UIC John Marshall Journal of Information Technology & Privacy Law

Volume 17
Issue 2 *Journal of Computer & Information Law - Winter 1999*

Article 2

Winter 1999

Computers and the Discovery of Evidence - A New Dimension to Civil Procedure, 17 J. Marshall J. Computer & Info. L. 411 (1999)

Mark D. Robins

Follow this and additional works at: https://repository.law.uic.edu/jitpl

 Part of the Computer Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Mark D. Robins, Computers and the Discovery of Evidence - A New Dimension to Civil Procedure, 17 J. Marshall J. Computer & Info. L. 411 (1999)

https://repository.law.uic.edu/jitpl/vol17/iss2/2

This Article is brought to you for free and open access by UIC Law Open Access Repository. It has been accepted for inclusion in UIC John Marshall Journal of Information Technology & Privacy Law by an authorized administrator of UIC Law Open Access Repository. For more information, please contact repository@jmls.edu.

COMPUTERS AND THE DISCOVERY OF EVIDENCE—A NEW DIMENSION TO CIVIL PROCEDURE

by MARK D. ROBINS†

† Mark D. Robins is an attorney in the litigation department and technology and intellectual property practice group of Hutchins, Wheeler & Dittmar, Professional Corporation, Boston, Massachusetts. The views expresed in this article should not be attributed to Hutchins, Wheeler & Dittmar or to any of its clients. © 1999 Mark D. Robins.

I. INTRODUCTION

Computers provide vast resources for the discovery of evidence—resources that have been largely untapped by litigators. Although form discovery requests increasingly employ definitions and instructions that purport to encompass materials residing in various media for computer storage, few attorneys give much thought to what types of evidence in any particular case might be found in such media and what methods of discovery will most likely yield this evidence. Indeed, many attorneys have little notion of what types of evidence are available from different computer-related resources.

As litigators begin to explore this electronic frontier, courts face similar obstacles in mapping this largely uncharted territory. Indeed, courts are hindered not only by technological obstacles to understanding the issues but also by the lack of any coherent body of law organizing the handful of relevant precedents in this largely discretionary realm of adjudication. Thus, in recent cutting edge decisions over discovery into an opponent's computer system, courts write as if on a blank slate, without acknowledging other decisions involving discovery of the same or analogous types of materials.[1]

1. *See, e.g.*, Fennel v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996); Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. Ct. App. 1996).

Compounding the difficulty courts confront in such discovery disputes is a unique mix of issues not present in other discovery contexts. On the one hand, courts must address how the liberal policy of open access to relevant information is to be applied in a world of changing technology where increasing amounts of relevant information will be found exclusively in computer storage media. Some of this information will be information that would have existed in hard copy in an earlier day and age. Yet other types of relevant information in computer storage media will be new types of evidence that were never traditionally available, but which may be invaluable fact-finding and truth-seeking tools.

On the other hand, discovery of computer-related information presents a novel mix of benefits and burdens. Although production of relevant information in machine-generated or machine-readable formats offers many efficiencies and enhancements to the fact-finding process, probing the depths of an opponent's computer system raises potential inefficiencies and dangers. In particular, inspection of an opponent's computer system and copying of an opponent's computer storage media may present business disruptions on a different scale than those encountered in responding to conventional discovery. Computer-related discovery may also raise the cost of the discovery process. Finally, such discovery may expose confidential or privileged materials residing in computer storage media.

This Article examines both the opportunities and the obstacles presented by discovery of evidence on the electronic frontier. Section II will map the technological terrain by introducing the nature of computer systems and computer storage media and by identifying the unique opportunities and hazards presented by discovery of such evidence. Section III will review the rules of procedure applicable to the discovery of computer-related evidence. In light of this procedural framework, Section IV will then review the types of cases in which computer-related discovery has been granted and denied. After setting these guideposts, Section V will then take a closer look at the benefits and burdens presented by this new form of discovery and will explore how courts should chart a course between competing interests in determining whether the discovery sought should be allowed and, if so, under what conditions. Finally, in light of the technological and legal landscapes, Section VI will review some unique procedural and practical obstacles presented by this new form of discovery in order to provide a roadmap for litigators considering whether to pursue evidence on the electronic frontier.

Through this journey, a paradox emerges. Existing discovery procedures seem to provide sufficient tools to resolve most, if not all, questions that arise in conducting computer-related discovery. Yet the technological complexity of computer-related discovery often demands that liti-

gants stretch the analytical framework of these procedural mechanisms beyond the limits of familiarity and, perhaps more importantly, often requires litigants both to consider using extraordinary procedures that are rarely used in civil litigation and also to conduct discovery under unusual precautions—precautions that safeguard against damaging disclosures of materials that are not properly the subject of discovery and precautions that ensure the fruits of that discovery will have evidentiary value in the litigation. Thus, although effective discovery of computer-related evidence may not require establishing new procedural rules, it does require mastering aspects of procedure that, for many, will seem quite new.

II. THE NATURE OF COMPUTER-RELATED EVIDENCE

A. NEW SOURCES OF DISCOVERY

Computers, and the various media in which computer-generated information is stored, provide a unique window into a company's memoranda, correspondence, strategies, business plans, product designs, analyses, projections, economic forecasts, statistics, and data. Computers may yield invaluable information in areas ranging from the composition of a company's labor force to the subjective motives of its officers and employees.[2] Computers also enable users to create summaries, indices, and methods of organizing vast quantities of information.

Not only do computers generate, sort, and store vast amounts of information useful to litigators, but they also provide a source of information that may not exist in paper form.[3] For example, some original documents, such as records regarding interbank financial transfers and retail and wholesale sales and inventory records, may reside in electronic storage.[4] Even where records once existed in hard copy, computers may store documents that no longer exist in that form.

In addition to generating hard copies of documents that are circulated for use, computers are also a source of information that may be translated to hard copy only partially, if at all. Take, for instance, drafts, spreadsheets, diaries, and e-mail. Similarly, some software applications enable users to record hidden text or comments that do not appear on the

2. *See* James H.A. Pooley & David M. Shaw, *Finding Out What's There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57, 60 (1995).

3. *See* John J. Dunbar, *When Documents are Electronic: Discovery of Computer-Generated Materials*, WASH. ST. BUS. NEWS, Apr. 1997, at 33-34; Peter V. Lacouture, *Discovery and the Use of Computer-Based Information in Litigation*, R.I.B.J., Dec. 1996, at 9 (estimating that 35% of corporate communications are never recorded on paper).

4. *See* Joseph J. Kashi, *How to Conduct On-Premises Discovery of Computer Records*, LAW PRAC. & MGMT., Mar. 1998, at 26 [hereinafter, Kashi, *How to Conduct On-Premises Discovery*].

screen and are not printed out.[5] Indeed, some operating systems maintain "system history files" that may retain such information as the dates on which documents were created or deleted or on which passwords were changed.[6] At a minimum, most systems retain the date and time that each file was last updated.[7] E-mail files may retain such valuable information as file names, comments appearing in headers or footers, indices, distribution lists, and the time the message was last accessed.[8] In addition, some software companies employ "version control programs," which maintain original versions of the source code in which programs are written and which store each new version of a program as deletions, insertions, and amendments to the original program. The resulting access to a source code's genealogy may be particularly useful in copyright, licensing, or warranty cases involving computer software.[9]

Because users do not expect the information entered into many of these formats ever to be put in hard copy, this information is likely to be less guarded and, therefore, more revealing and potentially damaging. Perhaps the best example of this phenomenon is the notoriously relaxed attitude of e-mail users whose spontaneity appears to be inspired by an instantaneous and seemingly private form of communication in which the presence of the interlocutor is not felt.[10] Similarly, a document's mere file name may be telling.[11]

Yet it is not only the unsuspecting computer novice who is susceptible to discovery of evidence residing in computer storage media. Even

---

5. *See* Andrew Johnson-Laird, *Smoking Guns and Spinning Disks*, COMPUTER LAW., Aug. 1994, at 1, 6; Pooley & Shaw, *supra* note 2, at 59.

6. *See* Susan E. Davis, *Elementary Discovery, My Dear Watson: Today's Evidence Comes in Bytes and Megabytes*, 16 CAL. LAW. 53, 54 (1996); *see, e.g.*, Momah v. Albert Einstein Med. Ctr., 164 F.R.D. 412, 418 (E.D. Pa. 1996) (discovery sought of a computer list files screen).

7. *See* Dunbar, *supra* note 3, at 34; Joseph M. Howie, Jr., *Electronic Media Discovery: What You Can't See Can Help (or Hurt) You*, TRIAL, Jan. 1993, at 70; Pooley & Shaw, *supra* note 2, at 59.

8. *See* James J. Marcellino & Anthony A. Bongiorno, *E-Mail is the Hottest Topic in Discovery Disputes*, NAT'L L.J., Nov. 3, 1997, at B10.

9. *See* Johnson-Laird, *supra* note 5, at 6-7.

10. *See, e.g.*, Lacouture, *supra* note 3, at 29; Heidi L. McNeil & Robert M. Kort, *Discovery of E-Mail: Electronic Mail and Other Computer Information Shouldn't Be Overlooked*, 56 OR. ST. BUS. BULL. 21-22 (1995); Marcellino & Bongiorno, *supra* note 8, at B10; Martha Middleton, *A Discovery: There May Be Gold in E-Mail*, NAT'L L.J., Sept. 20, 1993, at 1; Pooley & Shaw, *supra* note 2, at 63; Wendy R. Leibowitz, *E-Evidence Demands New Expert*, NAT'L L.J. Mar. 10, 1998, at A1, A13.

11. *See* Howie, *supra* note 7, at 70; Pooley & Shaw, *supra* note 2, at 59. Not only do such electronic communications provide evidence of matters referenced in the communications themselves and in the files containing the communications, but electronic communications are also spawning new genres of litigation for which they will have independent evidentiary significance. *See, e.g.*, Mark D. Robins, *Electronic Trespass*, COMPUTER LAW., July 1998, at 1.

sophisticated computer operators may leave electronic "footprints" when employing a computer system to perpetrate wrongdoing. For instance, a deleted system history file may indicate that a system has been tampered with and, thus, may undercut the inference that a document or diary entry was made on the date on which it purports to have been made.[12]

Thus, computers offer a window on a broader spectrum of information than is traditionally recorded in printed documents. In addition to expanding the breadth of available information beyond the four corners of printed documents, computers may add considerable depth to information that is recorded in printed documents. This depth can be provided by accessing earlier drafts of subsequently altered documents, as well as back-up copies of deleted files. These resources not only shed light on a document's genesis, but may also preserve the information contained in the document long after all hard copies have been lost.

Back-up copies of files may be available as a result of formal or informal preservation of information. Formally, companies often make timed back-ups of all of the information stored on a computer network at given points. These archival tapes may be preserved for short periods of time as a source of memory in the event of an emergency such as accidental deletion or loss of important data. Subsequently, such tapes may be recycled for further archiving or other use. Archival tapes may also be preserved for longer periods of time either because of government-mandated recordkeeping requirements or simply for purposes of historical preservation.[13] Informally, employees may make their own random back-up copies of files to guard against accidental deletion or system failure.[14] These back-ups may employ different file names. Indeed, different versions of an evolving document may be saved under different file names.

Consequently, there are several sources for retrieving deleted documents or drafts of documents. Archival tapes may contain final versions and drafts of documents that were subsequently deleted from the hard disk on a computer terminal or network file server. Similarly, copies or drafts of deleted documents may still be found on the hard disk of a com-

12. *See* Davis, *supra* note 6, at 54; *cf.* Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90, 120-21 (D. Colo. 1996) (finding that the absence of a footprint that would have been left if a disk had been wiped clean was probative of fact that disk had not been wiped clean).

13. *See* Alan Brill, *The Secret Life of Computer Data: How Valuable Evidence is Ignored by Litigators*, METROPOLITAN CORP. COUNS., Mar. 1994, at 32 [hereinafter, Brill, *The Secret Life of Computer Data*]; Patrick R. Grady, Comment, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give up More than Necessary*, 14 J. MARSHALL J. COMPUTER & INFO. L. 523, 531-43 (1996); Johnson-Laird, *supra* note 5, at 7-8; Joel B. Rothman, *Is it Really Gone? Data Recovery and Computer Discovery*, LEGAL TECH NEWSL., Jan. 1998, at 1, 8.

14. *See* Grady, *supra* note 13, at 531; Johnson-Laird, *supra* note 5, at 8.

puter terminal or network file server under different file names than the file that was deleted.

At a more esoteric level, because of the manner in which media for computer storage operate, word processing documents and e-mail messages that were deleted, erased, altered, or never saved may, nevertheless, be retrieved on the computer in their ultimate pristine form. This type of extraordinary retrieval is possible because of the nature of computer storage media. Specifically, computer files are stored in magnetic media, such as hard disks, floppy diskettes, and magnetic tapes, or in optical media, such as CD-ROMs. In magnetic media, computers store information by recording tiny changes in magnetic polarity in those media. By comparison, in optical media, computers store information by using a laser beam to burn pits into the smooth surface of a disk.[15]

No matter which medium is employed for storage, the information stored cannot be deleted in the sense that most people believe information to be deleted when they click on the "delete" option provided by their software programs. Rather, computers eliminate information that has been stored only by "overwriting" that information with new information to be stored in the same space.[16] When a user clicks on the delete option, the computer simply marks the file on the hard disk to be overwritten with new information. The file that was purportedly deleted, however, may not be overwritten for seconds, days, or even months.[17]

Not only do these "deleted" files continue to exist until overwritten, but, even when they are overwritten, the overwriting process may not wipe out the entirety of the original file. Specifically, portions of files may survive the overwriting process, because software programs generally allocate more space to a given file than is necessary. Thus, between the end of the memory block allocated to store a file and the "end of file" marker demarcating the end of whatever space is actually needed to store that file, there may lie remnants of files that have been partially overwritten.[18]

Similarly, reusing an archived magnetic tape may not eliminate all of the information earlier stored on it. If the new information archived consumes a smaller portion of the tape than the information previously archived, then some of the old information will be retained "off the end"

---

15. *See* Johnson-Laird, *supra* note 5, at 5.

16. *See* Dunbar, *supra* note 3, at 34; Johnson-Laird, *supra* note 5, at 5; Lacouture, *supra* note 3, at 9; Pooley & Shaw, *supra* note 2, at 64; Rothman, *supra* note 13, at 7; *see, e.g., Gates Rubber,* 167 F.R.D. at 90, 112 & 120 (discussing expert testimony regarding retrieval of deleted files and overwriting of deleted files).

17. *See* Davis, *supra* note 6, at 53; Johnson-Laird, *supra* note 5, at 5; McNeil & Kort, *supra* note 10, at 22; Pooley & Shaw, *supra* note 2, at 64; Rothman, *supra* note 13, at 7.

18. *See* Alan Brill, *A Lawyer's Place in Cyberspace*, AM. LAW. TECH. SUPP., Dec. 1995, at 10; Johnson-Laird, *supra* note 5, at 5-6.

of that part of the tape that remains active.[19]

Thus, a competent computer forensics technician can recover deleted files that have not been overwritten, remnants of files that have been partially overwritten, or "off the end" information from magnetic tapes.[20] To eliminate all such information from a computer's hard disk while maintaining the same software on the system one must use special programs designed to "wipe" all information out of storage or compress storage by rewriting existing information on "deleted" space so as to minimize the total space consumed by existing files.[21] Similarly, some software applications only save incremental changes to documents, thus, enabling a computer forensics technician to recover all deletions, amendments, and additions to documents.[22] Moreover, even broken hard disks may contain files that can be recovered.[23]

Not only can deleted files be recovered from these sources, but files that were never saved can sometimes be recovered. In particular, when a user sends a file to a printer, the computer will store a copy of that file in a "print buffer" from which the computer prints, while the user is able to continue using the original file. Even if the original file was never saved, the buffer copy may sometimes be recovered.[24]

These recovered files can be invaluable. Apart from providing information that may not exist in paper form, other circumstantial evidence surrounding recovered files can yield important clues. For instance, an individual's pattern of deleting certain types of information may shed light on that person's motive or state of mind.[25] The deletion of files before the time called for in a company's formal document retention program may yield similar inferences, as may the use of a special program to "wipe" a disk clean of deleted files.[26] Finally, remnants of files may provide information about the files that partially overwrite them. For instance, a document bearing one date whose file partially overwrites a document bearing a later date may have been deceptively antedated.[27]

---

19. *See* Johnson-Laird, *supra* note 5, at 9; Lacouture, *supra* note 3, at 9; Pooley & Shaw, *supra* note 2, at 64.

20. *See* Johnson-Laird, *supra* note 5, at 12; McNeil & Kort, *supra* note 10, at 22; *see, e.g.*, *Gates Rubber*, 167 F.R.D. at 90, 112, 120-21 (discussing retrieval of erased data from hard drives).

21. *See* Johnson-Laird, *supra* note 5, at 6; *see, e.g.*, *Gates Rubber*, 167 F.R.D. at 120-21 (discussing claim that computer disks had been wiped clean of all data).

22. *See* Johnson-Laird, *supra* note 5, at 6.

23. *See* Johnson-Laird, *supra* note 5, at 12-13; Pooley & Shaw, *supra* note 2, at 64-65.

24. *See* Brill, *A Lawyer's Place in Cyberspace*, *supra* note 18, at 10; Brill, *The Secret Life of Computer Data*, *supra* note 13, at 32.

25. *See* Pooley & Shaw, *supra* note 2, at 64.

26. *See* Grady, *supra* note 13, at 539-40; Johnson-Laird, *supra* note 5, at 12.

27. *But see* Fennel v. First Step Designs, Ltd., 83 F.2d 526, 533 (1st Cir. 1996) (plaintiff unsuccessfully sought discovery of defendant's hard drive to demonstrate that document

Not only do computers increase the pool of information-related evidence available to be culled by litigators, but computers also vastly enhance the power of litigators to process and store information-related evidence. For instance, computers enable one party to produce and another party to store mass quantities of documents in machine-readable form at greater convenience than with paper records.[28] When information is produced in this fashion, the discovering party can then employ computer technology to search for information by relevant categories such as titles, dates, topics, authors, and recipients, thus, enhancing the discovering party's ability to locate important information contained within the vast quantities of documents that are often produced in litigation.[29] The discovering party can search for files containing key words within a document or file or for terms contained in abstracts or indices.[30] Once key information is found, computers also facilitate processing that information by performing calculations, analyses, and projections.[31] The speed at which computers can process such information can reduce the amount of time spent culling through a massive production of documents.[32] Thus, computers can reduce the expense of litigation.[33]

In light of the many benefits of computer-related evidence, it is not surprising that such evidence is increasingly making a difference in reported decisions. One illustration can be found in the recent decision of *Sega Enterprises Ltd. v. MAPHIA*,[34] a case in the field of Internet law. In *Sega*, a video game manufacturer sued the operator of an electronic bulletin board for copyright and trademark infringement arising out of the distribution of unauthorized copies of the plaintiff's video games from the defendant's electronic bulletin board. The bulletin board in question,

---

was fraudulently antedated; plaintiff, however, was unable to articulate how this demonstration would be accomplished other than asserting that "there may be a way to determine the true date").

28. *See* Richard M. Long, Note, *The Discovery and Use of Computerized Information: An Examination of Current Approaches*, 13 PEPP. L. REV. 405, 406 (1986).

29. *See* David A. Nelson, Note, *The Impact of Computers on the Legal Profession*, 30 BAYLOR L. REV. 829, 832 (1978); Edward F. Sherman & Stephen O. Kinnard, *The Development, Discovery, and Use of Computer Support Systems in Achieving Efficiency in Litigation*, 79 COLUM. L. REV. 267, 269 (1979).

30. *See* Brill, *A Lawyer's Place in Cyberspace*, *supra* note 18, at 10; Barry E. Friedman, Note, *Computer Discovery in Federal Litigation: Playing by the Rules*, 69 GEO. L.J. 1465, 1483-84 & n.98; Haley J. Fromholz, *Discovery, Evidence, Confidentiality, and Security Problems Associated With the Use of Computer-Based Litigation Support Systems*, 1977 WASH. U.L.Q. 445, 459 (1977); Howie, *supra* note 7, at 71; Kashi, *How to Conduct On-Premises Discovery*, *supra* note 4, at 30; Sherman & Kinnard, *supra* note 29, at 269-71.

31. *See* Friedman, *supra* note 30, at 1467.

32. *See id.* at 1466-67; Nelson, *supra* note 29, at 832.

33. *See* Ellen G. Berndt, Note, *Discovery of Computerized Information*, 12 CAP. U. L. REV. 71, 77-78 (1982).

34. Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996).

a device consisting of computer storage media connected to telephone lines by a modem and operated by a computer, was employed by users to deposit and retrieve ("upload" and "download") unauthorized versions of the plaintiff's video games.[35] In proving that the defendant's operation of this bulletin board constituted contributory copyright infringement and direct trademark infringement, the plaintiff relied, in part, on evidence obtained pursuant to an *ex parte* seizure order. Under this order, the plaintiff was able seize the defendant's computer and memory devices and to copy the memory.[36] Among other things, the seized memory showed that the defendant tracked or had the ability to track user uploads and downloads of the plaintiff's video games, that the plaintiff's trademark was used in file descriptors to identify the game files contained in the bulletin board, and that the plaintiff's trademark was used to identify the file area on the bulletin board containing these games. This evidence helped to establish the defendant's knowledge of copyright infringement by users of the bulletin board, an element of contributory infringement, and the defendant's own use of the plaintiff's trademark, an element of trademark infringement.[37]

In such technologically focused cases, access to an opponent's computer memory has obvious benefits. But it is not just in the technology field that access to computer-related evidence can make a difference. Indeed, one survey of cases involving e-mail messages reported in the third quarter of 1997 found that employment issues predominated.[38] One example of the power of such evidence in employment law is *Strauss v. Microsoft Corp.*,[39] in which the defendant unsuccessfully moved to exclude from evidence certain e-mail messages that had been generated by one of the defendant's employees. The defendant argued that these messages, which contained inappropriate sexual and gender-related comments, were irrelevant and unfairly prejudicial. The court, however, found these messages directly relevant to the plaintiff's claim that she was discharged in retaliation for claiming that she was denied a promotion because of her gender. Specifically, the court concluded that the nature of these messages could lead a jury to believe that the defendant's proffered reason for failing to promote the plaintiff was not the true reason.[40] The court further found that any prejudice flowing from the admission of such evidence is "directly associated with the probative value

35. *See id.* at 927-29.

36. *See id.* at 927.

37. *See id.* at 933, 938.

