inadvertent production of privileged e-mail messages may result in the waiver of the privilege in part or in whole, against not only the immediate opponent but third parties as well. If the specter of privilege waiver could be removed, the cost and time of e-mail production would be reduced significantly. To facilitate discovery, the parties could negotiate an agreement regarding inadvertent production of privileged e-mail messages and have it endorsed as order from the court. By producing documents under such a court order, the parties may limit their exposure to each other and to possible third parties.

D. Deleted documents

In the conventional paper-based world, once a document is shredded, incinerated, or buried in a landfill, it is no longer subject to discovery as a practical matter. However, the routine “deletion” of a computer-based document does not destroy the data. Hitting the “delete” key merely renames the file in the computer, marking it available for overwriting if that particular space on the computer’s hard disk is needed in the future. The data may remain on the hard disk or on removable storage media for months or years, or may be overwritten only partially.

It is a relatively simple task for a computer forensics expert to restore routinely deleted data, but it is expensive and the results are uncertain. Although the general rule is that each party bears its own costs in discovery, restoration of routinely deleted records is often conditioned on payment of some or all of the costs by the requesting party.

Aside from the occasional practice of “dumpster diving,” the discovery of deleted computer documents does not have a close analogue in conventional, paper-based discovery. Therefore, it represents a potential increase in the volume of discovery, with associated increases in cost and delay. Although such discovery is within the scope of the discovery rules, counsel should be prepared to demonstrate that it is necessary and germane to the case. Before the Rule 16 pretrial conference, the attorneys should try to agree on whether restoration of deleted data is expected, to what extent restoration will be required, and who will bear the costs.

E. Backup tapes

Most businesses, as well as many individuals, periodically back up their data onto tapes or disks for disaster recovery purposes. Often these tapes are kept for months or even years. Data and documents that have been edited, deleted, or written over in the normal course of business may be recovered from these tapes or disks. Backup tapes, however, are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. Therefore, the organization of the data mirrors the computer’s structure, not the human records management structure, if there is
one. Special programs may be needed to retrieve specific information, and the process may be costly and time consuming.30

Although the discovery of backup tapes is within the scope of the discovery rules, it has the potential to increase the volume of discovery beyond what it would be in conventional, paper-based discovery, with associated increased in costs and delay. As with discovery of routinely deleted files, counsel should be prepared to demonstrate that this discovery is necessary and germane to the case. And as with the discovery of deleted files, retrieving documents from backup tapes may be conditioned on the requesting party paying some or all of the costs. Before the Rule 16 pretrial conference, the attorneys should agree on whether discovery of backup data is expected, to what extent it will be required, and who will bear the costs.

F. Archives and legacy data

Ideally, archival electronic files should be organized for identification and retrieval of individual documents or series of records. Ideally, as businesses, institutions, and government agencies adopt new computer systems, the data from older systems should be transferred to new media. In reality, such electronic records management processes are primitive or non-existent in many organizations.31 It is common to find that:

- unorganized backup tapes are kept as a substitute for organized archival files
- old data are impossible to read using current hardware and software
- old data transferred to current media and format have lost important elements necessary to establish context or authenticity.

As part of the initial disclosure process, attorneys should conduct a thorough survey of their clients' electronic archives and so-called "legacy data" in outmoded formats or on outmoded media. A realistic assessment must be made of the extent to which these files will be subject to discovery and how much it will cost to make these files searchable. In many cases, random samples of legacy data are restored and searched in order to establish a statistically valid likelihood of finding relevant information. Based on such statistics, balanced judgments can be made as to the value of the potential discovery weighed against the anticipated costs.32

G. On-site inspection

Computer-based discovery makes on-site inspections under Rule 34(b) of the Federal Rules of Civil Procedure particularly problematic. On the one hand, it may be necessary to view the computer system in operation to make sure the discovery protocols are being performed properly, to check the adequacy of security and chain of custody, or to ascertain the provenance of computer records. On the other hand, the nature of computer record storage and organization makes it virtually impossible to protect privileged or trade secret information in the context of an on-site inspection, and any manipulation of the computer by the opposing party, counsel, or expert may compromise the entire process.
In Gates Rubber Co. v. Bando Chemical Indus., Ltd., a botched on-site inspection resulted in the loss of possibly critical data by the party seeking discovery. Discovery had been protracted and acrimonious in this trade secret theft case when the plaintiff learned that an individual defendant had allegedly destroyed records on his computer. The plaintiff obtained a “Site Inspection Order” designed to allow it complete access to the defendants’ computers, while protecting the defendants’ rights to object to the production of irrelevant or privileged materials. As a result, the plaintiff documented several instances of what it characterized as destruction of evidence, but the magistrate judge denied most of the plaintiff’s motion for sanctions, citing the behavior of the plaintiff’s own expert. For instance, to examine one particularly important computer, the expert used a program that erased, at random, 7 to 8 per cent of the information that might otherwise have been available. The expert also failed to obtain and preserve the creation dates of essential files and failed to use accepted computer evidence preservation procedures.