38. *See* Samuel A. Thumma, *Employment Dominates 3d-Quarter E-Mail Cases*, INTERNET NEWSL.: LEGAL AND BUS. ASPECTS, Dec. 1997, at 10.

39. Strauss v. Microsoft Corp., 1995 WL 326492, at *1 (S.D.N.Y. 1995).

40. *See id.* at *4.

of the evidence."[41] The admission of such evidence cast a different light on claims that had been rejected by the Equal Employment Opportunity Commission as unsubstantiated.[42] The power of such evidence is readily apparent.

B. New Hazards of Discovery

Although computer systems are a potential gold mine to the discovering party, they are a potential mine field to the target of discovery. In addition to containing potentially damaging information, computer systems may store trade secrets and other proprietary or confidential materials, as well as communications to counsel, which are subject to the attorney-client privilege, and materials prepared in anticipation of litigation, which are subject to work product immunity.[43] Even databases employed by in-house and outside counsel may be targets for aggressive computer discovery.[44]

Moreover, a company that is overly aggressive in destroying computer records may find itself sanctioned or subjected to liability for spoliating evidence.[45] Indeed, the problem of spoliation is particularly thorny in the context of computer-related evidence given the routine destruction of information stored on computers, on the one hand, and given the dangers of fraudulent manipulation of evidence, on the other hand. Civil remedies for spoliation range from monetary fines to the striking of pleadings to the drawing of evidentiary inferences adversely to the sanctioned party to default judgments.[46] Some jurisdictions even recognize a cause of action for spoliation of evidence.[47]

The law of spoliation is not uniform. Thus, different jurisdictions take different positions on when a duty to preserve evidence arises. Sev-

---

41. *Id.* at *5.

42. *See id.* at *2-3.

43. *See* Fed. R. Civ. P. 26(c)(7) (trade secrets or confidential information may be protected from any discovery or may be discovered subject to protective conditions); Fed. R. Civ. P. 26(b)(1) (privileged matters not discoverable); Fed. R. Civ. P. 26(b)(3) (work product materials not discoverable without showing of substantial need and undue hardship).

44. *See* Grady, *supra* note 13, at 545-51; John T. Soma & Steven G. Austin, *A Practical Guide to Discovering Computerized Files in Complex Litigation*, 11 Rev. Litig. 501 (1992).

45. *See* Dunbar, *supra* note 3, at 39; Grady, *supra* note 13, at 539-43; Kashi, *How to Conduct On-Premises Discovery*, *supra* note 4, at 26; McNeil & Kort, *supra* note 10, at 23; Rothman, *supra* note 13, at 8; *see generally* Matthew J. Bester, Comment, *A Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence*, 6 Comm. L. Conspectus 75 (1998).

46. *See* Bester, *supra* note 45, at 81-83; Jamie S. Gorelick, et al., Destruction of Evid. § 13.2 (1989).

47. *See* Bester, *supra* note 46, at 83-84; Gorelick, *supra* note 46, § 4.1-4.23; *see generally* John K. Stipancich, Note, *The Negligent Spoliation of Evidence: An Independent Tort Action May Be the Only Acceptable Alternative*, 53 Ohio St. L.J. 1135 (1992).

eral courts, however, have found that such a duty arises when it is reasonably foreseeable that the evidence in question will be relevant to a lawsuit—even if the litigation has not yet commenced.[48] Courts also require different degrees of culpability to implement different remedies. For instance, although most courts require intentional conduct to draw an inference adversely to the spoliator, some courts only require negligent conduct, and most courts will impose other sanctions even where a party only acts negligently in destroying evidence.[49]

In the context of computer-related evidence, in cases where the evidence is directly at issue, a party's willful destruction can lead to outcome-determinative sanctions. For instance, in cases involving copyright protection for computer source code, courts may default a party who deliberately destroys source code needed for the court to determine if there has been unlawful copying.[50] Similarly, in other contexts where computer-related evidence has been relevant, a party's willful destruction has led to outcome-determinative sanctions.[51]

Although these decisions represent judicial vigilance against the fraudulent manipulation of computer-related evidence, courts have also shown sensitivity to the fact that some evidence maintained in computer storage media may be lost through ordinary, non-culpable use of computer systems. Thus, in one discrimination case where the defendant's personnel director had deleted a paragraph in a draft evaluation of the plaintiff and where the deletion occurred after the plaintiff had filed an administrative complaint, the court, nonetheless, found no duty to pre-

48. *See* GORELICK, *supra* note 46, §§ 2.9, 3.12, 13.3.

49. *See id.* §§ 2.8, 3.11 (main text and 1997 Supp.).

50. *See* Cabinetware Inc. v. Sullivan, 1991 WL 327959, at *4-*5 (E.D. Cal. 1991) (imposing default judgment for intentional destruction of source code); Computer Assocs. Int'l v. Am. Fundware, Inc., 133 F.R.D. 166, 170 (D. Colo. 1990) (same); *but see* Mohawk Mfg. Supply Co. v. Lakes Tool Die & Eng'g, Inc., 1994 WL 85979 (N.D. Ill. 1994) (holding that plaintiff acted prematurely in bringing cause of action for spoliation of computer drawings alleged to constitute infringements of plaintiff's copyrights and misappropriations of plaintiff's trade secrets, where underlying action was still ongoing and where, accordingly, plaintiff could not demonstrate prejudice to its ability to prosecute that action as result of spoliation). Ironically, in the *Computer Assocs.* case, the court ultimately removed the default judgment entered against the defendant, because the court learned that the plaintiff, too, had lost certain computer evidence, thus, demonstrating the ubiquitous and unpredictable nature of the spoliation issue in this context. *See* Computer Assocs. Int'l v. Am. Fundware, Inc., 831 F. Supp. 1516, 1531 (D. Colo. 1993).

51. *See* Stanton v. Nat'l R.R. Passenger Corp., 849 F. Supp. 1524, 1528 (M.D. Ala. 1994) (where defendant failed to preserve computer tape indicating speed of train at issue at time of accident, in violation of defendant's policy, court drew inference adversely to defendant so as to deny defendant's motion for summary judgment); Wm. T. Thomson Co. v. Gen. Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984) (default judgment, striking of pleadings, and monetary sanctions imposed on defendant who willfully destroyed evidence).

serve all drafts of internal memoranda.[52] Similarly, where a party destroys computer-related evidence pursuant to a routine policy or pursuant to ordinary operations and where the discovering party fails to take actions that would prevent that destruction, some courts have refused to impose sanctions for spoliation.[53] Indeed, because materials in computer storage media are often deleted, purged, or overwritten in the ordinary course of business and pursuant to established policies, it may often be difficult to establish the requisite level of culpable conduct required by some jurisdictions.[54]

One further aspect of computer-related evidence that may diminish the severity of sanctions for spoliation is the possibility of recovering deleted files. If such files can be recovered, there may be no prejudice to the discovering party and, hence, no basis for sanctions—at least of the outcome-determinative variety.[55]

A party who has destroyed computer-related evidence or who has allowed such evidence to be destroyed, however, should not take too much comfort in these decisions. In every case where a duty to preserve has attached, there is a real danger that the conduct of the spoliating

52. *See* McGuire v. Acufex Microsurgical, Inc., 175 F.R.D. 149, 155-56 (D. Mass. 1997).

53. *See* Stricklen v. Fed. Aviation Admin., 32 F.3d 572, 1994 WL 390001, at *2 (9th Cir. 1994) (table; text in Westlaw) (denying sanction for agency's destruction of radar data pursuant to agency policy where data would have been preserved under policy if petitioner had reported incident in timely fashion); Allen Pen Co. v. Springfield Photo Mount Co., 653 F.2d 17, 23-24 (1st Cir. 1984) (where plaintiff attempted to show injury from price discrimination by claiming reduced profits relative to competitors, court refused to infer such injury from defendant's destruction of computer-generated evidence of sales to plaintiff's competitors; although evidence was destroyed after commencement of case and after its identification in interrogatory answers, destruction was not result of "bad faith" or "consciousness of a weak case" and lost evidence would not itself have established competitor's profits but, rather, would only have provided starting point); Chidichimo v. University of Chicago Press, 681 N.E.2d 107, 110-11 (Ill. 1997) (denying sanction for defendant's routine purging of computer data where plaintiff failed to take reasonable steps to ensure preservation and protect against routine destruction).

54. *See, e.g., McGuire*, 175 F.R.D. at 155-56 (finding culpable conduct lacking where defendant's personnel director deleted paragraph in employee's evaluation by supervisor); Williams v. CSX Transp., Inc., 925 F. Supp. 447, 452 (S.D. Miss. 1996) (finding requisite level of bad conduct not present to warrant drawing adverse inference to party who destroyed evidence from computer), *aff'd*, 139 F.3d 899 (5th Cir. 1998) (table); ABC Home Health Servs., Inc. v. Int'l Bus. Machs. Corp., 158 F.R.D. 180, 182-83 (S.D. Ga. 1994) (finding requisite level of bad conduct lacking to warrant entering default judgment against party who destroyed documents on computer disk); *see generally* GORELICK, *supra* note 46, at § 2.22(H) (1997 Supp.); *but see* Grady, *supra* note 13, at 539-40 (suggesting that, if only unfavorable documents are destroyed, court may find that party used record retention policy in furtherance of scheme to destroy evidence).

55. *See, e.g., McGuire*, 175 F.R.D. at 156 (no prejudice to discovering party where deleted paragraph of document was recovered and immediately turned over to discovering party, who was afforded full opportunity to explore circumstances of deletion).

party will be found culpable.[56] In addition, even where outcome-determinative sanctions are not imposed, a court may allow evidence of the destruction to go before the jury as evidence of the spoliating party's intent and may even draw a presumption against the spoliator.[57]

Finally, although seemingly less egregious than the actual destruction of evidence, the failure to produce computer-related evidence in discovery can be equally harmful to a party's case.[58] Indeed, several courts have responded to a party's failure to produce computer-related evidence with outcome-determinative rulings.[59] Even where the sanction im-

56. *See* GORELICK, *supra* note 46, § 2.6 (noting that attempted destruction may, by itself, support inference that spoliator had wrongful motive).

57. *See McGuire*, 175 F.R.D. at 156-57 (holding deletion of paragraph of document may be relevant on question of bona fides of defendant's internal investigation of plaintiff's complaint and may be seen as implied admission); *ABC Home Health Servs.*, 158 F.R.D. at 183 (imposing presumption against spoliator); *see generally* GORELICK, *supra* note 46, 2.4.

58. *See* Marcellino & Bongiorno, *supra* note 8, at B10.

59. *See* Ryan v. Board of Police Comm'rs, 96 F.3d 1076, 1081-84 (8th Cir. 1996) (regarding officer's conduct during arrest, district court committed reversible error by admitting evidence of subsequent arrest, where defendants learned of subsequent arrest through access to database and where defendants failed to disclose documents relating to access to database in response to discovery request seeking such documents); Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993) (upholding district court order precluding defendant from introducing evidence in defense of counterclaim for broker's commissions and entering default judgment in favor of defendant on counterclaim where plaintiff failed to produce raw data contained in computer database, where defendant had requested production of "all documents relating to . . . calculations of . . . commissions," and where magistrate judge had ordered plaintiff to produce summaries of commissions, as well as "underlying documents;" appellate court rejected argument that raw data did not fall within meaning of "documents"); Shu-Tao Lin v. McDonnell Douglas Corp., 574 F. Supp. 1407, 1412-13 (S.D.N.Y. 1983) (granting motion to set aside verdict, *inter alia*, because of failure to make adequate pretrial disclosure of computer methodology and data that expert would rely on at trial), *aff'd in part, rev'd in part*, 742 F.2d 45 (2d Cir. 1984) (holding trial court's use of remittitur to be improper, because errors relating to expert testimony infected entire damages award); Am. Bankers Ins. Co. v. Caruth, 786 S.W.2d 427, 434-37 (Tex. Ct. App. 1990) (upholding trial court's order striking pleadings and entering default as sanctions for failure to produce information contained in computer database); *see also* Cook v. Rockwell Int'l Corp., 907 F. Supp. 1460 (D. Colo. 1995) (nonparty who entered into stipulated order requiring production of documents held in contempt for, *inter alia*, failing to identify computer tapes containing certain documents and failing to produce requested database); *but see* Baker v. Gen. Motors Corp., 86 F.3d 811, 816-17 (8th Cir. 1996) (reversing outcome-determinative sanction as too severe for defendant's belated production of computer summaries), *rev'd in part on other grounds*, 118 S. Ct. 657 (1998); E.E.O.C. v. Gen. Dynamics Corp., 999 F.2d 113, 116-17 (5th Cir. 1993) (reversing lower court's exclusion of plaintiff's expert testimony as sanction for failure to produce database relied on by expert in form of computer tape in response to order requiring production of all tangible things relied on by expert; lower court's order did not clearly require production of tapes); Cullins v. Heckler, 108 F.R.D. 172 (S.D.N.Y. 1985) (reversing magistrate judge's order of sanctions for failure to produce statistical information in response to interrogatories, where, although producing party would later state that a computer run dealing with some of requested information was in process and could be adjusted to provide responsive information, there was no evi-

posed is not dispositive of the case, it may financially burden the party who failed to produce.[60] Similarly, a party may also face exposure to sanctions from the negligent production of incomplete, outdated, or misleading computer data.[61]

III. THE PROCEDURAL FRAMEWORK GOVERNING THE DISCOVERY OF ELECTRONIC EVIDENCE

Before reviewing the types of cases where computer-related materials have been subjects of discovery, this Section will briefly sketch the procedural framework that governs these determinations. As with more traditional forms of discovery, the pertinent concepts are relevance, privilege, immunity, confidentiality, and burden. These concepts are all addressed by the Federal Rules of Civil Procedure, and there can be no doubt that those rules apply to the discovery of computer-related materials. Although the rules of procedure generally provide for liberal discovery of computer-related information, the rules also provide judges with broad discretion to curtail efforts that are not reasonably calculated to lead to the discovery of admissible evidence, that are overly broad or unduly burdensome, or that jeopardize confidential or privileged matter. Rule 26 of the Federal Rules of Civil Procedure defines the scope of discoverable materials to include "any matter . . . which is relevant to the subject matter involved in the pending action . . . including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter."[62] If there is any doubt as to whether the scope of discoverable subject matter under Rule 26 is sufficiently broad to include computer-related materials, Rule 34 of the Federal Rules of Civil Procedure specifies that a party may request the production of documents or "other data compilations from which information can be obtained, translated, if necessary, by respondent through detection devices into reasonably usable form . . . ."[63]

---

dence that, at time when interrogatories were initially answered, producing party knew of projected computer run or otherwise deceitfully withheld information).

60. *See, e.g.*, Nat'l Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 558-59 (N.D. Cal. 1987) (where defendant failed to produce computer data and destroyed other documents, court imposed as sanctions all fees and costs incurred by plaintiffs in connection with depositions, discovery, preparation, the hearing and other efforts related to motion for sanctions, as well as $15,000 fine to be paid to court).

61. *See* EEOC v. Sears, Roebuck & Co., 114 F.R.D. 615, 626-27 (N.D. Ill. 1987) (plaintiff required to compensate defendant for attorney's fees incurred as result of plaintiff's negligence in producing computer printouts containing incorrect, incomplete, and misleading data in response to defendant's discovery requests).

62. FED. R. CIV. P. 26(b)(1).

63. FED. R. CIV. P. 34(a).

The Advisory Committee that added this passage to the Rules in 1970 noted that the language "makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form." Although, the Advisory Committee noted that, "[i]n many instances, this means that respondent will have to supply a print-out of computer data," the Advisory Committee also contemplated that "the discovering party [may] need[ ] to check the electronic source itself. . . ."[64] According to Wright & Miller, this provision of Rule 34 brought the discovery process into the realm of computer technology.[65] Thus, by 1985, one court was able to conclude: "It is now axiomatic that electronically stored information is discoverable . . . if it otherwise meets the relevancy standard prescribed by the rules, although there may be issues in particular cases as to the form of what must be produced."[66] Accordingly, the *Manual for Complex Litigation* advises: "Any discovery plan must address . . . the search for, location, retrieval, form of production and inspection, preservation, and use at trial of information stored in mainframe or personal computers or accessible 'online.'"[67]

Yet if the liberal rules for discovery clearly apply to computer-related materials, so too do the various restrictions on discovery.[68] First, for information to be discoverable, it must be "reasonably calculated to

64. FED. R. CIV. P. 34(b)(1) advisory committee note, 48 F.R.D. 487, 527 (1970). Correspondingly, at least one court has ruled that information contained in electromagnetic media must be produced in response to a request under that state's public records statute. *See* Birmingham News Co. v. Perry, 21 MEDIA L. REP. 2125 (Ala. Cir. Ct. 1993).

65. 8A CHARLES A. WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE: CIVIL § 2218 (2d ed. 1994).

66. Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) (citation omitted); *accord* Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1382-83 (7th Cir. 1993) ("[T]he Advisory Committee notes to the 1970 amendment of Federal Rule of Civil Procedure 34 make clear that computer data is included in Rule 34's description of documents. Therefore, Crown Life's failure to make the raw data available [in response to court order requiring production of "underlying documents" supporting computer entries] amounts to a violation of discovery orders."); Santiago v. Miles, 121 F.R.D. 636, 640 (W.D.N.Y. 1988) ("A request for raw information in computer banks is proper and the information is obtainable under the discovery rules.") (collecting authority); *see also In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, *1 (N.D. Ill. 1995) (holding e-mail to be discoverable under FED. R. CIV. P. 26(b) & 34 in accordance with same rules governing discovery of tangible, written documents); Seattle Audobon Soc'y v. Lyons, 871 F. Supp. 1291, 1308 (W.D. Wash. 1994) (noting that earlier order had required production of electronic communications), *aff'd*, 80 F.3d 1401 (9th Cir. 1996).

67. FEDERAL JUDICIAL CENTER, MANUAL FOR COMPLEX LITIGATION § 21.446, at 79 (3d ed. 1995).

68. *See generally* 8A WRIGHT, *supra* note 65, § 2218, at 451.

lead to the discovery of admissible evidence."[69] Second, the scope of discoverable materials does not include materials that are privileged.[70] Third, work product materials that were prepared in anticipation of litigation can only be discovered where the discovering party can show both "substantial need" for the materials and that it is "unable without undue hardship to obtain the substantial equivalent of the materials by other means."[71] Fourth, "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense," a court may issue a protective order that precludes the discovery sought altogether, limits the discovery sought, or provides that trade secret or confidential information not be revealed or be revealed only in a specified manner.[72] Finally, under the Federal Rules, the court can limit the "frequency or extent of use of the discovery methods" if the court determines, among other things, either that "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive" or that "the burden or expense of the proposed discovery outweighs its likely benefit. . . ."[73]

Indeed, these restrictions on the scope of permissible discovery may apply with particular force in the context of computer-related materials. Thus, in commenting on the expanded definition of the term "document" in the 1970 changes to the Rules, the Advisory Committee made clear that courts can exercise their discretion under Rule 26(c) to protect responding parties from undue burden or expense. In particular, where a party seeks to inspect the electronic source of a respondent's computer evidence, courts "may protect [such a] respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs."[74]

In short, the Federal Rules of Civil Procedure authorize broad discovery of computer-related information, while affording many protections against unreasonably intrusive discovery of such materials. The general dictates of the Rules, however, leave much to the discretion of the trial court. Notably, the Rules do little to address particular problems presented by specific technological phenomena or to resolve the tension presented by those cases in which the potential benefits and burdens of computer-related discovery are both at their heights.

---

69. FED. R. CIV. P. 26(b)(1).

70. *Id.*

71. FED. R. CIV. P. 26(b)(3).

72. FED. R. CIV. P. 26(c)(1), (4) & (7).

73. FED. R. CIV. P. 26(b)(2).

74. FED. R. CIV. P. 34(b)(1) advisory committee note, 48 F.R.D. 487, 527 (1970).

IV. AN OVERVIEW OF CASES INVOLVING THE DISCOVERY OF COMPUTER-RELATED MATERIALS

Perhaps the first set of challenges to be encountered in approaching electronic discovery is to determine whether a particular type of case is a good candidate for such discovery and to determine which rules governing access to and protection of information are likely to apply to computer materials that are inviting targets for such discovery. This Section examines which types of computer-related materials have been subject to any particular extent of discovery in particular circumstances. Although any generalizations are hazardous in this inherently fact-specific area of the law, this Section divides the cases into four categories to impose some order on this inchoate but diverse body of contextually dependent decisions: (1) cases in which computer-related materials pertain to testimony that will be offered at trial; (2) cases involving computer-related materials whose discovery will facilitate trial preparation; (3) cases involving computer-related materials that have independent evidentiary significance; and (4) cases in which a party has sought discovery into the nature of the opposing party's computer-storage media.

A. Computer-Related Materials Pertaining to Trial Testimony

At one far end of the spectrum, courts have consistently allowed a party broad discovery into computer-related materials that will be relied on by the respondent at trial. These cases arose under the 1970 amendments to Rule 26 of the Federal Rules of Civil Procedure, which allowed a party to serve interrogatories requiring the identification of expert witnesses to be called at trial, a statement of the subject matter of the anticipated expert testimony, and a summary of the grounds for each opinion.[75] Under this version of Rule 26, to obtain additional expert discovery, a party was required to obtain leave of the court, which could impose restrictions as to the scope of any such discovery.[76] In addition, under the 1970 version of Rule 26, a party could generally obtain discovery of a non-testifying expert only if the party could show "exceptional circumstances under which it is impracticable for the party seeking discovery to obtain facts or opinions on the same subject by other means."[77] In cases that arose under this rule and that involved computer-related materials to be relied on by experts, courts allowed broad discovery, including into a variety of background materials related to computer evidence to be relied upon by an expert. Although this judicial tendency emerged in cases involving materials to be relied upon by experts, the approach of these cases may well be applied to computer-related materi-

75. *See* Fed. R. Civ. P. 26(b)(4)(A)(i) (1970 amendments; amended further in 1993).
76. *See* Fed. R. Civ. P. 26(b)(4)(A)(ii) (1970 amendments; amended further in 1993).
77. Fed. R. Civ. P. 26(b)(4)(B) (1970 amendments; amended further in 1993).

als pertaining to other testimonial or documentary evidence to be introduced at trial.

Early cases focused on a party's need to access sufficient computer-related materials to prepare an effective cross-examination. For example, in *City of Cleveland v. Cleveland Elec. Illuminating Co.*,[78] the defendant sought to compel pretrial production of data and calculations underlying the conclusions contained in the plaintiff's expert reports. The court granted the motion to compel. In explaining this ruling, the court drew upon several authorities addressing the disclosure of computer-related materials in the criminal context. The court found that these "authorities . . . have consistently recognized the discoverability of underlying data as well as plans and programming methods from which a particular system or computer study emerged."[79] From these authorities, the court determined that, whenever a witness will testify based upon computerized data, effective cross-examination may be impaired due to "the difficulty of knowing the precise methods employed in programming the computer as well as the inability to determine the effectiveness of the persons responsible for feeding data into the computer."[80] Therefore, the court concluded that, wherever expert reports are based on complex data, calculations, and simulations not disclosed by the reports themselves, discovery of such matters will be essential to effective cross-examination of the experts at trial.[81]

The need to assure affective cross-examination was similarly the focus of *Fauteck v. Montgomery Ward & Co.*,[82] a gender discrimination case. In *Fauteck*, the court required production of a database storing the defendant's personnel records, which was created to serve as the foundation for the defendant's expert trial testimony. Although the defendant argued that the database reflected legal judgments made in the course of its compilation, therefore placing it within the protection of work product immunity, the court found that such materials should be disclosed under Rule 26 "to assure competent cross-examination of trial experts."[83] The court, however, broadened the discovering party's rights under Rule 26 by allowing this discovery before the time for expert discovery under Rule 26. The court did so, because it found that the disclosure would "materially advance this litigation without seriously prejudicing [the] defendant."[84]

78. City of Cleveland v. Cleveland Elec. Illuminating Co., 538 F. Supp. 1257 (N.D. Ohio 1980).

79. *Id.* at 1266.

80. *Id.* (quoting United States v. Cepeda, 577 F.2d 754, 760-61 (1st Cir. 1978)).

81. *See id.* at 1267.

82. Fauteck v. Montgomery Ward & Co., 91 F.R.D. 393 (N.D. Ill. 1980).

83. *Id.* at 398.

84. *Id.* at 398.

In allowing discovery of computer-related materials to assure effective cross-examination of experts, courts have allowed access to a variety of background materials. For example, in *Williams v. E.I. du Pont de Nemours & Co.*,[85] a Title VII case, the court required production of a database that the plaintiff's expert compiled from records produced by the defendant—a database on which the plaintiff's testifying expert would rely in showing discriminatory motive through a statistical pattern. Yet, not only did the court require production of the database, but it also required the plaintiff to produce codebooks, a user's manual, and all documents used in encoding the database. In particular, the court found that "access to the Codebooks and users manual used to analyze the raw data and arrive at [the expert's] final report is necessary for effective cross-examination and to establish the accuracy of the data output."[86] The court refused, however, to require production of all documents relating to the programs used to create the database or of all print-outs generated through the use of the database, as the court found such discovery to be overly broad, beyond the proper scope of relevance, as well as likely to reveal alternative methods of analyses or alternative computer programs that were deemed beyond the proper scope of expert discovery under Rule 26.[87] On the whole, however, the *Williams* court found that the computer-related nature of the discovery materials in question demanded a liberal application of the discovery rules.

Similarly, in *Pearl Brewing Co. v. Jos. Schlitz Brewing Co.*,[88] the court even allowed discovery from a non-testifying expert, although, as in *Williams*, the *Pearl Brewing* court drew the line at discovery of alternative methods of analysis. *Pearl Brewing* was an antitrust case in which the plaintiff's testifying economics expert planned to rely on an econometrics model in one computer program, as well as on a series of computer programs that would be used to enable the testifying expert to determine the plaintiff's volume losses in each applicable market or submarket. All of these programs were developed by the plaintiff's non-testifying computer experts to test data and simulate market conditions. In these circumstances, the court required production of all system documentation revealing the details of these computer programs. In addition, however, the court found exceptional circumstances to justify allowing the defendant to depose the non-testifying computer experts as to the computer model and programs to be relied on by the testifying expert. Because the defendant needed to understand fully the nature of these computer programs, in order to prepare an effective cross-examina-

85. Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648 (W.D. Ky. 1987).

86. *Id.* at 651 (citations omitted).

87. *See id.*

88. Pearl Brewing Co. v. Jos. Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976).

tion of the plaintiff's testifying expert, and because only the non-testifying experts could interpret the computer programs to be used by the testifying expert, there were exceptional circumstances warranting discovery of the non-testifying experts.[89] The court, however, refused to allow the defendants to depose non-testifying experts on the subject of alternative models. The court ruled that, although the testifying expert had only limited knowledge of how the computer programs on which he would rely were created, the testifying expert would nonetheless be a sufficient source of discovery for the ideas and economic substance of the models on which he would rely and of rejected models. The court found the testifying expert to be a sufficient source for discovery of these ideas and models, because they originated with the testifying expert.[90] In light of the discovery permitted, however, the *Pearl Brewing* court takes the liberal spirit of *Fauteck* and *Williams* one step further—namely, by allowing some discovery from non-testifying experts based on the computer-related subject matter of the testifying expert's testimony.

Finally, the court even allowed discovery of alternative analyses in *Bartley v. Isuzu Motors Ltd.*[91] In *Bartley*, a products liability plaintiff retained an expert witness to conduct computer simulations of an automobile accident. The defendant sought disclosure of all simulations that the plaintiff's expert had run before arriving at the final simulation to be used at trial. The plaintiff, however, sought to limit the defendant to those computer reconstructions in which the results actually conformed to the known physical information corresponding to the accident in question. The court refused to impose such a restriction.

> When one party seeks to present a computer study, in order to defend against the conclusions that are said to flow from these efforts, the discovering party not only must be given access to the data that represents the computer's work product, but he also must see the data put into the computer, the programs used to manipulate the data and produce the conclusions, and the theory or logic employed by those who planned and executed the experiment.[92]

Many of these expert-related computer materials will now more plainly be discoverable under the Federal Rules of Civil Procedure. In 1993, Rule 26 of the Federal Rules of Civil Procedure was amended to require pretrial disclosure of, among other things, "all opinions to be expressed [by expert witnesses] and the basis and reasons therefor; [and] the data or other information considered by the witness in forming the opinions. . . ."[93] In light of these cases under the former version of Rule

89. *See id.* at 1138-39.
90. *See id.* at 1134-41.
91. Bartley v. Isuzu Motors Ltd., 151 F.R.D. 659 (D. Colo. 1993).
92. *Id.* at 660 (citations omitted).
93. FED. R. CIV. P. 26(a)(2)(B).

26, there can be no doubt that a party must disclose the computer-related materials that the party's expert considers in forming opinions, because these materials will fall within the meaning of "data or other information" that must be disclosed under the new version of the rule.[94] In addition, these cases indicate that the scope of discovery into such computer-related materials must be sufficiently broad to afford the discovering party with an adequate understanding of that technology in order to have a fair and effective trial presentation. Indeed, if a court denies access to such materials, the court may commit outcome-determinative error.[95]

B. Computer-Related Materials Whose Discovery Will Facilitate Trial Preparation

In addition to requiring parties to produce computer-related materials that will form the basis of trial testimony, courts will also require production of materials that will facilitate trial preparation, including, in some instances, databases that attorneys have prepared in connection with litigation. At the least controversial level, where one party seeks production of machine-readable data that has already been disclosed or of a database of documents that have already been produced in hard copy, some courts will require such production at the expense of the discovering party, in order to facilitate trial preparation.[96] By contrast, where an attorney has maintained a database to facilitate trial preparation, courts have divided over whether to protect that attorney's selection

94. *See* 7 James W. Moore, et al., Moore's Federal Practice § 34.12[c], at 34-42 (Rel. No. 113 1997).

95. *See* Shu-Tao Lin v. McDonnell Douglas Corp., 574 F. Supp. 1407, 1412-13 (S.D.N.Y. 1983) (granting motion to set aside verdict, *inter alia*, because of failure to make adequate pretrial disclosure of computer methodology and data that expert would rely on at trial), *aff'd in part, rev'd in part*, 742 F.2d 45 (2d Cir. 1984) (holding trial court's use of remittitur to be improper, because errors relating to expert testimony infected entire damages award); *but see* Perma Research & Dev. v. Singer Co., 542 F.2d 111, 115 (2d Cir.), *cert. denied*, 429 U.S. 987 (1976) ("While it might have been better practice for opposing counsel to arrange for the delivery of all details of the underlying data and theorems employed in these simulations in advance of trial . . . , [t]he trial judge did not abuse his discretion in allowing the experts to testify as to this particular basis for their ultimate conclusion . . . .").

96. *See* Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1161-62 (E.D. Pa. 1980) (requiring respondent's expert to create computer readable tape containing same information that respondent had produced in printed form in answering interrogatories); Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 221-22 (W.D. Va. 1972) (requiring production of computer cards or tapes and printouts of W-2 form information); *see also* Donaldson v. Pillsbury Co., 554 F.2d 825, 832 (8th Cir.) (suggesting that lower court reconsider, on remand, whether plaintiffs should be allowed request for machine-readable version of data that had been produced in hard copy), *cert. denied*, 434 U.S. 856 (1977).

of documents from discovery under the work product doctrine.[97] As Wright & Miller have observed, production of such litigation databases will become more likely as the process of selecting the data becomes increasingly mechanical or as the ability of counsel increases to redact fields inserted in the database to reflect legal analyses or strategic judgments.[98] Yet the more that a database's design reflects judgments of counsel relating to anticipated litigation, such as by selecting portions of documents for inclusion based on judgments of counsel as to their importance to the litigation, by arranging documents based on strategic priorities, and by using indices that relate to litigation needs, the more likely that database is to be protected from discovery by work product immunity.[99] Moreover, a purely legal database has been held to be non-discoverable subject matter, without even consideration of the work product

97. *Compare In re* Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844, 846 (8th Cir. 1988) (computer tape prepared by counsel and reflecting counsel's selection of categories of information was factual work product that was discoverable because information was useful and would involve duplication of effort and delay and expense to replicate without production of computer tape), *with* Santiago v. Miles, 121 F.R.D. 636 (W.D.N.Y. 1988) (computer printouts of raw data and statistical analyses protected as opinion work product because of participation of counsel, although discovering party could design computer request to seek raw data; but computer printouts prepared with pending litigation in mind were not protected as work product because primary motivation behind preparation was for use in normal course of business), *with* Indiana State Bd. of Public Welfare v. Tioga Pines Living Ctr., 592 N.E.2d 1274 (Ind. Ct. App. 1992) (computer simulations reflecting possible Medicaid reimbursement methodologies that Department of Public Welfare considered but did not adopt at time shortly after Department had been sued protected as work product, because primary purpose in creating methodologies was to assist litigation), *with* State of Colorado v. Schmidt-Tiago Constr. Co., 108 F.R.D. 731, 734-35 (D. Colo. 1985) (party opposing discovery failed to sustain burden of showing that computer printouts predating lawsuit were prepared in anticipation of litigation rather than in ordinary course of business; no work product protection afforded), *and with* Maloney v. Sisters of Charity Hosp., 165 F.R.D. 26, 30-31 (W.D.N.Y. 1995) (computer printouts containing statistical information pertaining to proposed reduction in force were prepared at counsel's direction in anticipation of litigation and were protected from disclosure as fact work product; discovering party failed to overcome protection by showing substantial need and inability to obtain substantial equivalent from alternative sources), Shipes v. BIC Corp., 154 F.R.D. 301, 309 (M.D. Ga. 1994) (in-house legal department's database protected as work product where it "would be impossible to separate [work product] from non-work product data" and where an "entire system arguably constitutes work product"), *In re* Conticommodity Servs., Inc., Secs. Litig., 123 F.R.D. 574, 578 (N.D. Ill. 1988) (computer runs showing various tax calculations were protected as work product because they were prepared for discussion of litigation strategy), *In re* IBM Peripheral EDP Devices Antitrust Litig., 5 Comp. L. Serv. Rtpr. 879 (N.D. Cal. 1975) (computerized trial support system consisting of summaries and analyses of certain documents that had been produced in discovery protected as work product), *and Nat'l Union*, 494 F. Supp. at 1259 (indicating that data stored and arrayed in particular way that may reveal trial strategy would be protected as work product).

98. *See* 8A WRIGHT, *supra* note 65, § 2218, at 461.

99. *See* Soma & Austin, *supra* note 44, at 519-20.

doctrine.[100]

C. Computer-Related Materials That Have Independent Evidentiary Significance

Although one might expect some judicial reluctance to allow a party to discover computer-related materials that were prepared in anticipation of litigation, courts have also divided over the extent to which a party can obtain discovery of computer-related materials that may have independent evidentiary significance. Because discovery of computerized record-keeping presents unique burdens relating to the cost of compliance, to the potentially confidential and privileged nature of materials residing on computer systems, and to the potential disruption to business operations that rely on computer systems for day-to-day performance, courts are grappling with where to draw the line circumscribing the extent of required disclosure of such materials. This Part traces the types of computer-related discovery that courts have allowed and denied. The question of how to analyze various burdens claimed to be entailed by discovery of computer-related materials is reserved for Section V.

At the least controversial level, where information residing in computer storage media necessarily has some obvious evidentiary significance, courts have allowed discovery, absent some overriding consideration such as privilege or undue burden. For example, courts have allowed discovery into computer-related materials in cases where rights to software programs are at issue or where the performance of software or hardware is at issue.[101]

---

100. *See* Indiana Coal Council v. Hodel, 118 F.R.D. 264, 265-68 (D.D.C. 1988).

101. *See, e.g.*, Haseotes v. Abacab Int'l Computers, Inc., 120 F.R.D. 12, 15 (D. Mass. 1988) (in action where plaintiff pressed various claims relating to defendant's alleged failure to perform under agreement whereby defendant was to transfer computer technology and employees to new corporations to be controlled by plaintiff, plaintiff was held entitled to inspect computer goods that were marketed by defendant; because characteristics of equipment's capabilities would enable plaintiff to determine marketability of product, characteristics were relevant to determining whether and how much profits were lost); Computer Teaching Corp. v. Courseware Applications, Inc., 199 Ill. App. 3d 154, 157-58, 556 N.E.2d 816, 818, 145 Ill. Dec. 198, 200 (Ill. App. Ct. 1990) (discovery of all documents relating to design and development of defendant's computer program was proper where plaintiff alleged that defendant copied specific aspects of plaintiff's computer program in violation of terms of joint venture agreement; where plaintiff had specified rationale for believing that external portions of computer program were improperly copied, plaintiff had right to determine whether additional internal elements were copied), *appeal denied*, 133 Ill. 2d 553, 561 N.E.2d 688, 149 Ill. Dec. 318 (1990) (table). However, where a party can present alternative evidence in support of its claim or defense, a court may deny discovery of computer-related materials. *See* Harris Mkt. Res. v. Marshall Mktg. & Communications, Inc., 948 F.2d 1518, 1526 (10th Cir. 1991) (in copyright infringement case, where defendant could have presented other evidence to dispute validity of copyright or infringement, lower court

Not only may discovery of computer-related materials be proper in cases involving rights to or performance of software or hardware systems, but computer-related discovery may also be appropriate where the processes or contents of electronic storage and data manipulation are at issue. For instance, both the processes and contents of electronic storage and data manipulation may be at issue in cases involving computerized accounting functions. One such case is *Smith v. MCI Telecommunications Corp.*,[102] where the plaintiff claimed that the defendant, her former employer, defrauded its salespersons by failing to pay them proper commissions. In *Smith*, the court found certain computer systems manuals to be relevant, notwithstanding the defendant's contention that the manuals were not related to the calculations and payment of commissions.[103] The court found the manuals to be relevant, because functions other than calculations and payment of commissions were contested. In particular, the issues in the case included order entry, order control, order maintenance, order installation, and transaction accounts.[104] As an example, the plaintiff argued that the defendant's knowledge of a malfunction in its interrelated computer systems was relevant to her claim of fraud.[105]

Similarly, the processes and contents of electronic storage and data manipulation may be proper subjects of discovery where statistics or data regarding similar occurrences are relevant. For instance, in *Dunn v. Midwestern Indemnity*,[106] a civil rights case where the plaintiffs sought to prove that the defendant insurers engaged in impermissible "redlining" through their underwriting practices, the plaintiffs sought production of information about the nature of the defendant's computer system and computer tapes containing information about past and present policyholders in the region in question. The court found the computer information relevant insofar as the defendants' computer capabilities may have fostered, contributed to, or reflected the application of the defendants' underwriting standards and also found the computer information relevant to rebutting a business judgment or necessity defense.[107]

---

was held to have properly denied discovery of information concerning internal workings of plaintiff's copyrighted computer program).

102. Smith v. MCI Telecomms. Corp., 137 F.R.D. 25 (D. Kan. 1991).

103. *See id.* at 26-27.

104. *See id.* at 27.

105. *See id.* at 26 & n.2.

106. Dunn v. Midwestern Indemn., 88 F.R.D. 191 (S.D. Ohio 1980).

107. *See id.* at 195-96; *see also* Zapata v. IBP, Inc., 1994 WL 649322, *2-*3 (D. Kan. 1994) (computer records of employee's historical information found relevant to certification of class action employment discrimination suit; even though requested information pertained to defendant's salaried workers and plaintiffs were hourly workers, computerized information regarding salaried workers was relevant insofar as plaintiff was entitled to

Finally, the processes and contents of electronic storage and data manipulation may be most directly at issue in litigation over rights and obligations relating to data contained in computer storage media. For example, in *Armstrong v. Bush*,[108] the plaintiffs brought an action challenging, among other things, the adequacy of the National Security Counsel's ("NSC") guidelines for preserving electronically stored information under the Federal Records Act. In *Armstrong*, the court found several types of computer-related materials to be relevant and discoverable. First, information on oral training for use of the computer system in question was relevant to the existence of informal guidelines on the preservation of records.[109] Second, hard copy print-outs from the computer system in question were also found relevant to the adequacy of the records preservation guidelines. In particular, the print-outs would reveal the NSC's practices regarding access to and use of these materials, which could shed light on whether the materials stored in the computer system were properly classified under the guidelines for records preservation.[110] Third, evidence of requests for information from the computer system by other governmental entities and of the NSC's responses was relevant to how information stored in the system was classified.[111] Fourth, evidence of how the software used to store the information in question had been altered was relevant insofar as it provided helpful context to assess the guidelines.[112] Fifth, information stored on the system in question but never printed was relevant to determining the adequacy of the guidelines for preserving that information.[113] Sixth, although materials generated on the computer system and preserved on

develop statistical proof of patterns and practices regarding assignments, transfers, and promotions); Gallagher v. Massachusetts Bay Transit Auth., 1993 Mass. App. Div. 9, 11 (Mass. App. Div. 1993) (where plaintiff sought to prove that transportation authority breached duty to protect him from violence from other passengers, computer print-out of crimes that occurred on train line in question was relevant to proving that attack on plaintiff was reasonably foreseeable so as to create duty); State Farm Mut. Auto. Ins. Co. v. Engelke, 824 S.W.2d 747, 749-51 (Tex. Ct. App. 1992) (where plaintiff sought information regarding other lawsuits filed against defendant insurance company to show bad faith claims handling, court ordered production of information in form of computer print-out); Dunn v. Midwestern Idemn., 88 F.R.D. 191 (S.D. Ohio 1980) (computerized evidence relating to insurer's policyholders held relevant to claim that insurer engaged in impermissible redlining); Ball v. State of New York, 101 Misc. 2d 554, 421 N.Y.S.2d 328 (Ct. Cl. 1979) (where plaintiff claimed defendant inadequately maintained roadway, defendant ordered to produce computerized data relating to other accident claims); Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W. Va. 1972) (defendant required to produce payroll information in machine-readable form in connection with plaintiff's employment discrimination claim).

108. Armstrong v. Bush, 139 F.R.D. 547 (D.D.C. 1991).

109. *See id.* at 550-51.

110. *See id.* at 551-52.

111. *See id.* at 552.

112. *See id.* at 553-54.

113. *See id.* at 555.

back-up tapes were similarly relevant, the court accepted the argument that producing these materials would be unduly burdensome.[114]

Such cases where the computer-related materials sought have some obvious, independent evidentiary significance are relatively easy. More difficult to evaluate are cases where an alternative source of the computerized information sought exists in hard copy but where discovery from the source computer is sought to impeach that hard copy document by showing it to be inaccurate or fabricated. It is here that the unique qualities of computer storage media may offer litigators the most innovative form of fact-finding, while at the same time potentially presenting one of the most burdensome and intrusive forms of discovery.

In light of this unique set of burdens, in cases where a litigant seeks discovery of information in computer storage media for purposes of challenging the veracity or reliability of information contained in hard copy or of a witness's testimony, courts are beginning to grapple with the question of whether the litigant seeking such discovery must first demonstrate that the case actually presents a legitimate opportunity to exploit the unique fact-finding value of computer-related discovery. To illustrate this conflict, on the one hand, one court has stated that "a requesting party need not accept only data that exists in traditional forms, but may discover the same information when it is electronically stored in a computer."[115] Yet, on the other hand, the same court recognized that, given the nature of computer technology, a party cannot simply open up its computer banks for inspection and copying at the expense of the discovering party, as would be feasible with an ordinary request for production of documents.[116] Many, if not most, electronic forms of records will contain more information than exists on printed hard copy versions of the same records.[117] The challenge is to determine when the extra information contained in computer storage media is relevant and justifies the burden of extracting that information.[118]

One example of a case in which a court refused to grant the discovering party the right to conduct its own independent computer-related dis-

---

114. *See id.* at 554.

115. Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) (citing Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W.D. Va. 1972)).

116. *See id.* at 466.

117. *See, e.g.,* Armstrong v. Executive Office of President, 1 F.3d 1274, 1283-85 (D.C. Cir. 1993) (holding e-mail communications were not mere "extra copies" of records that need not be preserved under Federal Records Act, because hard copy versions did not contain several significant types of information present in computerized versions).

118. *Cf. In re* Application for Water Rights of Hines Highlands L.P., 929 P.2d 718, 727 (Colo. Sup. Ct. 1996) (holding lower court did not abuse discretion in refusing to sanction party who initially refused to produce computer disk of expert's stream-flow model, where print-out that had been produced provided sufficient information to defend against expert's model).

covery to test all information provided by an opponent, is *Williams v. Owens-Illinois, Inc.*[119] In *Williams*, a discrimination suit, the plaintiff sought to obtain computer tapes of the defendants' statistical database, and the trial court limited such discovery to requiring the defendant to perform certain computer runs at the request of the plaintiffs. The United States Court of Appeals for the Ninth Circuit denied the plaintiff's attempt to obtain full disclosure of the tapes on the ground that all of the information in the tapes were available in wage cards that had been produced in discovery. The court was not persuaded by the plaintiff's argument that the order requiring the defendant to perform certain computer runs at the request of the plaintiff would result in a statistical case that was prepared for the plaintiff by the defendant.[120] In other words, the court refused to allow the plaintiff to discover the computer tapes where the plaintiff sought that discovery for the sole purpose of verifying the accuracy or demonstrating the inaccuracy of data provided by the defendant.