In the past two years, federal courts have begun establishing a set of accepted computer inspection procedures, based in part on the bitter lessons of Gates Rubber. Three recent federal cases -- Playboy Enterprises, Inc. v. Welles, Northwest Airlines, Inc. v. Local 2000 International Brotherhood of Teamsters, AFL-CIO, et al., and Simon Property Group, L.P. v. MySimon, Inc. – demonstrate this evolution. The procedure ordered by the court in each of these cases was:

- The parties agree on a neutral, third-party expert who will actually carry out the inspection as an officer of the court.
- The parties, with expert assistance, agree on the scope of the inspection, including target computers or servers; target individuals, departments, or data collections; date ranges; search terms; or other scope-defining criteria. They also agree upon the form of eventual production.
- The expert creates a “mirror image” of the computer data using accepted computer forensic procedures that preserve the integrity of the original evidence.
- The expert executes the search on the “mirror image” and identifies relevant data according to the agreed-upon specifications.
- The expert turns over the responsive data to the respondent’s counsel.
- Respondent’s counsel reviews the responsive data for relevance and privilege.
- Respondent’s counsel produces relevant, non-privileged data to the requesting party in the form agreed upon by the parties.

These protocols help the parties set clear goals for computer-based discovery, help limit the scope and cost, and may serve to protect legitimate privilege and privacy interests. They also provide a mechanism for shifting some of the costs, for in all three cases cited above the requesting party paid the expenses of the neutral expert.

The cost of an on-site inspection in terms of business disruption must be considered. It is one thing to inspect a conventional file room or document warehouse. The use of paper
files for short periods of time does not generally affect ongoing business operations. However, the use of the business computer system to conduct a wide-ranging search may require the business to shut down all operations completely. The protocols being developed for on-site inspection of computer files, particularly the creation of a “mirror image” of the data at the outset, help minimize business disruption.37

But the use of neutral experts has costs, too, and those costs must be weighed against the potential benefits. In the Simon Property case, the cost of implementing the protocol exceeded $200,000, and resulted in only a handful of new documents, none of which were material to the outcome of the case. The victorious plaintiff’s application for costs at the end of the case was denied, in part because the judge viewed the computer-based discovery as unnecessary and duplicative.38 Parties may also believe that they need to retain their own expert to review the work of the neutral expert, thus duplicating costs.

H. Form of production

In 1970, when Rule 34 of the Federal Rules of Civil Procedure was amended to include discovery of “data compilations,” the typical and preferred response to a computer-based discovery request was a printout of the computer data. In those days, few if any law offices had computers, and the software necessary to translate and manipulate the data was not mass marketed. Today, producing printouts of computer data is so unnecessary that it might be considered an abusive tactic. Many computer-based documents, such as relational databases and spreadsheets, are meaningless in printed form. The recipient is forced to reenter the data or spend long hours performing manual analysis. To avoid unnecessary costs and delay, courts have ordered production in electronic form even if it duplicates prior paper production or involves the creation of tapes or disks that did not hitherto exist.39

Today, electronic exchange of computer data is the preferred mode,40 but within that mode, plenty of room exists for dispute over the exact format. With the assistance of computer experts, the attorneys should establish common procedures and formats for the production of electronic information at the outset of discovery.

I. Need for expert assistance

As demonstrated above, both parties engaged in computer-based discovery will need the assistance of computer experts. This is costly, but in the long run may save costs and time. Once the experts have had an opportunity to assess their respective parties’ computer systems and capabilities, they will be in a much better position than the attorneys to negotiate the technical aspects of conducting discovery, including search protocols, privilege and relevance screening, and production. Often the lawyers can be taken out of the picture entirely. In many cases, the experts on opposing sides have met and worked out agreements on the exchange of computer system information, the procedures for inspection, the search terms each side will use, and other details best left to those with technical knowledge and experience.41
III. Judicial Management Tools for Computer-Based Discovery

It is not the judge’s role to dictate solutions to these thorny technical problems unless the parties reach an impasse. But to avoid an impasse, the judge must make sure the attorneys on both sides face these issues squarely, negotiate solutions, and follow through. Several tools are available to help judges manage computer-based discovery, limit costs and delay, and, if necessary, resolve discovery disputes.

A. Early exchange of computer system information

At the outset of litigation, before any document or computer-based discovery is initiated, the attorneys should be encouraged to exchange information about their clients’ respective computer systems. One of the most frustrating experiences for a judge, and an all-too-common one, is to conduct a pretrial conference with opposing counsel who do not know what their client has or can produce in discovery. In all fairness, attorneys cannot be expected to become computer experts for the purposes of discovery and should not do so. The judge can inject reality into the discovery planning process by encouraging communication between the people who actually know their respective computer systems. An informal meeting between the opposing sides’ computer experts will probably accomplish more than a meeting of the lawyers. Such a meeting may need a neutral moderator and blanket privilege protection, similar to a settlement negotiation or mediation.