Another case in which a court has set a high threshold to obtain computer-related discovery for the purpose of impeaching information existing in hard copy is *Fennel v. First Step Designs, Ltd.*[121] In *Fennel*, the United States Court of Appeals for the First Circuit upheld a district court decision denying discovery into an opponent's hard drive. In doing so, the First Circuit required the party seeking such discovery to proffer evidence in support of the alleged fabrication sufficient to survive rigorous judicial scrutiny.

In *Fennel*, the plaintiff sought to prove that she was wrongfully discharged in retaliation for reporting sexually offensive remarks made by her supervisor. The defendant, however, produced a memorandum undercutting this claim, which was dated a few weeks before the plaintiff's discharge and also before the date on which the plaintiff had reported her supervisor's remarks. This memorandum undercut the claim of retaliation, because it indicated that the plaintiff had been scheduled for a layoff. In particular, because the memorandum pre-dated the incident giving rise to the retaliation claim, the memorandum tended to show that the plaintiff's discharge was caused by the previously scheduled layoff rather than by retaliation for the subsequent reporting of the offensive remarks.[122]

To escape the import of this memorandum, the plaintiff sought access to the defendant's hard drive in order to demonstrate that the mem-

119. Williams v. Owens-Illinois, Inc., 665 F.2d 918 (9th Cir. 1982), *cert. denied*, 459 U.S. 971 (1982).

120. *See id.* at 932-33.

121. Fennel v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996).

122. *See id.* at 528-29.

orandum was in fact created after her discharge and was, thus, deceptively antedated. The plaintiff, however, first attempted to inspect the defendant's hard drive only after the close of discovery, and the vehicle of a Rule 56(f) motion was used to gain additional discovery in order to oppose the defendant's summary judgment motion.[123]

The district court denied the plaintiff's motion and awarded the defendant summary judgment. On appeal, the First Circuit affirmed. In doing so, the court found no plausible basis for believing that the plaintiff would have been able to discover specified relevant facts that were susceptible of collection within a reasonable time period. Although the First Circuit emphasized that "there may be cases where discovery of word processing files on a computer hard drive might well be warranted,"[124] the court set a threshold to obtain such discovery for the purpose of showing hard copies of documents which have been fabricated. Essentially, the First Circuit held that a district court has discretion to deny such discovery where the discovering party is unable to come forward with facts that unambiguously suggest a fabrication, as well as expert testimony demonstrating a likelihood beyond mere possibility of finding facts on the opponent's hard drive to confirm the fabrication.[125] Although, in *Fennel*, the plaintiff attempted to make such a proffer, that proffer did not survive the First Circuit's rigorous scrutiny.

As to the factual suggestion of fabrication, the court found that "five suspicious facts" offered by the plaintiff to show that the memorandum was fraudulently antedated were purely speculative. First, the plaintiff pointed to the fact that the memorandum included on its list of employees to be laid off, an employee who had already left the company by the date appearing on the hard copy version of the memorandum. The plaintiff saw this mistake as indicative of the memorandum having been prepared at a later point in time when the author's memory had faded. The court found this inference to be, "at best, extremely, attenuated."[126]

Second, the plaintiff pointed to the fact that the defendant had retained this memorandum, but not other similar memoranda. The court, however, found this fact to be "virtually non-probative" given that the sexual harassment complaint created an incentive to retain this particular document.[127]

Third, the plaintiff pointed to the fact that the author of the memorandum had made positive comments about the plaintiff's performance and job security shortly before the date on which the memorandum in

123. *See id.* at 529-30.

124. *Id.* at 534.

125. *See id.* at 530-35.

126. *Id.* at 533.

127. *Id.* at 533-34.

question purported to place her on the layoff list. The court, however, found this fact to be "not necessarily probative of fabrication" given that the plaintiff was discharged as part of a reorganization driven by financial concerns rather than for poor performance.[128]

Fourth, the plaintiff claimed that the defendant's managers inconsistently described the nature of and reasons for her discharge. The court, however, found that these statements were not suspicious. All of the statements related to the defendant's business objective of improving economic efficiency.[129]

Finally, the plaintiff pointed to the fact that some of the employees on the layoff list, in the memorandum, were not ultimately laid off. The court, however, found that this circumstance suggested that the layoff list in the memorandum was non-final, rather than that it was fabricated. The court observed that a fabricated list would more likely accurately reflect actual layoffs.[130]

Not only was the court unpersuaded by the plaintiff's factual support for her claim of fabrication, but the court also found that the plaintiff failed to demonstrate a sufficient likelihood that an inspection of the defendant's hard drive would ultimately demonstrate the memorandum's true date. The plaintiff's expert asserted that the original date of creation or last date of textual modification could be determined by reviewing the file on the defendant's hard drive. Accordingly, the plaintiff sought a "mirror image" copy of this hard drive for her expert to analyze.[131]

The defendant's consultant, however, determined that the defendant's computer system would not reveal the date on which the document was created or last modified. Moreover, the defendant objected to the plaintiff's proposed protocol for this discovery as failing to describe the methodology that would be employed to determine the date, as not adequately protective of information on the hard drive that was subject to the attorney-client privilege or to work product immunity, and as allowing unsupervised possession of the hard drive, which contained proprietary information.[132] Indeed, the defendant pointed to potential business risks resulting from accidental data loss, from incompatible hardware, and from system downtime and claimed that the process of copying and analyzing the hard drive was unknown and might temporarily or permanently affect the system and business operations.[133]

128. *Id.* at 534.

129. *Id.*

130. *Id.*

131. *Id.* at 531-32 & n.5.

132. *Id.* at 531-33 & n.6.

133. *Id.* at 532 n.6 & 533 n.8.

The First Circuit accepted the defendant's argument that the plaintiff's expert offered no more than conclusory assertions without foundation. Moreover, the court found that the plaintiff's expert could not predict a sufficiently conclusive result, but rather only took the position that "there may be a way" to determine the date in question. Finally, the court observed that the "lack of detail" in the protocol proposed by the plaintiff's expert "cast even more doubt on the soundness of the technical basis for the discovery venture."[134]

In light of the rigor with which the First Circuit scrutinized the plaintiff's proffer in *Fennel*, it is important to recognize the limitations of the court's decision. In *Fennel*, the First Circuit upheld a district court ruling that, in essence, the plaintiff had failed to "articulate a plausible basis for the belief that discoverable materials existed [in defendant's hard drive] which would have created a trial worthy issue."[135] In reviewing this ruling, the court applied the "abuse of discretion" standard.[136] When applying this standard of review, the broad latitude that is afforded to the lower court's decision considerably limits the precedential value of the appellate ruling. Specifically, when an appellate court applies the abuse of discretion standard, unless the lower court has used an improper legal standard or has incorrectly applied the law to the facts of the case, the appellate court will uphold the lower court's decision even if the appellate court itself would be inclined to rule differently were it considering the matter in the place of the lower court.[137] In light of this standard, the rigor to which the First Circuit subjected the plaintiff's proffer in *Fennel* can be seen merely as a way to arrive at one of a number of interpretations presented by the proffer and, specifically, an interpretation that justified the denial of discovery. Thus, were another court to be presented with a similar proffer in like circumstances, that court would be justified in viewing the proffer with the same scrutinizing lens and, therefore, in denying discovery. On the other hand, such a court might also view the proffer more broadly, with no definitive guidance from the outcome in *Fennel* as to whether the discovery sought should be allowed on such a broader view of such a proffer (although some aspects of the proposed protocol for computer discovery in *Fennel* may have been so deficient as to render any similar protocol inadequate as a matter of law). Finally, in addition to the peculiarities of the abuse of discretion standard of review, the precedential value of *Fennel* may also be limited by virtue of the fact that the plaintiff there sought the discovery in question pursuant to Rule 56(f), which requires a proffer as

134. *Id.* at 533.

135. *Id.* at 531.

136. *See id.* at 530.

137. *See* Am. Bd. of Psychiatry and Neurology, Inc. v. Johnson-Powell, 129 F.3d 1, 3 (1st Cir. 1997) (citing Celebrity, Inc. v. Trina, Inc., 264 F.2d 956, 958 (1st Cir. 1959)).

a prerequisite to obtaining discovery needed to oppose a summary judgment motion.[138] The required proffer under Rule 56(f) stands in contrast to the ordinary rule that a party resisting discovery bears the burden of demonstrating why the discovery sought should not be allowed.[139] In light of these limitations, the First Circuit carefully worded its conclusion: "While there may be cases where discovery of word processing files on a computer hard drive might well be warranted, [plaintiff] has not met her burden of demonstrating that the district court abused its discretion in denying that opportunity here."[140]

Not only is the precedential value of *Fennel* limited by reason of the standard of review applicable to that case, but, in addition, not all courts appear to require the type of proffer required by the First Circuit in *Fennel*. Perhaps the clearest authority for allowing discovery into computer storage media to test the reliability or veracity of information contained in hard copy is the case of *United States v. Davey*.[141] In *Davey*, the United States Court of Appeals for the Second Circuit held that the Internal Revenue Service should not be required to rely on the taxpayer's sworn assertion that a computer print-out of the taxpayer's financial recordkeeping system accurately reproduced all information on the computer tapes.[142] Because *Davey* was an IRS proceeding, however, its precedential value for discovery in civil litigation is unclear.

Similarly, one cryptic decision, *Momah v. Albert Einstein Medical Center*,[143] lends support to discovery into computer storage media to support claims that documents in hard copy were intentionally antedated. In *Momah*, the plaintiff claimed that he was unlawfully discharged from his employment by the defendants on the basis of his race.[144] To prove that the defendants' stated reasons for the discharge were pretextual, the plaintiff sought discovery of one of the defendants' computer records. Specifically, the plaintiff sought to obtain a copy of the "computer list files screen," which displays various information about documents created on the computer, including, among other items, the dates on which each document was created and last edited. By showing that a number of the documents supporting the discharge were backdated, the plaintiff hoped to cast doubt on the defendants' stated reason for termination.[145] The court allowed this discovery, deeming it "a close

138. *See Fennel*, 83 F.3d at 530-31 (quoting FED. R. CIV. P. 56(f)).

139. *See infra* notes 193-95 and accompanying text.

140. *See Fennel*, 83 F.3d at 534.

141. United States v. Davey., 543 F.2d 996 (2d Cir. 1976).

142. *See id.* at 1000.

143. Momah v. Albert Einstein Med. Ctr., 164 F.R.D. 412 (E.D. Pa. 1996).

144. *See id.* at 414.

145. *See id.* at 418.

question. . . ."[146] The court did not make clear, however, whether any threshold showing was required of the plaintiff to obtain this discovery. For instance, although the plaintiff "claim[ed] [one of the defendants] admitted to incorrectly dating a disciplinary memorandum relating to" the plaintiff, the court did not specify what type of evidence, if any, was proffered in support of this claim.[147]

If, in fact, no such proffer was required in *Momah*, the court's apparent permissiveness might be explained by the relatively unintrusive nature of the discovery sought. Producing a mere copy of a listing of computer files does not entail the same concerns as opening up all modes of computer storage media to scrutiny by an opponent. Yet, if a party is accused of antedating computer records, the discovery allowed in *Momah*—a mere listing of computer files—seems wholly inadequate, regardless of its unintrusive virtues. Simply put, a person who would antedate a document to further some deceptive scheme would be expected to cover any tracks left behind, including by manipulating the computer screen list of files. To unearth such truly deceptive behavior, much more intrusive discovery into hard drives or other forms of computer storage media would be necessary.

Finally, a Florida appellate court recently limited the requirement of a proffer to cases where the computer-related discovery sought would jeopardize privileged or confidential materials, and limited what the proffer must demonstrate to the technical feasibility of obtaining the information sought, the relative nonintrusiveness of the discovery procedure, and parameters and restrictions that would prevent overly broad disclosure or harm to the responding party's computer and databases. In particular, in *Strasser v. Yalamanchi*,[148] the court refused to allow unrestricted discovery into an opponent's computer system for the ostensible purpose of challenging the reliability of the information purportedly derived from that system. In doing so, that court appeared to leave open the door to discovery of such information only if the information sought could likely be obtained and obtained in a manner that would protect privileged and confidential information residing in the storage medium that is the subject of discovery. Specifically, in *Strasser*, a trial court had "allowed plaintiff unrestricted access to defendant's computer system, including all of his programs and directories, without protection for any privileged or confidential information and without safeguards or restrictions to minimize any potential harm to the computer system."[149] The appellate court quashed the lower court's order.

146. *Id.*

147. *Id.*

148. Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. Ct. App. 1996).

149. *Id.* at 1143.

Strasser involved a contract dispute between two plastic surgeons who agreed that the plaintiff would receive fifty percent of the collections of his gross billings. The defendant claimed that certain financial information had been purged from his system and was no longer in his possession. Accordingly, the plaintiff sought to inspect the defendant's computer system to search for the purged information.[150] Although the court's opinion was rather cryptic on the point, it appears that the plaintiff accused the defendant of understating gross billings and sought to prove this understatement by deriving the true state of gross billings from the defendant's computer system.

The competing arguments in *Strasser* played out in a battle of experts reminiscent of that in *Fennel*, although more stilted in terms of the respective experts' qualifications. Much like the plaintiff in *Fennel,* who offered a computer expert who could do no more than testify that there may be a way to obtain the information sought from the defendant's computer, the plaintiff in *Strasser* offered an accountant who could do no more than testify from his experience that purged data has been capable of retrieval. Much like the defendant in *Fennel,* who offered a computer expert to demonstrate that the information sought could not be found on the computer system in question, the defendant in *Strasser* offered a computer expert who testified that the defendant's computer system automatically overwrites deleted data during the purging process, thereby making retrieval impossible. In addition, in *Strasser*, the defendant's computer expert, actually logged onto the system and searched unsuccessfully for any sign of files containing the purged data. Indeed, in *Strasser*, one of the defendant's employees testified that she had employed this purging process three to five times in the ordinary course of business.[151] Also reminiscent of *Fennel*, in *Strasser,* the defendant resisted discovery on the ground that proprietary and privileged information would be revealed and that the computer system could potentially be exposed to inadvertent deletion of files or to the introduction of a virus.[152]

Unlike *Fennel*, however, although the *Strasser* court quashed an order allowing discovery into the opponent's hard drive and required an offer of proof before such discovery would be allowed, the *Strasser* court did not require, as a prerequisite to such discovery, a showing that the computer system not only contained the purged information, but that the purged information was consistent in content with the plaintiff's theory of the case. Indeed, the *Strasser* court left the door open to allowing the plaintiff some access on remand.

150. *Id.* at 1143-44.

151. *Id.* at 1144.

152. *Id.*

> If plaintiff can present evidence to demonstrate the likelihood of retrieving purged information, and if the trial court finds that there is no other less intrusive manner to obtain the information, then the computer search might be appropriate. In such an event, the order must define parameters of time and scope, and must place sufficient access restrictions to prevent harm to defendant's computer and data bases. One alternative might be for defendant's representative to physically access the computer system in the presence of plaintiff's representative under an agreed upon set of procedures to test plaintiff's theory that it is possible to retrieve this purged data.[153]

By refusing to set such a prerequisite and by opening the door to allowing some discovery on remand, the *Strasser* court may have been more lenient than the *Fennel* court, because, in *Strasser*, the plaintiff sought to discover information that no longer existed in hard copy, whereas, in *Fennel*, the plaintiff sought to discover computer-generated information about a document that did exist in hard copy. In this regard, *Strasser* may be somewhat different than other cases where a party seeks access to information stored in an opponent's computer system to undercut the reliability or veracity of information generated by that system. Indeed, there is at least anecdotal evidence that parties have succeeded in obtaining court orders allowing them to search their opponents' computer systems where they have argued that the electronic records were the sole existing source of a particular type of evidence.[154]

D. Discovery Into the Nature of an Opponent's Computer-Storage Media

Although one might expect some division over the extent of substantive discovery allowed into materials residing in various computer storage media, one would expect discovery into the nature of an opponent's computer system to be more straightforward. Here too, however, differences have emerged.

A number of courts have allowed discovery into the nature of an op-

153. *Id.* at 1145.

154. *See* Mariann Lavelle, *Digital Information Boom Worries Corporate Counsel*, Nat'l L.J., May 30, 1994, at B1 (quoting interview with John H. Jessen). At least one reported decision confirms this view. *See* Daewoo Elecs. Co. v. United States, 650 F. Supp. 1003 (C.I.T. 1986). In *Daewoo*, a party sought judicial review of an administrative proceeding and attempted to discover certain data sets reflecting information used by the government in connection with the administrative proceedings. Because the raw data reflected in these data sets were destroyed, the party seeking review was held to be entitled to production of the data sets in sequential files to be transferred from the government's mainframe computer. *See id.* at 1005-07.

ponent's computer system.[155] As illustrated by cases discussed above in connection with computer materials to be relied upon by experts at trial, courts are particularly likely to grant such discovery in connection with any computer-generated models that will form the basis for trial testimony.[156] By exposing flaws in procedures for inputting and processing information, such discovery enables the discovering party to obtain sufficient information to impeach whatever computer-related evidence may be offered by an opponent.[157] Similarly, to help the discovering party understand computer-generated evidence, a court may even require the producing party to assist the discovering party in reading and interpreting information that is stored in the producing party's computer system.[158]

In addition to the need for discovery relating to the nature of an opponent's computer system in order to understand evidence generated by or stored in that system, the discovering party may also need to obtain information relating to the nature of an opponent's computer system in order to understand what evidence may be found on that system and how best to obtain and preserve such evidence.[159] For example, the discovering party may need to know such information as what type of hardware and software systems an opponent uses, how such systems work, what type of computer storage media are used with such systems, and what type of archiving procedures, if any, are employed with such systems.[160] Such information is analogous to information about how an opponent maintains records—information that is plainly a proper subject of discovery when the records exist outside of computer storage media. Specifically, under Rule 26 of the Federal Rules of Civil Procedure, a party can conduct discovery to determine "the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any

155. *See, e.g.*, Dunn v. Midwestern Indemn., 88 F.R.D. 91 (S.D. Ohio 1980); *see also* Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) (citing *Dunn*) ("Depending on the type of case, a Court might even permit discovery of computer capabilities and capacities.").

156. *See supra* notes 78-95 and accompanying text.

157. *See* Long, *supra* note 28, at 407 n.6.

158. *See* Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1260-63 (E.D. Pa. 1980) (requiring production of data in magnetic computer-readable form instead of hard copy, in order to facilitate review by discovering party); Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W.D.Va. 1972) (same); *see also* Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) ("Indeed, some courts have required the responding party to develop programs to extract the requested information and to assist the requesting party in reading and interpreting information stored on computer tape.") (citing *Nat'l Union*).

159. *Cf.* Sherman & Kinnard, *supra* note 29, at 278-79 (noting that, under Rule 26(b)(1), party can be required to use computers to help identify and locate discoverable materials). This type of discovery is discussed in more detail in § VI.B, *infra*.

160. *See* Brill, *The Secret Life of Computer Data*, *supra* note 13, at 32; Davis, *supra* note 6, at 61; Howie, *supra* note 7, at 72; Pooley & Shaw, *supra* note 2, at 62 & 64-65.

discoverable matter."[161] Computer storage media are merely new forms of recordkeeping, and the information they store is itself plainly within the ambit of potentially discoverable subject matter.

Some commentators, however, have argued that such items as software and data processing procedures should not ordinarily be produced, except in such unusual instances as where the software or the computer's performance is directly at issue.[162] Apart from these few instances, information pertaining to the nature of an opponent's computer system may not, in and of itself, be probative of facts directly at issue and, also, may contain privileged, work product, and trade secret information.[163] Accordingly, courts must be sensitive to any efforts by the discovering party to use discovery requests pertaining to the nature of an opponent's computer system as a means to obtain discovery of subjects that would otherwise be improper. For example, where interrogatories inquiring into the nature of an opponent's computer files were found to be an improper attempt to determine the opponent's discovery plan, those interrogatories were barred by the work product doctrine.[164]

In another case, where discovery into the nature of an opponent's computer system similarly appears to have been employed in an attempt to gain discovery of an otherwise improper subject, the court's decision denying discovery includes broad language that appears to throw doubt on the right of litigants to obtain discovery of the nature of an opponent's computer system. In *Lawyers Title Insurance Corp. v. United States Fidelity & Guaranty Co.*,[165] the plaintiff sought to obtain discovery of confidential documents created by the defendant after the commencement of litigation—discovery that was denied as invasive of work product immunity.[166] In addition, the plaintiff sought discovery of information (unspecified in the court's decision) about the defendant's computer system. The plaintiff justified this request based on the plaintiff's desire to facilitate the defendant's production of relevant information, which the court interpreted as a desire to evaluate the adequacy of the defendant's production of the same work product documents that the court had protected from disclosure, as well as to help frame more effective discovery requests to capture such materials in the future.[167]

161. FED. R. CIV. P. 26(b)(1); *see generally* 8 WRIGHT, *supra* note 65, § 2012.

162. *See* Berndt, *supra* note 33, at 74 & 87; Friedman, *supra* note 30, at 1481-82; Long, *supra* note 28, at 407.

163. *See* Friedman, *supra* note 30, at 1481-82; Long, *supra* note 28, at 407.

164. *See* Hoffman v. United Telecomms., Inc., 117 F.R.D. 436, 439 (D. Kan. 1987).

165. Lawyers Title Ins. Corp. v. United States Fidel. & Guar. Co., 122 F.R.D. 567 (N.D. Cal. 1988).

166. *See id.* at 568-70.

167. *See id.* at 570.

Although the court held that its denial of discovery into the work product protected documents disposed of whether the plaintiff could obtain discovery of the nature of the defendant's computer system for storing such information, the court noted that it would deny the computer-related discovery even if discovery of the underlying documents were appropriate.[168] In doing so, the court used broad language to justify this result. Specifically, the court stressed the danger of revealing confidential methods that businesses use to process and store information. The court held that this danger was not outweighed either by the goal of determining whether an opponent's discovery responses are adequate or by the goal of facilitating the framing of better discovery requests.[169] Rather, for a party to obtain this type of discovery, the court set a threshold whereby the discovering party must show that conventional discovery has failed to produce information needed to litigate.[170]

Such a ruling is paradoxical, for no discovery is more conventional than discovery for the purpose of determining how a recordkeeping system operates. Although courts must be sensitive in determining whether the discovery of an adversary's computer system is undertaken for some illegitimate purpose, courts must also be sensitive to the legitimate purposes that such discovery may serve. As will be seen, parties should not be able to mask relevant information behind a complex recordkeeping system that cannot be subjected to full and fair discovery.[171] Moreover, as will also be seen, where such discovery implicates privileged, work product, or trade secret materials, the law of discovery provides ample tools for balancing such interests against the interest of a party in obtaining the information it needs to prepare its case.[172]

V. BALANCING THE BENEFITS AND BURDENS ASSOCIATED WITH DISCOVERY OF COMPUTER-RELATED MATERIALS

Underlying many, if not all, of the decisions regarding which types of computer-related materials are proper subjects of discovery is an explicit or implicit cost-benefit analysis. Indeed, what makes *Fennel* and *Strasser* so noteworthy is that, in each of those cases, when courts were presented with the greatest enhancement to the fact-finding function of litigation that computer technology has to offer, judicial sensitivity to the burdens resulting from that technology checked the fullest application of fact-finding discovery. In both *Fennel* and *Strasser*, the courts curtailed the litigants' opportunities to employ cutting-edge technology to exhume

168. *See id.*
169. *See id.*
170. *See id.*
171. *See infra* notes 215-20 & 236-42 and accompanying text.
172. *See infra* notes 189-226 and accompanying text.

evidence thought to have been interred through deletion or alteration. They did so because of the costs and invasiveness of the discovery needed to employ that technology, with a skeptical eye cast toward the capabilities of such retrieval technology. In *Strasser*, such concerns were explicitly stated as the rationale for the court's decision. In *Fennel*, the costs, hazards, and invasiveness of the discovery sought were a clear subtext to the rigorous offer of proof demanded by the court as a prerequisite to such discovery.

This Section takes a closer look at the benefits and burdens associated with discovery of computer-related materials. First, this Section will identify these various benefits and burdens. Second, this Section will briefly sketch the traditional procedural principles used for balancing such interests under the law of discovery. Third, this Section will examine how these principles have been applied in cases involving the discovery of computer-related materials.

Reviewing the handful of relevant precedents in light of the traditional principles for balancing the benefits and burdens of discovery yields at least four cautionary notes. First, the unknown or unfamiliar aspects of computer technology should not in and of themselves be grounds for assuming benefits or burdens that the law would otherwise require a proponent or opponent of discovery to demonstrate with concrete proof. Second, the law of discovery embodies a vast array of tools for resolving conflicts between various benefits and burdens claimed to be entailed by numerous types of discovery. When such conflicts occur in the electronic medium, there is no reason to believe that these tools are inadequate to the task, unless and until courts are shown otherwise.[173] Third, viewing the handful of precedents involving computer-related discovery through the lens of traditional discovery principles tends to underscore their fact-specific nature. Fourth, although some computer-related discovery may, in fact, increase the total amount of discoverable information in litigation, this form of discovery should not necessarily be seen as an enhancement to some equilibrium level of discovery that parties would otherwise ordinarily expect. Rather, enhanced technology for storing information will both increase the total amount of available recorded information and also eliminate some forms of hard copy recording of information that would have been available in an earlier era.

A. Identifying the Benefits and Burdens of Computer-Related Discovery

The benefits and burdens of computer-related discovery will depend largely on which form of computer storage media a party desires to dis-

173. *Accord* Friedman, *supra* note 30, at *passim* (advocating resolution of computer-related discovery issues can be accomplished by resort to Federal Rules of Civil Procedure).

cover, on the nature of information stored in those media, on whether the information exists in other forms, and, if so, on the accessibility and reliability of those other forms. Thus, how these benefits and burdens will balance will depend upon the facts of each case. Below is a summary of the benefits and burdens that have been encountered so far.

There are at least two types of benefits that flow from discovery of computer-related materials. The first type relates to the fact-finding function of litigation. The second type relates to efficiency in processing information.

Discovery into computer-related materials can enhance fact-finding in two often interrelated ways. First, computer storage media provide access to information that either does not exist in any other form or otherwise exists in some deceptive or misleading form. Second, discovery into computer storage media ensures access to types of evidence that would have been routinely available in hard copy in an earlier era, but are now maintained only in computer storage media. In other words, even where there is no deliberate attempt to hide information behind the cloak of computer technology, in some cases important evidence that is routinely discoverable may only be found in computer storage media. Thus, discovery into computer storage media will not only yield new types of evidence that were previously unavailable, but will also be necessary to ensure access to types of evidence that were previously available in other forms.

It is not necessarily true, however, that discovery into computer storage media only ensures access to materials that would have been stored in hard copy in an earlier era. For instance, before the advent of computers, all drafts of documents existed either in hard copy or on magnetic tapes that recorded dictation, or in some instances, possibly in microfilm or microfiche versions. Whether such drafts were maintained in any form of storage, depended upon the predilections and practices of the author, and upon the policies of the author's employer. Merely because such drafts can be retrieved from computer storage media today, does not necessarily mean that the drafts existing in such computer storage media represent evidence that would have been available from more accessible forms of storage in an earlier era, although in specific circumstances that may well be the case. Indeed, one commentator argues that, unlike paper documents where discarding of obsolete information is the norm, with computerized versions saving is the norm.[174]

Moreover, in addition to providing a source of documents that may or may not have existed in hard copy format in an earlier era, computer storage media provide access to forms of communications that never before existed, such as e-mail, electronic bulletin boards, and chat rooms.

174. *See* Pooley & Shaw, *supra* note 2, at 60.

Some of these electronic communications may, in an earlier era, have occurred through in-person, telephonic, or written communications, and some of those earlier forms of communications may or may not have been available for discovery in the form of retained hard copies of written communications, retained notes of oral communications, and memories of live witnesses. It is quite likely, however, that electronic communications media have increased the total volume of recorded communications that occur in the first instance. In any event, the total volume of such communications available to recall from computer storage media can be staggering.[175] Of course, these increased sources of information retrieval enhance the potential fact-finding powers of the litigator.[176]

In addition to gaining substantive evidence, by obtaining databases and machine-readable information, the discovering party may also realize substantial efficiencies. In particular, by obtaining mass quantities of data in such readily usable and manipulable forms, a party can sort, retrieve, and analyze information with greater speed and efficacy. Furthermore, in some instances, it may be less burdensome for the responding party to produce information in an electronic media than in hard copy. Indeed, judging from some instances in which broad discovery of computer-related materials has been allowed, it appears that access to computer storage media may undercut claims that complying with particular discovery requests would be unduly burdensome.[177]

On the other hand, discovery into computer storage media entails at least two types of potential burdens. Indeed, these two types of burdens mirror the two types of benefits from discovery into computer-related materials. The first type of burden relates to the enhanced danger of exposing information that is properly exempted from the discovery process and, thus, serves no proper part in the fact-finding process of litigation. The second type of burden relates to potential inefficiencies and costs entailed by discovery into computer storage media.

The danger of exposing materials that are not properly subjects of discovery results from the intermingling of those materials with properly discoverable materials within the same tangible medium for computer

175. *See* Bester, *supra* note 45, at 76.

176. *See* Pooley & Shaw, *supra* note 2, at 60.

177. *See* State of Missouri ex rel. Stolfa v. Ely, 875 S.W.2d 579, 582 (Mo. Ct. App. 1994) (rejecting argument that discovery request seeking claims files over three-year period was unduly burdensome where producing party had database of claims covering most of time period; fact that database was prepared by physical access to files undercut claim that locating and producing physical files would be inordinately difficult); State Farm Mut. Auto. Ins. Co. v. Engelke, 824 S.W.2d 747, 750-51 (Tex. Ct. App. 1992) (interrogatory seeking information relating to 500,000 other lawsuits brought against insurer held not unduly burdensome only insofar as responsive information could be generated from insurer's computer system).

storage. Thus, a single archive tape or a single hard disk might contain relevant information, as well as information that is privileged or immune from discovery or that contains confidential or trade-secret matter. If the discovering party seeks to inspect the storage medium itself, there may be no opportunity for the discovery target to withold such non-discoverable materials, as there would be with the production of documents in hard copy.

The potential inefficiencies from discovery into computer storage media may result from increased resources needed to undertake such discovery and disruptions to business operations that occur in conducting such discovery. First, the process of discovering and preserving computer evidence can be time consuming and costly, depending upon the size of the computer systems involved and the scope of the discovery sought. Second, the disruptions posed by such discovery are at least potentially greater than those presented by ordinary discovery (although not necessarily so). For example, gaining access to the hard drive of a particular network server may require curtailing all operations throughout the network. In addition, were any damage to occur to the computer equipment of the discovery target, the business disruption would be greatly magnified. Furthermore, devoting litigatory resources to the discovery of computer-related evidence can slow down and drive up the expense of litigation, particularly if the parties get bogged down in contentious disputes.

The clash between the potential benefits and burdens from discovery into computer storage media is well illustrated by two cases. On the one hand, the value of such computer forensics to litigation can be seen in the case of *Cerruti 1881 S.A. v. Cerruti, Inc.*[178] *Cerruti* was a trademark case where the plaintiff tried to establish its use in commerce of the mark in question through sales records. Specifically, the plaintiff relied upon hard copy print-outs of sales records kept on computer disk—print-outs that contained several inaccuracies and that were the subject of inconsistent testimony by the plaintiff's principal. The plaintiff's principal attributed these inaccuracies to an alleged mishap in transferring those records from main computer storage to a removable hard disk. To test this claim, the court appointed an expert who examined both the removable hard disk and the original computer source. The expert was able to determine that the relevant files in the removable hard disk had been compressed so as to block the expert's access. The expert, however, was able to find corresponding data files on the hard drive of the source computer, which the expert was able to match with the hard copy prints. The expert was further able to determine that the removable hard disk was not defective and that random numbers had been manually inserted

178. Cerruti 1881 S.A. v. Cerruti, Inc., 169 F.R.D. 573 (S.D.N.Y. 1996).

in the name and address fields of the records. Moreover, the expert was able to determine that the span of invoice numbers in computer storage was more than triple the number of records produced, notwithstanding the fact that the plaintiff's principal testified that the number of records produced was accurate. Based on the expert's findings, and on the inconsistent testimony of the plaintiff, the court concluded that the records were fabricated and that the random numbers inserted in the name and address fields were designed to prevent a survey of customers to determine whether they had actually made the purchases reflected on the records.[179]

On the other hand, the burdens and intrusions represented by this form of discovery can be seen in the case of *Gates Rubber Co. v. Bando Chemical Indus., Ltd.*[180] In *Gates Rubber*, the plaintiff brought suit against several individual and corporate defendants alleging trade secret misappropriation, copyright infringement, unfair competition, and breach of non-competition and fiduciary agreements. These charges stemmed from the defendants' alleged copying of two computer programs that had been developed by the plaintiff.[181]

During discovery, the plaintiff obtained evidence that one of the individual defendants had destroyed computer files and altered his computer menu to delete references to one of the two computer programs at issue in the litigation. Armed with this information, the plaintiff persuaded the court to enter a "Site Inspection Order" under which the plaintiff brought technicians into the defendants' facilities and copied numerous materials for preservation, including the hard drives of all computers at these facilities. During the implementation of this order, the plaintiff obtained evidence leading it to believe that the defendant had undertaken a campaign to destroy documents and evidence. Consequently, the plaintiff began to file multiple motions for sanctions. These motions then took on a life of their own, generating years of discovery and an evidentiary hearing, while litigation of the case on the merits was sidetracked.[182]

Ultimately, however, the plaintiff prevailed only with respect to one portion of one of its motions for sanctions, and was awarded for this partial victory only ten percent of the attorneys' fees and costs incurred because of the sanctions proceedings.[183] Many of the plaintiff's arguments

179. *See id.* For another instance in which a court appointed an examiner to supervise discovery of computer-related information after the producing party twice failed to make a sufficient production of information whose disclosure was mandated by court order, see United States v. Int'l Bus. Machs. Corp., 76 F.R.D. 97 (S.D.N.Y. 1977).

180. Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996).

181. *See id.* at 99.

182. *See id.* at 99-101.

183. *See id.* at 110-13 & 131.

failed as a result of the plaintiff's failure to take proper steps to copy and preserve the computer evidence at issue, and as a result of the fact that the plaintiff was unable to assess how much, if any, probative evidence was lost and to what effect. The plaintiff's proof fell short, because, in implementing the "Site Inspection Order," the plaintiff copied very little of the type of materials claimed to be destroyed and, furthermore, the plaintiff did not inspect many of the documents that were copied and preserved.[184] Moreover, the evidence supporting the limited finding of sanctionable conduct came from the deposition testimony that instigated the "Site Inspection Order," rather than from the fruits of that order's implementation.[185]

Not only did the plaintiff fail to prevail on all but one portion of one of its sanctions claims, but the court actually awarded sanctions against the plaintiff for having brought twelve of its eighteen sanctions claims without substantial justification. For this misconduct, the defendants were awarded sixty-five percent of the total attorneys' fees and costs incurred in connection with the sanctions proceedings.[186] In juxtaposition to the limited benefits obtained and great penalty incurred by the plaintiff, the court observed that the sanctions litigation arising out of the "Site Inspection Order" took several years, cost several millions of dollars, and impeded progress on the merits of the case.[187] The court concluded that "[i]n retrospect, the sanctions proceedings were an enormous waste of time, energy and money."[188]

B. How the Benefits and Burdens of Discovery are Balanced Under Traditional Discovery Principles

The general legal framework through which the benefits and burdens of discovery are balanced has already been discussed in Section III. Until special rules are adopted to address concerns unique to discovery of computer-related materials, the benefits and burdens of this type of discovery must be balanced by applying the same framework. Indeed, as previously indicated, in their present form, the Federal Rules of Civil Procedure contemplate their application to the discovery of computer-related materials.[189]

Under the traditional framework provided by the Federal Rules of Civil Procedure, there is a general bias in favor of disclosure.[190] Specifi-

184. *See id.* at 110, 112-13, 120.
185. *See id.* at 99 & 111-13.
186. *See id.* at 115, 116, 117, 118, 122, 123, 124, 125, 126, 128 & 131.
187. *See id.* at 112-13 & 130.
188. *See id.* at 130.
189. *See supra* notes 62-67 and accompanying text.
190. *See* 6 Moore, supra note 94, § 26.02, at 26-25 to 26-27; 8 Wright, *supra* note 65, § 2001, at 39-46.

cally, the Federal Rules relaxed stringent pleading requirements and, instead, gave parties liberal discovery procedures in order to garner the details necessary to prosecute and defend claims.[191] The Supreme Court has commented on this change in procedure: "Thus civil trials in the federal courts no longer need be carried on in the dark. The way is now clear, consistent with recognized privileges, for the parties to obtain the fullest possible knowledge of the issues and facts before trial."[192]

Consequently, the party objecting to a discovery request bears the burden of demonstrating why that discovery request should not be allowed.[193] This burden cannot be discharged with conclusory assertions that harm will be suffered if the discovery sought is allowed. Rather, a party seeking judicial protection from discovery must come forward with a specific factual proffer, usually in the form of affidavits from knowledgeable witnesses and, sometimes, *in camera* submissions to the court so that the court can assess the sensitivity and need for protection of the materials in question.[194] By following these procedures, the court can

191. *See* Conley v. Gibson, 355 U.S. 41, 47-48 (1957) (discussing how simplified notice pleading was made possible by liberal opportunities for discovery under Federal Rules); Hickman v. Taylor, 329 U.S. 495, 499-500 (1947) (same); *see generally* Mark D. Robins, *The Resurgence and Limits of the Demurrer*, 27 SUFFOLK U. L. REV. 637, 640-46 (discussing adoption of notice pleading under Federal Rules).

192. *Hickman*, 329 U.S. at 501.

193. *See* Flag Fables, Inc. v. Jean Ann's Country Flags and Crafts, Inc., 730 F. Supp. 1165, 1186 (D. Mass. 1990) (collecting authority); *see, e.g.*, Golden Valley Microwave Foods, Inc. v. Weaver Popcorn Co., 132 F.R.D. 204, 212 (N.D. Ind. 1990) (party opposing discovery bears burden of demonstrating why requested discovery is not relevant) (citation omitted); Weil v. Inv./Indicators, Res. & Mgmt., Inc., 647 F.2d 18, 25 (9th Cir. 1981) ("As with all evidentiary privileges, the burden of proving that the attorney-client privilege applies rests not with the party contesting the privilege, but with the party asserting it.") (citations omitted); Resolution Trust Corp. v. Dabney, 73 F.3d 262, 266 (10th Cir. 1995) ("The party asserting a work product privilege as a bar to discovery must prove the doctrine is applicable.") (citation omitted); Brittain v. Stroh Brewery Co., 136 F.R.D. 408, 412 (M.D.N.C. 1991) (party seeking protective order barring discovery of trade secrets bears burden of demonstrating good cause); Josephs v. Harris Corp., 677 F.2d 985, 992 (3d Cir. 1982) ("[T]he party resisting discovery must show specifically . . . how each question is overly broad, burdensome or oppressive.") (citations and internal quotation marks omitted).

194. *See* Panola Land Buyers Ass'n v. Shuman, 762 F.2d 1550, 1559 (11th Cir. 1985) ("To be adequate, objections which serve as the basis of a motion for protective order under FED. R. CIV. P. 26 should be plain enough and specific enough so that the court can understand in what way the interrogatories are alleged to be objectionable.") (citations and internal quotation marks omitted); *Josephs*, 677 F.2d at 992 ("[T]he mere statement by a party that the interrogatory was 'overly broad, burdensome, oppressive and irrelevant' is not adequate to voice a successful objection to an interrogatory."); Bucher v. Richardson Hosp. Auth., 160 F.R.D. 88, 92 (N.D. Tex. 1994) ("The movant must show a particular and compelling need for such an order. Conclusory assertions of injury are insufficient.") (citations omitted); *Brittain*, 136 F.R.D. at 412-13 ("The party [seeking a protective order] must make a particular request and a specific demonstration of facts in support of the request as opposed to conclusory or speculative statements about the need for a protective order and the

narrowly tailor protective orders so as to grant only that degree of protection demanded by the facts, thereby preserving the liberal spirit of the discovery rules.[195]

In addition, although there are several recognized shields to the discovery process, there are a number of limitations to these shields, some of which may have relevance when the discovery sought comprises computer-related materials. For instance, privileged materials may be discovered where the privilege has been waived.[196] Even where the privilege has not been waived, where a party contemplates waiving the privilege at trial, most courts will allow discovery of materials that are subject to that privilege.[197] Indeed, even where a party does not intend to use such privileged materials at trial, where the party takes a position that places the subject matter of those materials at issue, then the materials will be discoverable.[198] Thus, the very topics of the litigation may empower a party to discover privileged materials. Finally, even where these limitations will not strip materials of their privilege, the privilege will be narrowly construed.[199]

By comparison, work product protection is even less secure. Rule 26 affords two levels of work product immunity for materials "prepared in anticipation of litigation or trial. . . ."[200] Ordinary work product materials may be discovered "only upon a showing that the party seeking discovery has substantial need of the materials in the preparation of the party's case and that the party is unable without undue hardship to obtain the substantial equivalent of the materials by other means."[201] By contrast, Rule 26 instructs courts to shield from disclosure so-called opinion work product which consist of the "mental impressions, conclusions, opinions, or legal theories of an attorney or other representative of a party concerning the litigation."[202] Thus, even where a party seeking to discover work product material can demonstrate substantial need and undue hardship, the courts must still protect opinion work product from disclosure.[203] Many courts, however, will allow discovery even into opin-

---

harm which would be suffered without one . . . . Such demonstrations are preferably made by affidavits from knowledgeable persons and may include *in camera* submissions or *in camera* proceedings attended by opposing counsel.") (citations omitted).

195. *See generally* 6 MOORE, supra note 94, § 26.102[1]; 8 WRIGHT, *supra* note 65, §§ 2035-36.

196. *See* 6 MOORE, supra note 94, § 26.47[5]; 8 WRIGHT, *supra* note 65, § 2016.2.

197. *See* 8 WRIGHT, *supra* note 65, § 2016.2.

198. *See* 6 MOORE, *supra* note 94, § 26.47[5]; 8 WRIGHT, *supra* note 65, § 2016.2.

199. *See* Weil v. Inv./Indicators, Res. & Mgmt., Inc., 647 F.2d 18, 24 (9th Cir. 1981) (collecting authority).

200. FED. R. CIV. P. 26(b)(3).

201. *Id.*

202. *Id.*

203. *See* 6 MOORE, *supra* note 94, § 26.70[b].

ion work product upon a showing of extraordinary need for such materials.[204] In addition, like privileges, work product immunity can be waived.[205]

Even trade secrets and highly confidential materials are not granted any blanket privilege or immunity from discovery.[206] If the trade secret or confidentiality of particular materials can be established, Rule 26(c)(7) allows the court either to protect such information from any disclosure or to allow such information to "be revealed only in a designated way. . . ."[207] Accordingly, rather than foreclose any discovery into such materials, courts may simply restrict disclosure to some select group such as counsel only or counsel and experts only and/or restrict the use to which such information can be put.[208] In many cases, courts will impose such limited restrictions, rather than impose blanket restrictions against any disclosure.[209] If the party producing the discovery seeks to prevent any particular disclosure, that party must demonstrate to the court how it would be harmed from that disclosure.[210] Even where the producing party can make this demonstration, the party seeking discovery will still gain access to the information where that party can show that the harm from disclosure is outweighed by the relevance and necessity of the information to the case.[211]

---

204. *See id.* § 26.70[5][e]; 8 WRIGHT, *supra* note 65, § 2026.

205. *See* 6 MOORE, *supra* note 94, § 26.70[6].

206. *See* 1 MELVIN F. JAGER, TRADE SECRETS LAW § 5.06[2] (Rel. No. 23 1997); 3 ROGER M. MILGRIM, MILGRIM ON TRADE SECRETS § 14.02[a] (Rel. No. 54 1996); 6 MOORE, *supra* note 94, § 26.46[16]; 8 WRIGHT, *supra* note 65, § 2043.

207. FED. R. CIV. P. 26(c)(7).

208. *See* 6 MOORE, *supra* note 94, § 26.108[b]; 8 WRIGHT *supra* note 65, § 2043; *see, e.g.*, Ares-Serono, Inc. v. Organon Int'l B.V., 862 F. Supp. 603, 608-09 (D. Mass. 1994) (restricting disclosure); *In re* First Peoples Bank Shareholders Litig., 121 F.R.D. 219, 230 (D.N.J. 1988) (restricting disclosure and limiting use); GTE Prods. Corp. v. Gee, 112 F.R.D. 169 (D. Mass. 1986) (restricting disclosure); Alloy Cast Steel Co. v. United Steel Workers of Am., 70 F.R.D. 687, 689 (N.D. Ohio 1976) (restricting disclosure and limiting use), *modified*, 429 F. Supp. 445 (N.D. Ohio 1977).