The information each side needs to know includes identifying which computer systems are in place at the moment, which computer systems were in place during the period of time relevant to anticipated discovery, the extent of the computerized information (including backups and archives) that will need to be searched in the course of discovery, the capabilities of each party to perform searches and produce material in a useable format, and the measures being taken to secure and preserve potential computer evidence.

If the parties insist on a formal, adversarial approach, the judge can allow each side to depose the opposing party’s most knowledgeable computer person under Rule 30(b)(6) of the Federal Rules of Civil Procedure. Although Rule 26(d) generally does not allow formal discovery before the parties met and conferred under Rule 26(f), the judge has the power to order such preliminary discovery as may be necessary to lay the foundation for a productive Rule 26(f) meeting and subsequent Rule 16(c) pretrial conference.

B. Rule 16(c) pretrial conference agenda

Perhaps the most important judicial management tool in computer-based discovery cases is the Rule 16(c) pretrial conference. Rule 16(c) of the Federal Rules of Civil Procedure lists several issues that may be addressed during the pretrial conference, but a judge may supplement that list with additional points on computer-based discovery and issue a memo to the attorneys before the conference, preferably at the outset of the litigation. There is a risk associated with such a procedure: The judge may alert counsel to issues that they had not considered, inadvertently expanding the scope of discovery. But given
that computer-based discovery and its associated issues will become the norm, not the exception, in the future, this risk may be small.

The Appendix to this article is a checklist of possible agenda items and questions about computer-based discovery for a Rule 16(c) pretrial conference. It represents a maximalist approach, and should be scaled to fit the needs of the particular case, the resources of the parties, and the litigating styles of the attorneys involved.

C. Rule 26(a)(1) initial disclosures

On 1 December 2000, initial disclosure became the rule throughout the federal court system, except for cases so small and routine that they normally involve little or no discovery of any type. Under initial disclosure, first adopted as an optional rule in 1993, the parties must unilaterally disclose the existence of relevant documents and other categories of information before receiving a discovery request. However, in proposing to make the initial disclosure requirement uniform across the nation, the Civil Rules Advisory Committee also included a major compromise with disclosure opponents in the organized bar. The scope of document disclosure found in the current Rule 26(a)(1)(B) was narrowed from documents “relevant to disputed facts alleged with particularity in the pleadings” to documents “the disclosing party may use to support its claims or defenses.” In the same round of amendments, the Committee reinforced Rule 37(c)(1) to make it clear that a party is not permitted to use evidence at trial, at a hearing, or on a motion that was not disclosed initially or included in an original or amended discovery response. The Advisory Committee Note to the 2000 Amendment of Rule 26 states that this serves to bolster the requirement that denials in pleadings be “warranted on the evidence” under Rule 11(b)(4).

While Rule 26 initial disclosure may be viewed primarily as a device to expedite attorney-managed discovery, it may also be viewed as a judicial management and dispute resolution device. Where the Rule 26 initial disclosure requirement was in effect before 1 December 2000, it forced attorneys to investigate the factual basis of their case or defense early, before the first Rule 16 scheduling conference, allowing them to provide the judge with a much clearer picture of what formal discovery in the case might involve.

The narrowed scope of the current Rule 26 disclosure does not eliminate that advantage. In a world in which most documentary evidence will be computer-based, initial disclosure under Rule 26(a)(1) requires that attorneys undertake a reasonable investigation of their clients’ computer files and disclose computer-based evidence that they may use to the support their claims or defenses. Failure to do so in a timely manner may preclude them from mounting any effective case or defense. Instead of entering the Rule 16 pretrial conference ignorant (perhaps blissfully) of their clients’ computer systems, they must meet with opposing counsel, confer, and exchange initial disclosure of computer-based evidence, even if that evidence is largely self-serving, or face sanctions under Rule 37(c)(1). In addition, if counsel discloses computer-based evidence, he or she may be under an obligation to disclose relevant aspects of the source computer system, including such important matters as the location of the disclosed computer files,
backup and archiving procedures assuring that the disclosed information will be available for production, and the extent to which the disclosed information may need to be recovered from legacy or deleted files. At the very least, counsel should be prepared to face later discovery on these issues.

Although Rule 26 initial disclosure statements will seldom if ever filed with the Court, they will undoubtedly become a subject of discussion in the Rule 16(c) pretrial conference if the parties fail to reach an agreement on the scope and conduct of discovery beforehand. As such, they may enable a judge to make a more informed decision if asked to expand or limit the scope of discovery, compel or protect production of particular data, weigh the benefits and burdens of discovery, or shift discovery costs.