209. *See* 8 WRIGHT, *supra* note 65, § 2043.

210. *See id.*

211. *See id.* Disclosure, even under restrictive conditions, however, is by no means an inevitable outcome of the litigation process. In some instances, the sensitivity of trade secret information may be so great as to justify exempting it from discovery. For example, even where a plaintiff seeks to shield from discovery the very trade secret that it accuses the defendant of misappropriating, the court may protect against compounding the harm allegedly inflicted by the defendant through either requiring that the plaintiff merely specify certain characteristics of the claimed trade secret or foreclosing any discovery in instances where there the defendant would not need to ascertain the trade secret in order to mount a defense that is available on the facts. *See* 3 MILGRIM, *supra* note 206, §§ 14.02[2]-[3][a]. In addition, nonparties may be entitled to greater protection against disclosure of their trade secrets or confidential information. *See* FED. R. CIV. P. 45(c)(B)(ii) (authorizing court to protect against nonparty disclosure of trade secrets or confidential information,

Finally, it would be a mistake to assume that burdensome discovery can be avoided merely because it is burdensome. Rule 26(c) provides for protection only against burden that is "undue."[212] Rule 26(b)(2) enables courts to limit burdensome discovery only where "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."[213] Thus, mere inconvenience and expense, in and of themselves, will not warrant entry of a protective order.[214]

One application of these principles that has particular salience to the discovery of computer-related materials is the rule that an inadequate filing system will not excuse a party from producing requested documents.[215] This rule stems from the decision in the case of *Kozlowski v. Sears, Roebuck & Co.*[216] In *Kozlowski*, the plaintiff brought suit against the distributor of pajamas that allegedly caused the plaintiff to suffer severe burns.[217] The plaintiff sought discovery of all complaints and communications concerning similar occurrences in order to demonstrate that the product was unreasonably dangerous or that the defendant knew or should have known of the danger.[218] The defendant, however, resisted discovery on the ground that its practice of indexing claims alphabetically by claimant, rather than by type of product, made it practically impossible to determine whether there have been complaints of similar occurrences.[219] The court, however, flatly rejected this argument:

> The defendant may not excuse itself from compliance with Rule 34 . . . by utilizing a system of record-keeping which conceals rather than dis-

---

unless party seeking discovery can show "substantial need . . . that cannot be otherwise met without undue hardship"); Dart Indus. Co. v. Westwood Chem. Co., 649 F.2d 646, 649 (9th Cir. 1980) ("While discovery is a valuable right and should not be unnecessarily restricted, . . . the 'necessary' restriction may be broader when a nonparty is the target of discovery. . . . [T]here appear to be quite strong considerations indicating that discovery would be more limited to protect third parties from harassment, inconvenience, or disclosure of confidential documents.") (citations and internal quotation marks omitted); Laxalt v. McClatchy, 116 F.R.D. 455, 458 (D. Nev. 1986) ("The rule is thus well established that nonparties to litigation enjoy greater protection from discovery than normal parties."); *see also* 1 JAGER, *supra* note 206, § 5.06[2] (discussing factors to be weighed in determining whether trade secrets of nonparty should be subject to discovery).

212. FED. R. CIV. P. 26(c).

213. FED. R. CIV. P. 26(b)(2).

214. 6 MOORE, *supra* note 94, § 26.104[2]; 8A WRIGHT, *supra* note 65, § 2214.

215. *See* 7 MOORE, *supra* note 94, § 34.14[3]

216. Kozlowski v. Sears, Roebuck & Co., 73 F.R.D. 73 (D. Mass. 1976).

217. *See id.* at 74.

218. *See id.* at 74-75.

219. *See id.* at 75-76.

> closes relevant records, or makes it unduly difficult to identify or locate them, thus rendering the production of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules.[220]

This is not to say that a party responding to discovery requests for computer-related materials is powerless to protect itself from harmful disclosures and onerous intrusions. The protections in the Federal Rules for materials that contain privileged, work product, or trade secret information are real. Thus, Rule 26 gives the court ample power to limit and preclude discovery into such matters.[221] Accordingly, the Advisory Committee Note to Rule 34(a) makes clear that a party whose computer system is subjected to inspection may be protected, among other things, as to the "confidentiality of nondiscoverable matters. . . ."[222] The Rules also empower the court to apportion costs attendant to computer-related discovery. For instance, Rule 26(c)(2) enables the court to order that discovery be had "only on specified terms and conditions. . . ."[223] Under this provision, courts can require the discovering party to compensate the responding party for costs caused by the discovery sought.[224] Moreover, the Advisory Committee Note to Rule 34(a) also provides that a party whose computer system is subjected to inspection may be protected with respect to costs.[225] In this vein, the *Manual for Complex Litigation* advises using appropriate safeguards to protect against the disclosure of irrelevant, trade secret, or work product protected materials when employing database searches of materials in computer storage media.[226]

Thus, although the protections afforded by the rules are real, phrases such as "privilege," "work product," "trade secrets," and "undue burden" are not talismans that ward off discovery by their mere mention. Rather, each of these concepts has precise prerequisites that must be established to obtain protection from the discovery process, and the protection these concepts afford is often quite limited. This texture of the law of discovery should particularly be kept in view when examining the discovery of computer-related materials. For in this technologically sophisticated medium, the complexity that must be grappled with in apply-

220. *Id.* at 76. Nonetheless, even where expense, interference with business operations, or the difficulty of working with a cumbersome filing system will not defeat discovery altogether, they may justify protective conditions governing the timing, location, and procedure for production. *See* 7 MOORE, *supra* note 94, § 34.14[3].

221. *See* FED. R. CIV. P. 26(c).

222. FED. R. CIV. P. 34(a), advisory committee note.

223. FED. R. CIV. P. 26(c)(2).

224. *See* 8 WRIGHT, *supra* note 65, § 2038.

225. FED. R. CIV. P. 34(a), advisory committee note.

226. MANUAL FOR COMPLEX LITIGATION, *supra* note 67, § 21.446, at 80.

ing these established discovery concepts makes short-circuiting these concepts an alluring proposition.

C. How the Benefits and Burdens of Computer-Related Discovery Have Been Balanced by Courts

Now that the types of benefits and burdens entailed by discovery of computer-related evidence have been identified and the traditional tools for resolving such conflicts have been outlined, this Part will examine how courts have attempted to resolve such conflicts in the context of computer-related discovery. Specifically, this Part will review how courts approach three types of issues that arise in balancing the benefits and burdens entailed by computer-related discovery: (1) whether to grant or deny any access to computer-related materials; (2) what protective measures to order as a condition to allowing discovery of computer-related materials; and (3) how to apportion the cost of discovery of computer-related materials among the parties.

1. *Access*

One way in which courts balance the benefits and burdens of computer-related discovery is by determining whether or not to allow such discovery at all. Cases in which courts have determined whether to grant or deny access range from cases where the information sought is both relevant and likely to promote efficiency and the burdens claimed to flow from the discovery are either nonexistent or unsupported to cases where the information sought has little or no likely value in the litigation and the discovery sought is both invasive and costly. In cases of competing claims of benefits and burdens that would flow from the requested discovery, the burden of proof imposed on one or the other party for establishing the claimed benefits or burdens plays a central role in determining whether access shall be allowed or denied. Thus, in evaluating such competing claims, it will be crucial to pay careful attention to the evidentiary burdens that the Federal Rules of Civil Procedure set for establishing these interests.

At one end of the spectrum, where the information sought is both relevant and likely to enhance efficiency, and where the intrusive nature of the discovery can be ameliorated with protective measures, then the discovery sought will likely be allowed. For instance, in the case of *Adams v. Dan River Mills, Inc.*,[227] an employment discrimination case, the plaintiff sought production in machine-readable form of payroll-related data that the defendant contended had already been produced in hard copy. The court ordered the defendant to produce such information. The

227. Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W.D. Va. 1972).

plaintiff sought this information to prepare accurate, up-to-date, statistics to determine whether discriminatory practices had occurred. Based upon "the accuracy and inexpensiveness of producing the requested documents,"[228] the court ordered production. The court held that a protective order would adequately address the defendant's concern regarding the trade secrecy of labor cost data reflected in the materials to be produced.[229]

By contrast, where the responding party comes forward with a properly supported claim of classic undue burden, the balance may shift. For instance, in the case of *Union Fidelity Life Insurance Co. v. Seay*,[230] the plaintiff sought production of all records of the insurance company defendant regarding denial of coverage for claims made under policies containing a particular type of language. Because the records requested related to 45,000 policies, the court denied the discovery as "unduly oppressive and burdensome . . . ."[231] The court made this finding even though the records requested were available in computer storage, albeit out of state.[232] Accordingly, the mere fact that the information requested exists in computer storage will not necessarily make proper discovery requests that are otherwise unduly burdensome.

On the other hand, where the discovery requested is both focused and relevant, the availability of the information sought in a computerized format may, in some instances, eliminate what would otherwise be an undue burden. For example, *State Farm Mutual Automobile Insurance Co. v. Engelke*,[233] the plaintiff sued the insurance company defendant for bad faith handling of the plaintiff's personal injury claims. The plaintiff served an interrogatory requesting information regarding each lawsuit filed against the defendant in the previous five years involving an allegation of bad faith. The trial court ordered the defendant to answer the interrogatory over the objection that the interrogatory was overly broad, burdensome, and harassing.[234] Based upon testimony that much of the information sought could be obtained by programming the defendant's computer system, the appellate court upheld the decision ordering the defendant to answer the interrogatory but only insofar as the lower court's order required the defendant to provide a computer printout of the requested information and only insofar as this information related to claims in the state where the plaintiff was located.[235]

228. *See id.* at 222.
229. *See id.*
230. Union Fidelity Life Ins. Co. v. Seay, 378 So.2d 1268 (Fla. Dist. Ct. App. 1979).
231. *Id.* at 1269.
232. *See id.*
233. State Farm Mut. Auto. Ins. Co. v. Engelke, 824 S.W.2d 747 (Tex. Ct. App. 1992).
234. *See id.* at 749.
235. *See id.* at 750-51.

Indeed, where a party resists computer-related discovery with a claim of classic undue burden, courts are particularly likely to require that party to meet a high threshold where the information sought is relevant and does not exist in any other form. For example, one of the most compelling cases for production was *Daewoo Electronics Co. v. United States*,[236] which involved judicial review of an administrative proceeding before the Department of Commerce. In the administrative proceeding under review in *Daewoo*, the government had employed certain computer programs, data sets, and related technical aids. The government was willing to produce computer tapes of the raw data, but not of the distilled data sets that were stored in its mainframe computer. The information needed to recreate the data sets from the raw data had been destroyed, however, and the data sets were the only source of the actual data used by the government in generating the final results under review.

The government resisted discovery on the ground of undue burden insofar as the discovering party wanted the government to transfer the data sets in the form of sequential files so that the data sets could be used on the discovering party's smaller computer. The court, however, likened the burden of placing this data into sequential files to the normal burden of ordering files in routine discovery. Thus, the court ordered production of the data sets, noting that key evidence of decisionmaking should not be cloaked behind the complexity of electronic transmittal processes.[237]

> It would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation. The use of excessive technical distinctions is inconsistent with the guiding principle that information which is stored, used, or transmitted in new forms, should be available through discovery with the same openness as traditional forms.[238]

---

236. 650 F. Supp. 1003 (C.I.T. 1986).

237. *See id.* at 1005-07.

238. *See id.* at 1005-06; *see also In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, at *2 (N.D. Ill. 1995) (holding discovering party should not bear burden of responding party's choice of cumbersome procedure for computer storage); Bills v. Kennecott Corp., 108 F.R.D. 459, 463-64 (D. Utah 1985) (holding information in computers should be discoverable to same extent as other information). Indeed, a party who tries to use the complexity of computer storage systems as a cloak for withholding information does so at its peril. Where a court twice ordered a party to produce computer-related information and where the producing party combined the highly technical nature of the subject matter with an overly narrow interpretation of the courts orders in order to withhold key statistics from two sets of computer files, the court found "exceptional circumstances" to justify appointing an examiner under FED. R. CIV. P. 53. The court granted the examiner broad powers to supervise discovery, including authority to visit the producing party's premises to inspect and copy evidence, as well as the authority to conduct hearings. *See* United States v. Int'l Bus. Machs. Corp., 76 F.R.D. 97 (S.D.N.Y. 1977).

Similarly, in *Dunn v. Midwestern Indemnity*,[239] the court echoed this rationale in limiting claims of undue burden in the context of computer-related discovery. In that case, after the court found computerized information regarding an insurer's policyholders to be relevant to claims that the insurer had engaged in impermissible redlining, the court then scheduled an evidentiary hearing to assess the defendants' arguments that complying with the discovery requests would be unduly burdensome. The court stressed, however, that the focus of this hearing would be on whether compliance would be "impossible," rather than merely "time-consuming and laborious."[240] In doing so, the court relied on the *Kozlowski* rule that a party may not avoid discovery on the ground of undue burden, merely because it maintains an inadequate filing system.[241] Finally, the court readily disposed of the defendants' confidentiality and trade secrecy based objections to discovery, noting that the materials discovered would be subject to a protective order restricting their disclosure.[242]

The evidentiary hearing scheduled by the *Dunn* court indicates that, not only must the type of burden claimed be extraordinary to justify denying relevant computer-related discovery, but the claim must also be properly supported by competent evidence. Indeed, the failure of a responding party to make this type of evidentiary showing resulted in the overruling of an undue burden objection in the case of *Zapata v. IBP, Inc.*[243] In *Zapata*, the class action plaintiffs sought production from the

239. Dunn v. Midwestern Indemn., 88 F.R.D. 191 (S.D. Ohio 1980).

240. *See Dunn*, 88 F.R.D. at 197; *see also* Armstrong v. Bush, 139 F.R.D. 547, 554-55 (D.D.C. 1991) (where defendant resisted Freedom of Information Act request to produce back-up tapes on ground that request imposes undue burden, plaintiff held entitled to examine defendant's witnesses on assumptions behind assertion of undue burden).

241. *See Dunn*, 88 F.R.D. at 197-98 (quoting Kozlowski v. Sears, Roebuck & Co., 88 F.R.D. 73 (D. Mass. 1976)). Indeed, no less an authority than the United States Supreme Court has observed:

> [A]lthough it may be expensive to retrieve information stored in computers when no program yet exists for the particular job, there is no reason to think that the same information could be extracted any less expensively if the records were kept in less modern forms. Indeed, one might expect the reverse to be true, for otherwise computers would not have gained such widespread use in the storing and handling of information.

Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 362 (1978). This is not to say that the mere use of computer storage media should result in automatic access to any quantity of data no matter how large and no matter how attenuated the connection may be between that data and the case at issue. *See* Union Fidel. Life Ins. Co. v. Seay, 378 So.2d 1268, 1269 (Fla. Dist. Ct. App. 1979) (quashing deposition subpoena that sought production of all records concerning denial of insurance coverage for claims under particular type of policy—without limitation as to time or number of claims for which records must be produced—and where compliance would require producing 45,000 insurance policies stored on computer).

242. *See Dunn*, 88 F.R.D. at 198.

243. Zapata v. IBP, Inc., 1994 WL 649322 (D. Kan. 1994).

defendant employer of computerized data consisting of historical information regarding employees to demonstrate commonality of employment discrimination claims among members of the putative class. After the court found the data to be relevant insofar as statistics regarding the defendant's patterns of job promotions and transfers would be probative of commonality, the court then rejected the defendant's claim that the discovery requested was unduly burdensome.[244] The court found that, when balanced against the clear relevance of the requested data, the defendant completely failed to proffer affidavits or evidence of record that would demonstrate how the discovery sought was unduly burdensome. Accordingly, the requested production was compelled by the court.[245]

By contrast, where the information sought bears no relevance to the claims at issue, discovery of computer-related materials will be denied no matter how greatly such discovery may enhance the discovering party's ability to process information and no matter how easily the requested materials can be produced. Such a result was reached by the court in *Haroco, Inc. v. American National Bank & Trust Co.*[246] (*"Haroco I"*), where the claimed efficiencies that would flow from requiring production of computer tapes gave way to what the court determined to be the irrelevance of such materials. In *Haroco I*, the plaintiff sued its bank for allegedly defrauding the plaintiff by calculating interest rate payments on loans at an announced prime rate that was higher than the defendant's actual undisclosed prime rate.[247] The defendant moved for summary judgment and predicated this motion on an analysis of loans showing that the alleged interest rate disparities did not really exist. In response, the plaintiff argued that the category of loans analyzed by the defendant was not sufficiently broad and moved pursuant to Rule 56(f) for discovery to analyze additional loans.[248]

In particular, the plaintiff sought discovery of certain computer tapes in order to analyze other loans. In support of this effort, the plaintiff argued that the computer tapes would save time and ensure greater accuracy in analyzing the relevant data. Notably, the court agreed that time savings and accuracy would ordinarily warrant such discovery. The court, however, held that the information sought did not have sufficient probative value with respect to the matters at issue.[249] Essentially, the

244. *See id.* at *2.

245. *See id.* at *3; *see also* Ball v. State of New York, 101 Misc. 2d 554, 562, 421 N.Y.S.2d 328, 333 (Ct. Cl. 1979) (defendant failed to show undue burden when evidence demonstrated it could retrieve computerized information sought within 24 hours).

246. Haroco, Inc. v. Am. Nat'l Bank & Trust Co., 662 F. Supp. 590 (N.D. Ill. 1987), *vacated,* 1987 WL 17486 (N.D. Ill. 1987).

247. *See id.* at 591-92.

248. *See id.* at 593.

249. *See id.* at 596.

court found that the information sought lacked relevance.

The court's determination that the information sought lacked relevance flowed from its acceptance of the defendant's definition of the relevant category of loans at issue. Specifically, the plaintiff failed to satisfy its burden on summary judgment of coming forward with evidence of trade usage that would broaden the definition of the type of loans at issue. After accepting the defendant's narrow definition of the type of loans at issue, the court noted conflicting testimony offered by the parties as to whether the computer tapes contained information relevant to the category of loans that were the subject of the defendant's analysis. Ultimately, however, the court credited the testimony of the defendant's affiant to the effect that the computer tapes had little, if any, information relevant to the narrow category of loans at issue. Consequently, the court denied the request for discovery and entered summary judgment in favor of the defendant.[250]

Instructively, however, when presented with a motion for reconsideration that altered the court's perception of relevance, the court vacated the summary judgment and approached the request for discovery of computer tapes differently. In *Haroco, Inc. v. American National Bank & Trust Co.*[251] (*"Haroco II"*), the plaintiff came forward with evidence of trade usage indicating that the type of loans at issue were defined in the industry more broadly than defined by the defendant. Based upon this information, in *Haroco II*, the court vacated its earlier summary judgment.[252] The court then noted that this ruling revived the plaintiff's motion to compel production of the defendant's computer tapes. In addressing this issue, the court noted once again the conflicting testimony offered regarding the utility of files stored on the computer tapes. After broadening the scope of relevant materials, however, the court concluded that "the surest way to resolve this debate is to allow plaintiffs access to a copy of the tapes they seek under whatever confidentiality restrictions may be appropriate."[253]

Thus, from the two *Haroco* decisions it appears that a marginal claim of relevance for the materials sought will warrant denying discovery even where the materials sought would enhance the discovering party's ability to process information. By contrast, where the only question as to relevance relates to a technical dispute over what can be derived from the responding party's computer system, it appears that the discovering party will be given the benefit of the doubt. In arriving at this result, however, the *Haroco* court does not appear to have been

250. *See id.* at 596-97.

251. Haroco, Inc. v. Am. Nat'l Bank & Trust Co., 1997 WL 17486 (N.D. Ill. 1987).

252. *See id.* at *2-*3.

253. *Id.* at *3.

presented with serious claims by the responding party that the discovery sought presented any of the types of burdens that are often associated with discovery of evidence from computer storage media. Cases involving such claims present much more of a challenge—particularly in instances where a court cannot accept the discovering party's assertion that the information sought can be obtained from the responding party's computer system without either discrediting the responding party's claims that such information does not exist or accepting the discovering party's claim that a tangible document reflecting information supposedly contained in computer storage media is, in fact, different from the version in computer storage because of some inaccuracy or fabrication. As seen in Section IV, this problem was confronted by the courts in *Strasser v. Yalamanchi*[254] and in *Fennel v. First Step Designs, Ltd.*[255]

In *Strasser*, the plaintiff sought access to the defendant's computer system to locate information that was essential to the plaintiff's case but that the defendant claimed did not exist. Not only did the defendant claim that the information sought had been purged from the system, but the defendant proffered expert testimony that the purged information could not be retrieved and further claimed that the unrestricted access sought would jeopardize privileged and confidential materials. In the face of the parties' competing interests, the court denied the requested discovery unless the defendant could make a satisfactory offer of proof. The elements of the required proffer, however, included only logistical matters such as the technical feasibility of the proposed data retrieval, the relative lack of intrusiveness of the discovery procedure, and the parameters and restrictions needed to prevent overly broad disclosure or harm to the responding party's computer and databases.[256]

Similarly, in *Fennel*, the court required an offer of proof where the plaintiff sought access to the defendant's computer system to locate an electronically stored version of a document, which version the plaintiff claimed would demonstrate the hard copy version of the same document to have been deceptively antedated. As in *Strasser*, the defendant came forward with evidence that the information sought was not technically capable of retrieval, that the procedure proposed by the plaintiff would expose privileged and confidential information, and that the procedure proposed also presented a variety of business risks. Much like the court in *Strasser*, the court in *Fennel* resolved the parties' competing interests by denying the proposed discovery on the ground that the plaintiff had failed to proffer sufficient evidence. Like the *Strasser* court, the *Fennel* court required a proffer as to the technical feasibility of the proposed pro-

254. Strasser v. Yalamanchi, 669 So.2d 1142 (Fla. Ct. App. 1996).

255. Fennel v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996).

256. *See supra* notes 148-54 and accompanying text.

cedure. Unlike *Strasser*, however, the *Fennel* court also required a proffer of independent evidence supporting the claim sought to be proved through computerized evidence—namely, that the document in question was back-dated. *Fennel*, however, presented the unusual circumstance, not present in *Strasser*, of a Rule 56(f) motion, which itself requires a proffer to obtain discovery.[257]

Thus, the handful of decisions in which courts have considered whether to grant or deny access to computer-related evidence raises the questions of when courts will require offers of proof as a prerequisite to obtaining such discovery and what such offers must contain. These questions should be answered first by resorting to the traditional tools afforded by the law of discovery for weighing the benefits and burdens presented by any particular form of discovery.

Foremost among these tools is the presumption in favor of disclosure. Attendant to this presumption is the burden placed on the responding party to come forward with competent evidence demonstrating that the information sought by the discovering party falls within one or more of the narrow categories of materials that are properly shielded from the discovery process. Thus, it is the responding party and not the discovering party who must make an offer of proof, in the first instance. This procedural framework is particularly important in light of the unfamiliar and technical nature of discovery into computer-related materials, which may make it tempting to assume that this form of discovery presents dangers and burdens that have not been demonstrated by persuasive evidence.[258] Therefore, until such dangers and burdens have been demonstrated, the discovering party is entitled to the requested discovery.[259] Moreover, in assessing claims that such dangers and burdens exist, courts must be sensitive to the differences between the types of computer storage media that are the subject of the requested discovery and to the various types of protective measures available in these media.

If the responding party is able to demonstrate that the discovery sought encompasses materials that are properly shielded from discovery

257. *See supra* notes 121-40 and accompanying text.

258. *Cf.* Berndt, *supra* note 33, at 77-78 (noting that, although courts have been willing to shift costs of computer-related discovery, use of computers in discovery can, in fact, decrease total litigation expense).

259. One example of a case in which concerns over disruptions to business operations appear to have been a clear subtext to the decision is Fennell v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996). For instance, in that case, the court observed that the responding party "expressed concerns over business risks resulting from accidental data loss, incompatible hardware, and system downtime." *Id.* at 532 n.6. Similarly, the court observed that the responding party "argued that the unknown mirroring process and analysis of its system might temporarily or permanently affect their computer system and business operations." *Id.* at 533. It is unclear from the decision, however, whether and to what extent these arguments were supported by competent proof.

and if that protection does not amount to a categorical shield of all the materials sought, then the burden will shift to the discovering party. It is at this point, where the discovering party must offer competent proof supporting such matters as need for the materials sought and the relative non-intrusiveness of the requested discovery. Yet, if the discovering party can come forward with persuasive evidence that the procedure to be employed in copying and/or retrieving materials from computer storage media will safeguard protected materials from exposure without imposing an inordinate burden, then the offer of proof should not be required to go any further. In many cases, however, discovery of computer-related evidence will necessarily entail some danger of exposing confidential information, and of imposing burdens and disruptions greater in magnitude than those associated with conventional discovery.[260] In these instances, the need for the evidence to be discovered (*i.e.*, the likelihood that the discovery sought will yield probative evidence for which there is no readily available substitute) assumes importance. Where relevance is established and the computer-related materials sought are the only existing source of the information in question, the need for and, hence, the right to obtain the requested discovery is usually clear.[261] By contrast, it is in cases such as *Fennel*, where another purported source of the information in question exists, albeit in a form whose reliability is questioned, that courts may be more likely to demand an offer of proof that gives some reason to question how well the alternative source of information will serve as a substitute for computer-related discovery.

The precedential value of each of these cases, however, must be assessed in light of the particular mix of benefits and burdens presented by the discovery sought in these cases. For example, a case such as *Fennel* must be seen as a case in which the discovery sought posed heavy burdens in the service of gaining questionable benefits. Thus, courts should be hesitant to infer from such a case any hard and fast rule about matters such as discovery into an opponent's hard drive for purposes of demonstrating fraud in the creation of a document from a computer system. Indeed, one respected commentator has observed that the broad scope of discovery under the Federal Rules of Civil Procedure serves as a palliative to the ever-present danger that computers will be used fraudulently

260. *See, e.g.*, Am. Brass v. United States, 699 F. Supp. 934, 937 (C.I.T. 1988) ("A higher risk of unauthorized disclosure of confidential printouts warrants a heightened level of protection for computer tapes.") (citation omitted). Indeed, if not done properly by a qualified technician, the discovery of evidence from computer storage media can endanger both the particular storage media to be accessed and the computer system in general. *See* Brill, *A Lawyer's Place in Cyberspace, supra*, note 18, at 10.

261. *See supra* note 154 and accompanying text.

to manufacture or manipulate evidence.[262]

2. *Protective Orders*

A second way in which courts balance the benefits and burdens of computer-related discovery is by restricting and conditioning disclosure of materials through a protective order. The availability of such protective measures is often dispositive of the access question, as courts conclude that appropriate protective orders justify allowing discovery of computer-related materials.[263] This Sub-Part reviews some of the different balances that can be struck in fashioning protective orders.

One of the most restrictive forms of protective conditions available is to limit access to a party's attorneys only.[264] With regard to trade secret materials, as long as the attorneys granted access are not involved in competitive decisionmaking, the level of protection afforded by such a restriction is generally considered to be strong.[265] Of course, such a protective condition would not adequately safeguard privileged or work product information contained in any production of materials.

Although restricting disclosure to outside counsel is generally an inviting alternative for a party seeking maximal protection, in the context of computer-related discovery, the discovering party will often need some expanded form of disclosure. In particular, most lawyers will need some form of technical assistance to retrieve and process computer-related materials, and they may need experts to testify based on such evidence.[266] Thus, in *American Brass v. United States*,[267] the court held that production of computer tapes to outside counsel should not be foreclosed by the mere fact that attorneys who would be granted access would need to rely on third parties to assist in processing the informa-

262. *See* 6 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE, § 1001.11[2] (Joseph M. McLaughlin ed., 2d ed. 1998).

263. *See, e.g.*, Haroco, Inc. v. Am. Nat'l Bank & Trust Co., 1987 WL 17486, *3 (N.D. Ill. 1987); *Am. Brass*, 699 F. Supp. at 937; Dunn v. Midwestern Indemn., 88 F.R.D. 191, 198 (S.D. Ohio 1980); Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972); Computer Teaching Corp. v. Courseware Applications, Inc., 199 Ill. App. 3d 154, 157-58, 596 N.E.2d 816, 818, 845 Ill. Dec. 198, 200 (Ill. App. Ct. 1990), *appeal denied*, 133 Ill. 2d 553, 561 N.E.2d 688, 149 Ill. Dec. 551 (1989).

264. *See supra* notes 208-211 and accompanying text.

265. *See* 3 MILGRIM, *supra* note 206, § 14.02[4][f] (noting tendency of courts to assume that restriction of disclosure to attorneys only will provide adequate protection); Brown Bag Software v. Symantic Corp., 960 F.2d 1465, 1470-71 (9th Cir. 1992) (citing U.S. Steel Corp. v. United States, 730 F.2d 1465, 1468 n.3 (Fed. Cir. 1984)) (holding that disclosure should be prohibited to attorneys involved in competitive decisionmaking), *cert. denied*, 506 U.S. 869 (1992). Even this level of protection, however, cannot prevent inadvertent disclosures or prevent willful or reckless disregard of a protective order, and some materials may be so sensitive as to justify denying disclosure of them altogether. *See supra* note 211.

266. *See* 3 MILGRIM, *supra* note 206, § 14.02[4][f].

267. Am. Brass v. United States, 699 F. Supp. 934 (C.I.T. 1988).

tion. "To conclude otherwise would effectively make computer tapes unavailable in any case where counsel find it necessary to seek the assistance of computer programmers."[268]

To be sure, a responding party may have valid reasons for objecting to disclosure of confidential information to an expert retained by the discovering party. For instance, the expert may be a competitor of the responding party.[269] Similarly the expert may be a former employee of the responding party, which may compound any disclosure.[270] In such instances, protective orders can employ procedures for screening and disqualifying objectionable experts.[271]

In some instances, clients as well as experts may need access to the opponent's computer-related materials in order to assist in the litigation of the case. In such instances, measures can be taken to restrict the conditions of disclosure and the types of information subject to disclosure. Such measures may be useful for preventing or limiting disclosure not only of trade secret materials but, in some cases, also of privileged and work product information.

For instance, in some cases, disclosure to individuals other than attorneys may be made possible by restricting the location at which computer-related evidence will be processed. For example, in *American Brass*, the fact that third parties would assist counsel in processing the computer tapes in question may not have been so great of a concern in light of the fact that all processing of the tapes would be performed at a computer facility on the business premises of the discovering party's attorneys.[272]

In addition, courts can preserve confidentiality and prevent damaging disclosures of privileged or work product information by ordering that materials to be disclosed first be subjected to screening procedures. The most basic and probably least protective form of screening would be to allow the discovering party to designate an individual to conduct a preliminary review of computer-related evidence to select those portions that would be produced. Thus, one court deemed "extremely reasonable" a proposal by the producing party that the discovering party conduct a preliminary review of a computer program whose production was re-

268. *Id.* at 939.

269. *See, e.g.*, Mid-Atlantic Equip. Corp. v. Cape Country Club, Inc., 1997 WL 535156, *3 (E.D. Pa. 1997) (entering protective order prohibiting disclosure of confidential information to expert who is competitor); Langer v. Dista Prods. Co., 1991 WL 349606, *2 (N.D. Ill. 1991) (same).

270. *See* 3 MILGRIM, *supra* note 206, § 14.02[4][e] (noting that courts will prohibit use of former employee of opponent as expert).

271. *See id.* § 14.02[4][g][ii] (sample protective order which provides for identifying proposed experts and giving opponent opportunity to object to use of identified experts).

272. *See id.* at 937.

quested. After undertaking this review, the discovering party could select specific portions of the program for production.[273]

Of course, the preliminary screening can be fashioned in a more protective manner, such as by limiting the individuals who may conduct the screening and by allowing the producing party to seek additional protections with regard to materials that are selected for production. One example of a more elaborate form of screening was employed in the case of *Easley, McCaleb & Assoc. v. Perry*,[274] which involved discovery of deleted files from a hard drive. In this case, the court provided that each party would designate an unaffiliated computer technician to assist in recovering information from the producing party's hard drive. The two technicians would jointly access the hard drive and create two complete backup images, both of which would be deposited in the court under seal. The technicians would print hard copies of directory and file lists for both active and deleted files. The producing party would be afforded an opportunity to redact privileged items, and the court would review *in camera* both redacted and unredacted copies of the print-outs. The court further protected privileges and other rights inhering in the information by ordering that the two computer technicians neither disclose nor reveal the nature or content of any information designated as private or privileged and by further ordering that, by disclosing such materials to the technicians, the responding party does not waive any rights or protections inhering in the materials.[275]

Arguably, the disclosure of such basic information as mere file names and dates that documents were created will not implicate protections afforded by privileges or work product immunity. These doctrines do not protect the fact that a communication occurred, the topic or purpose of the communication, the date and time of the communication, and the identities of the parties to the communication.[276] Although a file name may reveal substance beyond the mere topic of the communication, a party that stores protected and unprotected information in mingled

273. *See* Rates Tech., Inc. v. Elcotel, Inc., 118 F.R.D. 133, 135 (M.D. Fla. 1987).

274. Easley, McCaleb & Assoc. v. Perry, No. E-26663 (Ga. Super. Ct. July 13, 1994). This case was reported in *Current Developments: Litigation,* COMPUTER LAW., Sept. 1994, at 28.

275. *See id.*; *see also* Timken Co. v. United States, 659 F. Supp. 239, 243 (C.I.T. 1987) (ordering that party producing data may select data services company that will copy computer tapes and redact confidential information and requiring discovering party to pay for costs of copying and redacting).

276. *See* ROGER S. HAYDOCK & DAVID F. HERR, DISCOVERY PRACTICE § 2.9 (1996). Indeed, under Rule 26(b)(5), wherever a party withholds information from discovery based upon a claim of privilege or work product immunity, that party must "describe the nature of the documents, communications, or things not produced or disclosed in a manner that, without revealing information itself privileged or protected, will enable other parties to assess the applicability of the privilege or protection." FED. R. CIV. P. 26(b)(5).

fashion with such revealing file names may have to bear some of the risk of exposure, in order to allow parties to conduct legitimate discovery of the unprotected information, particularly where the disclosure is limited in the first instance to a technician-intermediary who is bound by protective order.

Not only can disclosure be limited by using file names as a screening device, but technology provides other potential screening devices. For instance, information can be retrieved from databases and computer storage media by conducting searches for key words or terms that are likely to appear only in the particular documents or files that are sought.[277] Thus, a narrowly focused search of materials copied from computer storage media may facilitate a limited disclosure of relevant materials that either do not encompass or only minimally encompass sensitive information.

Finally, where materials whose production is requested are highly sensitive and where alternative protections are inadequate, the court may appoint an independent expert to assist with the discovery of computer-related evidence.[278] Such an expert may conduct an investigation and report findings to the court as was done in the case of *Cerruti 1881 S.A. v. Cerruti, Inc.*[279] Such an expert might also conduct a review solely for ensuring that disclosure to the discovering party is limited to properly discoverable materials.[280]

Thus, from the fact that a computer network is used pervasively in the course of a company's operations courts should not presume that discovery of computer-related materials will necessarily jeopardize privileged or confidential information. The party resisting discovery still retains the burden of demonstrating that such privileged or confidential information exists within the scope of the discovery sought and that protective conditions under which the discovery is to be conducted would not suffice to prevent the threatened harm from occurring. In light of the limitless possibilities for fashioning protective orders, and in light of changing technology, numerous perceived obstacles to discovery can be overcome.[281]

3. *Cost Allocation*

A third way in which courts balance the benefits and burdens of computer-related discovery is by allocating costs. Although discovery of

277. *See supra* note 30 and accompanying text.

278. *See* Dunbar, *supra* note 3, at 38; Kashi, *How to Conduct On-Premises Discovery*, *supra* note 4, at 28; Soma & Austin, *supra* note 44, at 516; 8 WRIGHT, *supra* note 65, § 2043.

279. Cerruti 1881 S.A. v. Cerruti, Inc., 139 F.R.D. 573 (S.D.N.Y. 1996). *See supra* notes 178-79 and accompanying text.

280. *See* Soma & Austin, *supra* note 44, at 516.

281. *See* 8 WRIGHT, *supra* note 65, at § 2043.

computer-related materials may increase efficiencies and reduce some of the costs of litigation, computer-related discovery may also increase some of the costs associated with discovery.[282] For example, a party may have to create new software programs to obtain from its computers information requested by the discovering party, or it may have to shut down its computer system in order to facilitate discovery procedures. In addition, discovery of an opponent's computer data may expose sensitive information, thereby necessitating screening procedures and imposing risk.

Although the Rules provide tools to allocate such costs, the framework that the Rules provide for cost allocation in conventional discovery does not precisely fit computer-related discovery, and the discretion that the Rules afford courts to adjust the allocation leaves much uncertainty as to how and when such adjustments should be undertaken. Indeed, cost allocation for discovery of computer-related evidence has been litigated all the way to the Supreme Court[283] and, nonetheless, remains clouded. Commentators have noted judicial authority and even a judicial tendency to allocate costs of computer-related discovery, but have provided little in the way of precise guidance as to how the task should be performed.[284]

As with other areas in which courts balance the benefits and burdens associated with computer-related discovery, the Federal Rules of Civil Procedure provide the starting point for analysis. In the area of cost allocation, however, the guidance provided by the Rules is far less certain. Typical of this uncertainty, the Supreme Court has articulated two contrapuntal themes underpinning the Rules. First, a party must generally bear the burden of financing its own case.[285] This principle is implicit in Rule 54(d), which awards costs to the prevailing party in the discretion of the court and in 28 U.S.C. § 1920, which specifies limited categories of costs that may be awarded and which does not include attorneys' fees unless specifically authorized by a separate law.[286] The principle also underlies the work product doctrine, which protects the fruits of each party's trial preparation labors from discovery by the other

282. *See* Friedman, *supra* note 30, at 1491.

283. *See* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978).

284. *See* Berndt, *supra* note 33, at 77-78; Fromholz, *supra* note 30, at 454; Long, *supra* note 28, at 408. Although some commentators offer suggestions for cost allocation, they do so without following the precise burden-shifting mechanisms provided by the Rules and without acknowledging the manner in which computer-related discovery is often incompatible with the burden-shifting mechanisms provided by the Rules. *See* Friedman, *supra* note 30, at 1491-93; Sherman & Kinnard, *supra* note 29, at 295-98.

285. *See id.* at 356 (citing Eisen v. Carlisle & Jacquelin, 417 U.S. 156, 179 (1974)).

286. *See* FED. R. CIV. P. 54(d); 28 U.S.C. § 1920; *see generally* 10 MOORE, *supra* note 94, §§ 54.103, 54.170.

party.[287] Second, a party responding to discovery requests generally must bear the expense entailed by any response.[288] This principle is explicit in Rule 26(c), which places the onus on the responding party to seek protection from expense, and offers such protection only where the expense is undue.[289]

Accordingly, while generally the discovering party must finance the costs of obtaining what that party needs to litigate its case, in those specific instances where the Rules impose requirements on the responding party, the responding party must bear the costs entailed by those obligations, unless the Rules provide otherwise. Even where those Rules directly applicable to discovery expressly impose obligations on the responding party, the Rules often subtly shift the cost of compliance to the discovering party. For example, when the discovering party serves interrogatories seeking information that can be derived from business records and where the cost of deriving that information is substantially the same for each party, the responding party need not undertake the burden of culling this information but, rather, may simply identify those records and make them available to the discovering party for inspection.[290] Similarly, when the discovering party serves a request for the production of documents, the discovering party cannot compel its opponent to make photocopies of the documents at the opponent's expense but, rather, can only compel its opponent to make the documents available for the discovering party to inspect and copy.[291] Thus, the Rules indirectly impose on the discovering party much of the cost associated with obtaining discovery.

Moreover, in some instances, the Rules impose such costs on the discovering party more directly. For instance, when the discovering party deposes an opponent's testifying expert, the discovering party must pay that expert a reasonable fee for the time spent in responding to the discovery.[292] Similarly, in those instances when the discovering party is able to obtain discovery from an opponent's nontestifying expert, the discovering party must pay a fair portion of the fees and expenses reason-

287. *See* FED. R. CIV. P. 26(b)(3), advisory committee note ("[T]he requirement of a special showing for discovery of trial preparation materials reflects the view that each sides informal evaluation of its case should be protected, that each side should be encouraged to prepare independently, and that one side should not automatically have the benefit of the detailed preparatory work of the other side."); Hickman v. Taylor, 329 U.S. 495, 516 (1947) (Jackson, J., concurring) ("Discovery hardly was intended to enable a learned profession to perform its functions either without wits or on wits borrowed from the adversary."); *see generally* Friedman, *supra* note 30, at 1485.

288. *See Oppenheimer Fund*, 437 U.S. at 358.

289. *See* FED. R. CIV. P. 26(c); *see also Oppenheimer Fund*, 437 U.S. at 358.

290. *See* FED. R. CIV. P. 33(d).

291. *See* FED. R. CIV. P. 34(a).

292. *See* FED. R. CIV. P. 26(b)(4)(A)(i).

ably incurred by the opponent.[293] According to the Advisory Committee, this compensation reflects the notion "that it is unfair to permit one side to obtain without cost the benefit of an expert's work for which the other side has paid, often a substantial sum."[294] With regard to either type of expert, the court has the discretion not to impose such costs on the discovering party where "manifest injustice would result. . . ."[295]

Because cost allocation for expert discovery is more clear, expert discovery is a logical starting for the analysis. Under Rule 26(b)(4)(C), the cost of discovering computer-related materials from an opponent's expert will generally be borne by the discovering party. Thus, in the case of *Pearl Brewing Co. v. Jos. Schlitz Brewing Co.*,[296] the court ordered the plaintiff both to produce all system documentation revealing the details of computer programs that would form the basis of the plaintiff's economics expert's testimony, and to make available for deposition non-testifying computer experts who could interpret the computer programs. The court also required the defendant to pay all costs related to this discovery.[297] In this instance, the computer-related nature of the discovery only provides a context for the basic application of the cost allocation rule for expert discovery.

The analysis may be somewhat more complicated, however, where the materials encompassed within the production of computer-related expert discovery include databases developed by the responding party for its own use in the litigation and will provide the discovering party with value in the litigation. In such instances, courts must steer between, on the one hand, allowing the discovering party a "free ride" off the work done by the responding party in compiling the database and, on the other hand, allowing the responding party to have its compilation work funded by a discovering party who needs access to the database in order to meet that evidence at trial.[298] In these situations, courts have responded by requiring the discovering party to pay only a "fair portion" or an equal portion of the fees and expenses incurred in compiling the database.[299] These results are consistent with Rule 26, insofar as that rule only re-

293. *See* FED. R. CIV. P. 26(b)(4)(A)(ii).

294. *See* FED. R. CIV. P. 26(b)(4)(C), advisory committee note (citations omitted).

295. FED. R. CIV. P. 26(b)(4)(C).

296. Pearl Brewing Co. v. Jos. Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976).

297. *See id.* at 1138-41.

298. *See* Friedman, *supra* note 30, at 1485; Sherman & Kinnard, *supra* note 29, at 295.

299. *See* Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648, 651 (W.D. Ky. 1987) (where plaintiff's expert developed database of information produced by defendant to plaintiff, and where plaintiff was ordered to produce database to defendant, defendant was required to pay fair portion of fees and expenses incurred by plaintiff's expert); Fauteck v. Montgomery Ward & Co., 91 F.R.D. 393, 399 (N.D. Ill. 1980) (where defendant developed database in connection with litigation, court conditioned production of database on plaintiff's willingness to reimburse defendant for half of compilation costs).

quires the payment of a "reasonable fee" for discovery from a testifying expert and "a fair portion of the fees and expenses" for discovery from a non-testifying expert, and insofar as the rule does not require such payments where "manifest injustice would result. . . ."[300]

Outside the expert context, a similar problem to the "free riding" problem can occur when a party maintains computerized records that are insufficiently accurate to suit the litigation needs of the discovering party.[301] For instance, in *Penk v. Oregon St. Bd. of Higher Educ.*,[302] a group of faculty members at the defendant university brought a sex discrimination suit, and the plaintiffs sought discovery of the defendant's central computer base tapes of faculty information. The tapes, however, contained inaccuracies for which the plaintiffs moved to compel corrections. The lower court held that the defendant was not required to make its computerized records more accurate than they are, in fact, maintained in the ordinary course of the defendant's business. The lower court, however, exercised its discretion under Rule 26(c)(2) to require that the parties split the costs of revising the data.[303] The Ninth Circuit affirmed, holding that the defendant had no obligation to subsidize the plaintiff's litigation costs and that the apportionment of costs was not an abuse of discretion.[304]

In *Penk*, the court's resort to Rule 26(c)(2) illustrates that, outside the expert context, how the framework of the Rules applies to computer-related discovery is less obvious, and, thus, courts may increasingly resort to discretionary exceptions to the ordinary cost allocation provisions of the Rules. For instance, in theory, when faced with a request for specific information within computer storage or for documents residing in computer storage, a party could shift the cost of discovery to the discovering party by simply making the computer records available for inspection and copying pursuant to Rule 33(d) or Rule 34(a). In practice, however, many parties will not respond in this manner either because they wish to protect privileged, work product, and trade secret information that may be mingled with other information on the system, because they wish to avoid the business interruption that would result from such an inspection, or because they have a unique ability not possessed by the discovering party to find responsive information located in their own computer systems. Thus, many parties responding to discovery requests for com-

300. FED. R. CIV. P. 26(b)(4)(C).

301. Some of the evidentiary foundational requirements relating to the accuracy of computer-related evidence are explored in more depth in § VI.C, *infra*.