D. Proportionality

Under Rule 26 of the Federal Rules of Civil Procedure, the trial court has the power to limit discovery “if the burden or expense of the proposed discovery outweighs its likely benefit.” This language was added 1983 to combat “excessively costly and time-consuming activities that are disproportionate to the nature of the case, the amount involved, or the issues or values at stake …[by] giving the court authority to reduce the amount of discovery that may be directed to matters that are otherwise proper subjects of inquiry.” Ten years later, the Advisory Committee made further amendments and created the current Rule 26(b)(2)(i), (ii), and (iii), citing the “information explosion of recent decades [which] has greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument of for delay or oppression.” Just to make sure no one misses the point, the 1 December 2000 amendments added yet further language to Rule 26(b)(1), reminding litigants that “all discovery is subject to the limitations imposed by subdivision (b)(2)(i), (ii), and (iii).”

If extraordinary discovery efforts, such as on-site computer inspection or the recovery of deleted data, are not justified by some showing that the efforts are likely to result in the production of relevant and material information, it is within the judge’s discretion to limit such discovery. In Fennell v. First Step Designs, the plaintiff warehouse worker claimed she was discharged for making allegations of sexual harassment. The defendant employer countered that her layoff was part of a routine seasonal layoff of a number of employees, and offered as evidence a memorandum listing her name with other employees scheduled for termination. The memo was dated before her sexual harassment allegation and corroborated by testimony from three managers, but the plaintiff claimed the memo was a forgery. She proposed inspection of the employer’s computer system, on which the memo was created, for evidence supporting her claim. The proposed discovery was denied after the parties could not agree on a protocol that would reasonably determine whether the memorandum had been altered as the plaintiff claimed, appropriately limit the scope of computer-based discovery to protect privilege, and prevent a “fishing expedition” for unrelated evidence.

It should be noted that the computer inspection in Fennell was proposed in the context of a pending Rule 56 summary judgment motion after formal discovery was closed, and the
appeals court based its decision on the procedural posture of the case as well as the merits of the proposed discovery. But the appellate court cited both Rule 56(f) and Rule 26(b)(2)(iii), and went into considerable detail on the proposed computer inspection protocol, the risks and cost involved, and the likelihood that the proposed discovery would not result in any significant new information, concluding that the trial judge did not abuse his discretion in denying the plaintiff’s request.47

Rule 26(b)(2)(iii), which provides judges with the power to limit burdensome discovery, may also be invoked by the court to compel discovery and fashion a computer-based discovery protocol. One of the most recent reported computer-based discovery cases to cite Rule 26(b)(2)(iii), Simon Property Group, L.P. v. MySimon, Inc.48 represents a step in the process initialed in Playboy Enterprises, Inc. v. Welles39 (which also cited Rule 26(b)(2)(iii)), and refined in Northwest Airlines, Inc. v. Local 2000 International Brotherhood of Teamsters, et al.50 All three of these cases allowed discovery to proceed under a narrowly-crafted protocol, designed to protect the respondents’ rights to object to the actual production of irrelevant or privileged material.

If the court is convinced that extraordinary discovery efforts are justified but costly, a motion to compel or a negotiated protocol may be conditioned on the party seeking discovery bearing the costs. But the recent debates of the Civil Rules Advisory Committee and the Judicial Conference over cost-bearing, discussed in the following section, indicate a grave concern that monetary cost not be the overriding factor in the proportionality consideration.

E. Cost-bearing

The normal rule in document discovery is that each side bears its own costs. The court has the inherent power to shift such costs to the discovery proponent, balancing the needs of justice with the resources of the parties. During the most recent round of rules amendment discussions there was an effort on the part of the Advisory Committee on Civil Rules to codify this inherent power. In 1998, it published a proposed amendment to Rule 34, which governs document requests. The proposed amendment to Rule 34(b) would have added the sentence:

On motion under Rule 37(a) or Rule 26(c), or on its own motion, the court shall – if appropriate to implement the limitations of Rule 26(b)(2)(i), (ii), or (iii) – limit the discovery or require the party to pay part or all of the reasonable expenses incurred by the responding party.51

During 1999, this proposed new language was modified and moved to Rule 26(b)(2), immediately preceding the proportionality considerations of Rule 26(b)(2)(i), (ii), and (iii), thus linking proportionality and cost-bearing.52

There was vigorous debate in the Advisory Committee over this amendment. While acknowledging the courts’ inherent power to shift costs, the opponents stated that this should not be explicitly encouraged, particularly in the context of a rule on
proportionality, as it could have the dual effect of expanding the scope of discovery available to those who can afford it, while restricting the scope of discovery for those who could not. The Justice Department commented that the amendment might encourage judges to order that the United States pay for discovery that it would previously have been entitled to under the usual cost-bearing rule.53

Computer-based discovery played an important part in the argument on cost-bearing. As stated in the Advisory Committee’s Minutes,

A plaintiff, for example, may want to “map” a defendant’s e-mail system, a measure that might cost $250,000; the question of responsibility for paying for such discovery is an important one, and it should be made clear that judges have authority to consider the question directly. [Advisory Committee Member Myles V. Lynk] suggested that lawyers are prepared now to argue about paying the costs of electronic discovery; this explicit rule provision is not needed for that reason. 54

The proposed amendment was approved by the Advisory Committee by a vote of eight to five.55 However, it was rejected by the full Judicial Conference56 and was not included in the package of amendments that went into effect on 1 December 2000. There is no indication that this action represented a rejection of the concept of cost-bearing by either the Judicial Conference or the Supreme Court. As stated by both sides of the debate at the Advisory Committee level and reflected in the Judicial Conference’s consideration of the issue, the courts have inherent powers to manage discovery, including the power to condition discovery in some cases upon the bearing of costs.57

Computer-based discovery may involve extraordinary costs that are clearly outside the usual cost of doing business. In *Anti-Monopoly v. Hasbro*,58 the defendant stated that the data requested by the plaintiff could be extracted from its database only by special programming techniques. Otherwise, the defendant would be forced to give entire database over to a competitor. The court required the plaintiff to pay the defendant’s reasonable costs to produce data in computerized form. In the recent line of cases involving computer inspection protocols culminating in *Simon Property Group, L.P. v. MySimon, Inc.*59 costs were shifted by virtue of requiring the party seeking discovery to assume the expense of the computer expert, even though that expert was a neutral officer of the court.

F. Special master or court-appointed expert

Under Rule 53 of the Federal Rules of Civil Procedure and Rule 706 of the Federal Rules of Evidence, the judge has the power to appoint a neutral expert to act as a special master or as an expert in computer-based discovery. If the parties cannot provide their own expert, or if the situation is contentious, the judge may appoint a neutral third party to break an impasse, supervise technical aspects of discovery, or act as a secure repository for sensitive or disputed data. Courts may understandably be reluctant to utilize an neutral
expert or special master. Rule 53 itself discourages the practice. But even a suggestion by the judge to bring in a neutral expert may help bring the attorneys to an agreement.

While court-appointed experts may help in large-scale or contentious computer-based discovery, they may be absolutely necessary in on-site computer inspections. In Gates Rubber Co. v. Bando Chemical Indus., Ltd., the parties each appointed their own expert, with varying degrees of competence, and the results were counter-productive. Simon Property Group, L.P. v. MySimon, Inc., and the cases cited therein reflect the evolution of the courts’ use of experts to conduct on-site computer-based discovery. The use of court-appointed neutral experts in these may represent the “state of the art” in discovery management. But is also represents a major step in the ongoing evolution of the role of the judge in discovery, from bystander and occasional referee to active manager, and many judges may have reservations about taking that step.

Conclusion

Computer-based discovery has the potential to reduce costs and shorten the length of civil litigation, although it is widely viewed by the legal profession as costly, time-consuming, and more complicated than conventional discovery. Most observers believe that in spite of its costs, computer-based discovery will eventually overtake conventional discovery, as more and more information is routinely generated, transmitted, and stored on computers. Many of the costs associated with computer-based discovery are avoidable through proper management of the discovery process, particularly early identification of potential problems and their solutions. Unless and until attorneys develop more familiarity with computer-based discovery, judges can take the lead by utilizing existing case management techniques, particularly by setting the Rule 16(c) pretrial conference agenda, creatively sequencing discovery events, and limiting or shifting discovery costs. In contentious situations where potentially intrusive inspection of computer facilities and files is demanded, judges may assume an even broader managerial role.
APPENDIX A

A Rule 16(c) Pretrial Conference Agenda for Computer-Based Discovery

The following checklist represents a maximalist approach. It should be scaled to fit the needs of the particular case, the resources of the parties, and the litigating styles of the attorneys involved.

I. When is a Detailed Rule 16 Notice Most Appropriate?

- When the substantive allegations involve computer-generated records, e.g., software development, e-commerce, unlawful Internet trafficking, etc.
- When the authenticity or completeness of computer records is likely to be contested
- When a substantial amount of disclosure or discovery will involve information or records in electronic form, e.g., e-mail, word processing, spreadsheets, and databases
- When one or both parties is an organization that routinely used computers in its day-to-day business operations during the period relevant to the facts of the case
- When one or both parties has converted substantial numbers of potentially relevant records to digital form for management or archival purposes
- When expert witnesses will develop testimony based in large part on computer data and/or modeling, or when either party plans to present a substantial amount of evidence in digital form at trial
- In any potential “big document” case in which cost associated with managing paper discovery could be avoided by encouraging exchange of digital or imaged documents (especially if multiple parties are involved)

The purpose of a detailed Rule 16 notice is to save the parties time and expense by anticipating the most common issues of computer-based discovery, developing a reasonable discovery plan, and avoiding unnecessary conflict. A detailed Rule 16 notice would not be appropriate if, in the opinion of the judge, the notice might serve to alarm the parties needlessly, raise unreasonable expectations or demands, or encourage the parties to engage in wasteful discovery.

II. Preservation of Evidence

A. What steps have counsel taken to ensure that likely discovery material in their clients’ possession (or in the possession of third parties) will be preserved until the discovery process is complete? If counsel have not yet identified all material that should be disclosed or may be discoverable, what steps have been taken to ensure that material will not be destroyed or changed before counsels’ investigations are complete?

If more specific direction is needed:
B. Have counsel identified computer records relevant to the subject matter of the action, e.g.,

- Word processing documents, including drafts or versions not necessarily in paper form
- Databases or spreadsheets containing relevant information
- E-mail, voicemail, or other computer-mediated communications
- Relevant system records, such as logs, Internet use history files, and access records

C. Have counsel located the following computer records:

- Active computer files on network servers
- Computer files on desktop or local hard drives
- Backup tapes or disks, wherever located
- Archival tapes or disks, wherever located
- Laptop computers, home computers, and other satellite locations
- Media or hardware on which relevant records may have been “deleted” but are recoverable using reasonable efforts

D. Have counsel made sure all relevant computer records at all relevant locations are secure, e.g.,

- Suspended all routine electronic document deletion and media recycling
- Segregated and secured backup and archival media
- Created “mirror” copies of all active network servers, desktop hard drives, laptops, and similar hardware

E. Have counsel considered entering into an agreement to preserve evidence?

F. Does either party plan to seek a preservation order from the court?

III. Disclosure and Preliminary Discovery

A. Have counsel designated technical point-persons who know about their clients’ computer systems to assist in managing computer records and answering discovery requests?

B. Have counsel prepared a description of their respective parties’ computer systems for exchange? Does either party need to know more before discovery can proceed?

If, after considering whether the hints in the following list may do more harm than good, the judge determines that the parties are unclear as to what they need to know at this stage and should get further guidance, the judge may suggest that they exchange information on the following points:

- Number, types, and locations of computers currently in use
• Number, types, and locations of computers no longer in use, but relevant to the facts of the case
• Operating system and application software currently in use
• Operating system and application software no longer in use, but relevant to the facts of the case
• Name and version of network operating system currently in use
• Names and versions of network operating systems no longer in use, but relevant to the facts of the case
• File-naming and location-saving conventions
• Disk or tape labeling conventions
• Backup and archival disk or tape inventories or schedules
• Most likely locations of records relevant to the subject matter of the action
• Backup rotation schedules and archiving procedures, including any backup programs in use at any relevant time
• Electronic records management policies and procedures
• Corporate policies regarding employee use of company computers and data
• Identities of all current and former personnel who had access to network administration, backup, archiving, or other system operations during any relevant time

C. Do counsel anticipate the need to notice any depositions or propound any interrogatories to obtain further information about the opposing party’s computer systems or electronic records management procedures?

D. Have counsel explored with their clients (in appropriate situations) the procedures and costs involved to:

• Locate and isolate relevant files from e-mail, word processing, and other collections
• Recover relevant files generated on outdated or dormant computer systems (so-called “legacy data”)
• Recover deleted relevant files from hard drives, backup media, and other sources

E. Do counsel anticipate the need to conduct an on-site inspection of the opposing party’s computer system?

• Consideration of an agreed-upon protocol
• Permission to use outside experts
• Agreement on neutral expert

IV. Electronic Document Production

A. Will counsel use computerized litigation support databases to organize and store documents and other discovery material?

B. Have counsel considered common formats for all electronic document exchange, e.g., TIFF images with OCR-generated text, e-mail in ASCII format, etc.?
C. Have counsel (particularly in multi-party cases) considered a central electronic document repository?

D. Have counsel considered an attorney-client privilege non-waiver agreement, to avoid the costs associated with intensive privilege screening before production?

E. Do counsel anticipate requesting data in non-routine format, e.g.,
   - Printing by respondent of electronic documents not normally in print form
   - Creation by respondent of customized database reports
   - Performance by respondent of customized searches or data mining

F. Have counsel agreed upon cost allocation outside the usual rule that parties absorb their own disclosure costs, e.g.,
   - Requesting parties will pay non-routine data retrieval and production costs
   - Parties will negotiate data recovery and legacy data restoration costs

G. Does either party anticipate objecting to the production of computer records or software necessary to manipulate the records based on:
   - Trade secret
   - Licensing restrictions
   - Copyright restrictions
   - Statutory or regulatory privacy restrictions

V. Testifying Experts

A. Will any testifying expert(s) rely on computer data provided by either party, or rely on his or her own data?

B. Will any testifying expert(s) use custom, proprietary, or publicly-available software to process data, generate a report, or make a presentation?

C. Do counsel anticipate requesting discovery of either the underlying data or the software used by any testifying expert?

VI. Anticipating Evidentiary Disputes

Have counsel considered discovery procedures designed to reduce or eliminate questions of authenticity, e.g.,
- Computer discovery supervised by neutral party
- Neutral, secure electronic document repository
- Exchange of read-only disks or CD-ROMs
- Chain-of-custody certifications
Endnotes

1. Kenneth J. Withers is a Research Associate at the Federal Judicial Center, Washington D.C. The opinions expressed in this article are those of the author and not necessarily those of the Federal Judicial Center or any other agency of the United States Courts. The author thanks Chief Magistrate Judge Robert Collings of the District of Massachusetts for suggesting the creation of a Rule 16 agenda for computer-based discovery, and Prof. Thomas D. Rowe, Jr. of Duke University School of Law for his tough but benevolent editorial review of an earlier version of this paper. Any errors or omissions, however, are attributable solely to the author.

2. In a recent survey of participants at an American Bar Association meeting, 70% of respondents stated that they believed the use of technology in discovery, particularly computer forensics and review of electronic information, will be “increasing dramatically” in the future. PricewaterhouseCoopers/Section of Litigation of the American Bar Association Pulse Survey (15 May 2000) (copy on file with the author).

3. During the summer of 2000, researchers at the Federal Judicial Center sent surveys on computer-based discovery to 400 federal magistrate judges and had received 115 replies. 71 magistrate judges reported that they were aware of computer-based discovery activity in the civil cases assigned to them. Most, but not all, reported disputes arising from discovery. 27 reported fewer disputes coming to their attention than the number of cases in which there was computer-based discovery, implying that some cases presented no discovery disputes. Ten reported no disputes at all associated with computer-based discovery. Four magistrate judges expressly commented that computer-based discovery had presented no unique problems, and one judge made the observation that he may have more cases involving computer-based discovery than those of which he is aware. Federal Judicial Center, Survey Of United States Magistrate Judges On Experiences With Discovery Of Computer-Based Evidence (June/July 2000) (survey returns and preliminary analysis on file with the author).


5. Lawrence Argon, E-mail Is Not Beyond the Law, PC Week, 6 October 1997 at 111 (the cost of reviewing ten years worth of data in a recent case was over $500,000); Kim Nash, Computer Detectives Uncover Smoking Guns, ComputerWorld, 9 June 1997 at 1A (twelve months of e-mail generated by 50 people will cost between $60,000 and $75,000 to examine).

6. See, e.g., Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super. Ct.), in which the defendant was ordered to bear all fees and costs associated with computer-based
discovery based on its failure, “be it unintended or willful,” to respond adequately to the plaintiff’s discovery requests for e-mail from back-up tapes. *Id.* at 8. *See also* GFTM, Inc. et al. v. Wal-Mart Stores, Inc., 2000 WL 335558 (S.D.N.Y.), in which the defendant was sanctioned for counsel’s initial representation that requested computer data did not exist, contradicted a year later by deposition testimony that the data existed when they were requested, but were subsequently destroyed.


8. In the Federal Judicial Center survey cited in endnote 3, 14 of the 71 judges who reported computer-based discovery activity in the cases assigned to them reported “significant cost savings” over conventional discovery in some or all of those cases.

9. In the nationwide breast implant litigation, MDL-926, conversion of just one-third of the discovery documents and court papers to computer form resulted in an estimated savings of $1,146,500 in copying costs per party requesting a complete set of the documents. E-mail message from Tina J. Crowe, Supervisor, National Multidistrict Litigation Document Repository, to Kenneth J. Withers (27 April 2000) (on file with the author). This savings potential has also been noted in British civil litigation, Grupo Torras v. Sheik Fahad Mohammed al Sabah [1998] Masons Computer L. Rpts. 90.


14. In the Microsoft antitrust litigation, the task of quantifying potential damages was simplified by the court granting the Department of Justice direct access to Microsoft’s computerized sales and pricing data. Kim S. Nash and Patrick Thibodeau, *What’s In a Database? Microsoft Sales Evidence: Court Allows DOJ to Check Files in Redmond*, Computerworld, 19 October 1998, at 4.


18. A 1998 survey conducted by the American Bar Association and the American Corporate Counsel Association indicated that while 92% of respondents’ corporations stored records in electronic form, just under 40% had electronic records management programs, and only 28% monitored compliance. Thomas J. Smedinghoff, ABA/ACCA Survey of Electronic Commerce Practices (1998) (on file with the author). A more recent survey of litigation attorneys by the American Bar Association and PricewaterhouseCoopers indicated that only 11.5% of the respondents’ corporate clients had “an electronic data classification mechanism that allows one to quickly locate data relevant to a particular area of litigation.” PricewaterhouseCoopers/Section of Litigation of the American Bar Association Pulse Survey, Digital Discovery and Its Importance on the Practice of Litigation (15 May 2000) (on file with the author). Based on his own survey of practices in corporations and government agencies, Prof. David A. Wallace of the University of Michigan School of Information stated that the need to develop electronic records management systems is the “single most important priority” for the recordkeeping professions. David A. Wallace, Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice, (paper prepared for the 1998 Annual Meeting of the Society of American Archivists) at http://www.rbarry.com/dwallace.html.


21. “While the court certainly recognizes the significant cost associated with restoring and producing responsive communications from these tapes, it agrees with the District Court for the Northern District of Illinois In re: Brand Name Prescription Drugs Antitrust Litigation that this is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world… To permit a corporation such as Wyeth to reap the business benefits of such technology a simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.” Id. at 6, citing In re Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360525 (N. D. Ill.); see also GFTM, Inc. v. Wal-Mart Stores, Inc., supra note 6.

22. One Internet market research company estimates that the average American processes 26.4 messages per day, one-third of which (8.8 per day) they generate. EMarketer Tallies the Number of E-Mail Messages Sent, Emarketer (1 February 2000). If 100 employees of a business generate 8.8 messages per day, 5 days a week, for 48 weeks per year (allowing for vacations and holidays), the business will accumulate 211,200 messages annually, not counting copies or backups.


26. Texas has a new rule that may serve as a model for such an agreement in other jurisdictions. Rule 193.3(d) of the Texas Rules of Civil Procedure, adopted in 1999, states, “Privilege not waived by production. A party who produces material or information without intending to waive a claim of privilege does not waive that claim under these rules or the Rules of Evidence if – within ten days or a shorter time ordered by the court, after the producing party actually discovers that such production was made – the producing party amends the response, identifying the material or information produced and stating the privilege asserted. If the producing party thus amends the response to assert a privilege, the requesting party must promptly return the specified material or information and any copies pending any ruling by the court denying the privilege.”

27. For an examination of the typical state of computer files subject to discovery and the role of the computer forensics expert, see Andy Johnson-Laird, Smoking Guns and Spinning Disks, 11 Computer Law. 1 (1994).

28. This cost-bearing shift is codified in Texas R. Civ. P. 196.4, which states in part: “If the responding party cannot – through reasonable efforts—retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.” It also forms the basis of the August 1999 American Bar Association Section of Litigation’s Civil Discovery Standards 29(b)(iii).


31. See supra note 18.
32. Such a procedure was used in the Phen-Fen multidistrict litigation, In re Diet Drugs Products Liabilities Litigation, MDL 1203 (E.D. Pa. 1999), Letter from Eric Rubel to Michael D. Fishbein (21 April 1999) (on file with the author) (agreement between Plaintiffs’ Management Committee and defendant American Home Products concerning the restoration of sample backup tapes).


34. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

35. Civil Action No. 00-08 (D. Minn. Feb, 2, 2000) (Order on Defendants’ Motion for Protective Order and Plaintiff’s Motion to Compel Discovery).


38. Telephone conversation with Judge David F. Hamilton, October 2, 2000 (notes on file with the author), see also Simon Property Group, L.P. v. MySimon, Inc., 2001 WL 55408 (S.D. Ind.).


41. At a recent “mini-conference” on computer-based discovery issues sponsored by the Discovery Subcommittee of the Civil Rules Advisory Committee of the Judicial Conference of the United States held at Hastings College of Law in San Francisco on 27 March 2000, panelists Joan Feldman and Andy Johnson-Laird commented that experts from opposing sides will often meet and confer on discovery logistics.

42. The narrow exceptions may be found at Fed. R. Civ. P. 26(a)(1)(E)(i) – (viii).


45. Fed. R. Civ. P. 26(b)(2) reads as follows: “(2) Limitations. By order, the court may alter the limits in these rules on the number of depositions and interrogatories or the length of depositions under Rule 30. By order or local rules, the court may also limit the number of requests under Rule 36. The frequency or extent of the use of discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expansive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties’ resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues. The court may act upon its own initiative after reasonable notice or pursuant to a motion under Rule 26(c).”

46. 83 F. 3d 526 (1st Cir. 1996).

47. Id. at 534.


49. 60 F. Supp. 2d 1050, 1054 (S.D. Cal. 1999).

50. Civil Action No. 00-08 (D. Minn. Feb, 2, 2000) (Order on Defendants’ Motion for Protective Order and Plaintiff’s Motion to Compel Discovery).


53. Minutes of the Civil Rules Advisory Committee, 19-20 April 1999, 1999 WL 1702844, 26-29. This document is also available on the Internet at <http://www.uscourts.gov/rules/Minutes/0499civilminutes.htm>

54. Id. at 28.

55. Id. at 29.


58. 1996 WL 22976 (S.D. N.Y.). Cf., In re Brand Name Prescription Drug Antitrust Litigation, 1995 WL 3360526 (N.D. Ill. 1995), in which the cost to the producing party of searching 30 million e-mail messages for relevant information, estimated at $50,000 to $70,000, was held not to be “undue” and would not be shifted to the requesting party.


60. Fed. R. Civ. P. 53(b) states in part, “A reference to a master shall be the exception and not the rule… a reference shall be made only when the issues are complicated… a reference shall be made only upon a showing that some exceptional condition requires it.”