302. Penk v. Oregon St. Bd. of Higher Educ., 816 F.2d 458 (9th Cir. 1987), *cert. denied*, 484 U.S. 853 (1987).

303. *See* FED. R. CIV. P. 26(c)(2) (granting district court discretion to order that "discovery may be had only on specified terms and conditions").

304. *See Penk*, 816 F.2d at 467-68.

puter-related evidence will not use the standard cost-shifting devices in Rules 33 and 34 but, rather, will employ their own technicians to locate and retrieve responsive information that can be produced in a useful format.[305] Moreover, even the responding party may not always have sufficient software programs and resources to retrieve all responsive information residing in computer storage media.[306] In such instances, some courts have required responding parties to develop or modify programs needed to extract requested information from computer storage.[307] Indeed, even where the responding party could produce the requested information in a traditional hard copy format, it has been held that the responding party can, nonetheless, be compelled to produce the same information in a machine readable or electronic format.[308] In these respects, the framework of Rules 33 and 34 does not fit aptly to the discovery of computer-related evidence.

The Rules do not, however, leave the responding party without power to obtain the sort of cost-free discovery response available under Rules 33(d) and 34(a) in the context of conventional discovery. First, the Advisory Committee Note to Rule 34 explains that computer-related discovery may implicate the sort of "undue" burden that warrants cost-shifting pursuant to Rule 26(c).[309] This rationale appears to have led at least one court to impose on the discovering party the cost of producing information in machine readable form.[310] Second, when the responding party must employ a technician to program a computer to produce information requested in discovery, the situation is arguably analogous to that covered by Rule 26(b)(4)(B), where the discovering party seeks to obtain facts known by a non-testifying expert that the responding party

305. *See* Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985); *see, e.g., In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, *1 (N.D. Ill. 1995) (defendant argued that producing e-mail requested of it would require spending $50,000 to $70,000 in compiling, formatting, searching, and retrieving responsive e-mail); *cf.* Sherman & Kinnard, *supra* note 29, at 278 (arguing that critical purpose of discovery will be frustrated where one party is handicapped in duplicating opponents litigation support system due to unique information and expertise possessed by opponent).

306. *See* Nelson, *supra* note 29, at 835.

307. *See, e.g.*, Mackey v. IBP, Inc., 167 F.R.D. 186, 188-89 (D. Kan. 1996), *reconsideration denied*, 1996 WL 417513 (D. Kan. 1996); Nat'l Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980); *see also Bills*, 108 F.R.D. at 461 (citing *Nat'l Union Elec.*).

308. *See Nat'l Union Elec.*, 494 F. Supp. at 1257; Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W.D. Va. 1972); *see also Bills*, 108 F.R.D. at 461-62 (citing *Adams*); Bell v. Auto. Club of Michigan, 80 F.R.D. 228, 233-34 (E.D. Mich. 1978) (parties ordered to cooperate in compiling database), *appeal dismissed*, 601 F.2d 587 (6th Cir.) (table), *cert. denied*, 442 U.S. 918 (1979); Friedman, *supra* note 30, at 1490 (arguing that Rule 34 gives discovering party choice of medium in which discovery shall be produced).

309. *See* FED. R. CIV. P. 34(a), advisory committee note; *see also* FED. R. CIV. P. 26(c).

310. *See* Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972).

has retained to assist in the conduct of the litigation.[311] Indeed, one commentator has even analogized litigation support systems themselves to non-testifying experts.[312] In such situations where discovery is compelled from non-testifying experts, Rule 26(b)(4)(C) requires the court to make the discovering party pay a fair portion of the fees and expenses incurred by the responding party in obtaining these facts, unless manifest injustice would result from the imposition.[313]

From these arguments, however, courts should not necessarily conclude that the cost of computer-related discovery should ordinarily be imposed on the party seeking such discovery. For instance, under the rationale of *Kozlowski v. Sears Roebuck & Co.*,[314] the discovering party should not be required to bear any discovery-related burden that results from the defendant's use of a peculiarly cumbersome recordkeeping system. First, the expense of discovering information contained in computer storage media may not have existed if the information had been maintained in a traditional recordkeeping format, although this conclusion will depend largely on the type of record involved and the circumstances of the responding party's business. Second, the fact that the responding party may face practical difficulties in employing the cost-shifting device of opening up its records for inspection under Rules 33(d) and 34(a) may be seen as attributable to the responding party's own choice to maintain a computerized recordkeeping system that is not susceptible to being made open for inspection.[315] Thus, based upon the *Kozlowski* rule, the court in *In re Brand Name Prescription Drugs Antitrust Litig.*[316] concluded that the plaintiffs should not be required to pay the estimated $50,000 to $70,000 cost of retrieving e-mail from the defendant's computer system where part of that cost was attributable to the limitations of the software program that the defendant chose to employ in its operations. Rather, the court only required the plaintiff to pay a $0.21 per page fee representing the typical photocopying cost that would be borne by a discovering party in litigation.[317]

---

311. *See* FED. R. CIV. P. 26(b)(4)(B).

312. *See* Sherman & Kinnard, *supra* note 29, at 295.

313. *See* FED. R. CIV. P. 26(b)(4)(C)(ii).

314. Kozlowski v. Sears Roebuck & Co., 73 F.R.D. 73 (D. Mass. 1976).

315. *Cf.* United States v. Davey, 543 F.2d 996, 1001 (2d Cir. 1976) (holding that cost of duplicating computer records that taxpayer must produce to IRS is "reasonable cost of doing business which should be borne by the taxpayer").

316. *In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 60526, *2-*3 (N.D. Ill. 1995).

317. *See id.* at *3; *see also* Daewoo Elecs. Co. v. United States, 650 F. Supp. 1003, 1006 (C.I.T. 1986) ("It appears to the court that the placing of this data into sequential files is comparable to the normal ordering of files which would have to be done by the respondent in routine discovery of documents. The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable

In addition to the *Kozlowski* rule, there may be other reasons not to impose on the discovering party the cost of obtaining computer-related information from an opponent. First, there may be gross disparity in the ability of the respective parties to pay for the discovery at issue, and obtaining the information may be a relatively routine task for the party from whom the information is requested.[318] Second, there may be some benefit to the responding party in its case from producing the information.[319] Third, although there is expense attendant to hiring a technician to screen from production sensitive materials in computer storage media, many parties in litigation routinely subject their documents to extensive review by attorneys before production. There is no measurable data on whether the expense of such review is increased by having a technician screen materials stored electronically and, if so, by how much. Indeed, it is entirely possible that the expense of such review could be reduced in situations where technicians can screen privileged materials by simply performing an electronic search for documents containing an attorney's name.

Thus, there are several reasons why it may not be appropriate to impose the costs of computer-related discovery on the party conducting discovery. Nonetheless, these precise reasons did not carry the day for the discovering party that asserted them in the one case to present the Supreme Court with the question of how to allocate the costs of computer-related discovery. Due to the peculiar context of this decision, however, the case has limited precedential value and adds little clarity to the debate. Indeed, read carefully, the Court's decision actually supports the relevance to cost allocation of at least some of the factors described above.

Specifically, in *Oppenheimer Fund, Inc. v. Sanders*,[320] the Supreme Court overturned a district court ruling that had imposed on an investment fund the cost of compiling a list of class members' names and ad-

---

burden of a respondent in the absence of a showing of extraordinary hardship."); Bills v. Kennecott Corp., 108 F.R.D. 459, 463-64 (D. Utah 1985) (holding that one factor weighing against finding of undue burden was "that information stored in computers should be as freely discoverable as information not stored in computers"). Although these decisions only reject cost-shifting arguments grounded in Rule 26(c), the same *Kozlowski* rationale would apply equally with respect to an effort to analogize computer-related discovery to discovery of a non-testifying expert under Rule 26(b)(4)(B). If the information requested had been maintained in a traditional format, it would be unlikely that the responding party would need the equivalent of expert assistance to respond. Thus, under this view, the need for a technician to extract information may be seen as resulting from the responding party's own choice of how to maintain its records.

318. *See* Mackey v. IBP, Inc., 167 F.R.D. 186, 199 (D. Kan. 1996), *reconsideration denied*, 1996 WL 41753 (D. Kan. 1996); *Bills*, 108 F.R.D. at 464.

319. *See Bills*, 108 F.R.D. at 464.

320. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978).

dresses that was sought by the class plaintiffs. This list was requested by the class plaintiffs to help them send to class members the notice ordered by the Court under Rule 23(d) of the Federal Rules of Civil Procedure.[321] To compile such a list, the fund would have needed to employ a third party to sort through voluminous paper records, to keypunch between 150,000 and 300,000 computer cards, and to create eight new computer programs at a cost of $16,000 in 1973 dollars.[322] Although the Court held that the plaintiffs' request for this information was governed by Rule 23(d), which generally imposes the cost of sending class notification on plaintiffs, rather than by the rules of civil discovery, the Court looked to the civil discovery rules as analogous authority in assessing whether the district court properly exercised its discretion under Rule 23(d) by placing the responsibility and cost of deriving the information sought on the fund.[323]

The Court broke its analysis into two steps: (1) determining which party should be responsible for culling the information sought; and (2) if that responsibility is placed on the responding party, determining whether the responding party may shift the cost of that responsibility to the discovering party. In determining which party should be responsible for culling the information, the Court noted that, as a general rule, the representative plaintiff bears the burden of sending class notification under this rule. The Court, however, then held that, in some situations, where "the defendant may be able to perform a task with less difficulty or expense than could the representative plaintiff," the district court has discretion to order the defendant to perform the task itself.[324] In reaching this result, the Court analogized to Rule 33, which enables a defendant to respond to an interrogatory by producing business records, where the cost of to each party of deriving the information sought is substantially the same. Thus, where the cost to each party of deriving the information is substantially the same, Rule 33 imposes responsibility for the task that generates this cost on the party who would benefit from the information, much like Rule 23(d) imposes the task of class notification on the party who would benefit from that notification. But where the cost of deriving the information sought is substantially less for the responding party, then Rule 33 requires the responding party to undertake that task.[325] Thus, where the difficulty or expense of deriving class notification-related information from computer storage media is substantially less for the defendant than for the class plaintiffs, the court has

321. FED. R. CIV. P. 23(d).

322. *See Oppenheimer Fund*, 437 U.S. at 345.

323. *See id.* at 349-63.

324. *See id.* at 356.

325. *See id.* at 357.

discretion to order the defendant to obtain this information for the plaintiff.

After addressing the district court's discretion to impose on the defendant the task of gathering class notification-related information, the Court then turned to the issue of whether the cost of that task should be shifted to the plaintiffs. The Court held that the district court has similar discretion to determine which party shall bear the costs of this task. In determining how this discretion should be exercised, the Court analogized to the cost-shifting power of courts under Rule 26(c). The Court noted, however, that, unlike Rule 26(c), which shifts costs to the discovering party as the beneficiary of the task giving rise to such costs, in the Rule 23(d) context, the defendant's own case will rarely benefit from the notification task. Thus, as long as the cost of the notification-related task is merely "substantial" rather than "undue," the plaintiff should bear that cost. In some instances, however, the Court noted that "it may be appropriate to leave the cost where it falls because the task ordered is one that the defendant must perform in any event in the ordinary course of its business."[326]

The Court then held that the district court abused its discretion by imposing on the defendant the cost of compiling the notification-related information. In particular, the Court found that the plaintiffs had the right to control the records in question and that the expense of culling the information would be no greater for the plaintiffs than for the fund.[327] The Court specifically rejected the argument that the fund should be required to bear the cost due to the relatively modest size of the expense in comparison to the fund's total assets. Although the Court found that the ability of a party to bear the expense may be relevant in some cases, the district court's comparison was improper in light of the rule that costs can only be shifted when those costs are undue and not merely substantial.[328] Finally, the Court rejected a *Kozlowski*-type argument that imposing the cost on the defendant was warranted either to create a disincentive for potential defendants to bury information in computer storage media in a manner that makes retrieval difficult or to ensure that no greater burden is imposed on the discovering party due to the responding party's use of computer storage media instead of more traditional recordkeeping systems. The Court found these arguments inapplicable insofar as there was no suggestion that the fund had tried to conceal any information and insofar as there was no reason to believe that the information sought would have been more easy to extract if it

326. *See id.* at 358-59.

327. *See id.* at 359-60.

328. *See id.* at 361-62.

had been stored in a less modern form.[329]

At bottom, the discretionary exercise of a court's authority to allocate costs is inherently uncertain, and the peculiar context of *Oppenheimer Fund* limits that decision's value for reducing that uncertainty in the context of computer-related civil discovery. Some aspects of the decision, however, are instructive, even if by analogy. First, courts should consider which party may be able to perform tasks required for computer-related discovery with substantially less difficulty or expense.[330] Second, the Court specifically noted that, under Rule 26(c), whether a party's own case will benefit from the discovery sought will be relevant to determining whether that party should bear some of the expense.[331] Third, in determining how to allocate costs, it may be relevant that the task involved is one that one of the parties must routinely perform in the course of its business.[332] Fourth, the relative inability of one of the parties to pay may be a relevant circumstance in determining which party should bear the costs of computer-related discovery, although this consideration is likely to be a minor one.[333]

Thus, read carefully, *Oppenheimer Fund* supports the use of many of the factors relied on by other courts to allocate costs in the context of computer-related discovery, even though those factors were not successful for the party who advanced them in that case. Indeed, even the Court's rejection of the *Kozlowski*- type arguments were narrowly limited to the circumstances of "this case."[334] Specifically, although there was no reason to believe that the names and addresses of so many class members could have been more easily retrieved from some more conventional form of storage, in other cases there may be reason to believe that the records in question are of a variety that would have been easily accessible if they had been maintained in a more conventional format or that the particular form of computer storage used by the responding party was peculiarly cumbersome in comparison to other computer storage systems.[335]

Accordingly, much like the handful of precedents in the context of computer-related discovery, *Oppenheimer Fund* leaves courts with several factors to weigh in determining how to allocate costs entailed by

329. *See id.* at 362-63.

330. *See id.* at 356.

331. *See id.* at 358.

332. *See id.* at 359.

333. *See id.* at 361-62.

334. *See id.* at 362.

335. *See, e.g., In re* Brand Name Prescription Drugs Antitrust Litig., 1995 WL 360526, * 2-*3 (N.D. Ill. 1995).

such discovery.[336] In weighing such factors, courts must be mindful of the fact that Rule 26(c) places the burden of persuasion on the party responding to such discovery requests.[337] The difficult task courts must face is determining whether that burden should be lessened by virtue of the fact that the responding party will often be unable to avail itself of the cost-shifting devices in Rules 33(d) and 34(a) where the information sought resides in computer storage media or must be generated by computer systems. In making this determination, courts must balance the need to preserve inexpensive access to relevant information that has traditionally been available at little expense in conventional discovery with the need to avoid penalizing the use of new technologies with whose evolution the Rules have not kept pace. In light of the competing mix of potential interests that may be presented by different parties in different cases, courts will probably continue to balance the factors discussed in this Sub-Part in an *ad hoc* fashion, while avoiding the question of whether a fundamental recalibration is needed to make up for the loss of the burden-shifting mechanisms in Rules 33(d) and 34(a).

Finally, it should be noted that technology may increasingly offer solutions to minimize costs and, thereby, avoid or reduce the cost-shifting problem. For example, one recent case in the Seventh Circuit may foretell the future path of courts through cost allocation. In *Sattar v. Motorola, Inc.*,[338] the plaintiff moved to compel the production of 210,000 pages of hard copy reflecting e-mails. The defendant had produced these e-mails, but in the form of tapes for which the plaintiff did not have the necessary software to obtain access. Rather than simply ordering the production in hard copy, the district court allowed the defendant to use a combination of downloading the data from the tapes to conventional computer disks or a computer hard drive, loaning the plaintiff a copy of the necessary software, or offering the plaintiff on-site access to the defendant's computer system. In the event these options did not afford sufficient access, the district court ordered the production in hard copy, with each party to bear half the costs of copying. When the plaintiff appealed this decision, the Seventh Circuit found the district court's resolution to be "entirely reasonable . . . and far from an abuse of discretion."[339]

Before leaving the subject of cost allocation, one last aspect of the subject deserves mention—namely, the award of costs to the prevailing party. As noted, Rule 54(d) states, as a general rule, that "costs shall be allowed as of course to the prevailing party. . . ."[340] These costs are spec-

336. *Accord* Bills v. Kennecott Corp., 108 F.R.D. 459, 463-64 (D. Utah 1985) (applying case-specific, multi-factor approach).

337. *See* FED. R. CIV. P. 26(c).

338. Sattar v. Motorola, Inc., 138 F.3d 1164 (7th Cir. 1998).

339. *Id.* at 1171.

340. FED. R. CIV. P. 54(d).

ified in 28 U.S.C. § 1920.[341] Although courts may not award costs other than those authorized by § 1920, courts may interpret the statutory language to cover expenses not explicitly listed.[342] Among the costs specified in § 1920 are those in subsection (4): "Fees for exemplification and copies of papers necessarily obtained for use in the case."[343]

Thus, through interpretation of § 1920(4), it is possible that costs associated with computer-related discovery may be recovered. So far, most reported decisions in this area have involved computerized litigation support systems. In these cases, courts have denied an award of costs on the ground that such expenses are more in the nature of expenses incident to attorneys' fees incurred in reviewing documents.[344] Where, however, such expenses arise from copying evidence from computer storage media, courts may well grant an award of costs. Such expenses may be seen as relating to "exemplification and copies of papers necessarily obtained for use in the case" within the meaning of § 1920(4).[345] For instance, some courts have allowed as costs the expenses of such items as photographs, charts, and motion pictures.[346]

By the same token, such costs will be denied when the items of expense do not materially assist the disposition of the case or where the evidence obtained is merely illustrative or repetitive of otherwise adequate evidence.[347] Recovery of such costs is limited by § 1920(4) to items

341. *See* 28 U.S.C. § 1920.

342. *See* 10 MOORE, *supra* note 94, § 54.103[3][a].

343. 28 U.S.C. § 1920(4).

344. *See* Northbrook Excess & Surplus Ins. Co. v. Proctor & Gamble Co., 924 F.2d 633, 643-44 (7th Cir. 1991) ("P & G is quite correct in arguing that expenditures for a computerized litigation support system are not taxable costs under section 1920.") (citations omitted); U.S. Indus., Ind. v. Touche Ross & Co., 854 F.2d 1223, 1246-47 (10th Cir. 1988) (upholding district court's decision not to award costs related to computerized document analysis); Chicago College of Osteopathic Med. v. George A. Fuller Co., 801 F.2d 908, 911-13 (7th Cir. 1986) (stating in *dicta* that costs of computerized document retrieval system are not recoverable); E.E.O.C. v. Sears, Roebuck & Co., 111 F.R.D. 385, 394-95 (N.D. Ill. 1986) ("As with computerized legal research, a computerized retrieval system performs the work an attorney, paralegal or law clerk would have to perform in its absence. Therefore, expenses for such systems are more properly considered expenses incidental to an award of attorneys' fees, not costs of suit . . . .") (citations omitted).

345. 28 U.S.C. § 1920(4).

346. *See* Deaton v. Dreis & Krump Mfg. Co., 134 F.R.D. 219, 224 (N.D. Ohio 1991) (awarding $600 for preparation of diagram of machine); Barth v. Bayou Candy Co., 379 F. Supp. 1201, 1205 (E.D. La. 1974) (awarding $200 for photographer's fees); Kaiser Indus, Corp. v. McLouth Steel Corp., 50 F.R.D. 5, 11 (E.D. Mich. 1970) (allowing costs of, among other things, motion pictures); *see generally* 10 MOORE, *supra* note 94, § 54.103[3][d]; *but see* Fulton Fed. Savs. & Loan Ass'n v. Am. Ins. Co., 143 F.R.D. 292, 299 (N.D. Ga. 1991) (holding such costs to be unrecoverable as outside the literal language of § 1920).

347. *See Kaiser Indus.*, 50 F.R.D. at 11 (citing H.C. Baxter & Bro. v. Great Atlantic & Pacific Tea Co., 44 F.R.D. 49 (D. Me. 1968)).

that were "necessarily obtained" for the case.[348] Thus, one court denied an award of $200 to the prevailing party to compensate for the expenditure of computer time in obtaining a tape and print-outs that were used at trial. The court found the expenditure to be "an extraordinary cost which should have been submitted to the court for approval prior to being incurred."[349] Although the increasing presence of computers in the workplace and the courtroom may ultimately change judicial perceptions of such expenses, the danger that such expenses may multiply unnecessarily will likely result in courts making such awards with caution.

VI. APPROACHING DISCOVERY ON THE ELECTRONIC FRONTIER

Although the standard discovery procedures in the Federal Rules offer ample tools for determining whether, to what extent, and under what conditions access to computer-related evidence should be afforded, discovery of computer-related evidence also often involves procedural issues that are unfamiliar to many litigators. Often these procedural issues are driven by technological factors unique to discovery in this context. These technological and procedural issues combine to present lawyers with a unique mix of strategic and tactical considerations that must be addressed in pursuing computer-related discovery. These considerations include timing of discovery, relative importance of the evidence sought both to the merits of the litigation and to the costs of the discovery procedures proposed, the discovering party's knowledge regarding the nature of the evidence sought and the nature of the opponent's computer system, the scope of discovery that would be needed to obtain the evidence sought, the invasiveness to the responding party of the proposed discovery procedures, and the discovering party's ability to conduct discovery of computer-related evidence in a manner that is likely to preserve the integrity of that evidence for use at trial.

This Section sketches a roadmap for navigating through these strategic and tactical issues. Part A reviews procedures relating to the timing of discovery. Part B addresses informational challenges in approaching computer-related discovery. Part C addresses evidentiary issues that impact computer-related discovery.

A. TIMING OF DISCOVERY

Because electronically stored information is subject to deletion at any time, and because such deleted information is subject to being overwritten at any time, commentators consistently stress the need to act

348. *See* 10 MOORE, *supra* note 94, at § 54.103[3][d]; 10 CHARLES A. WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE: CIVIL § 2677 (3d ed. 1998).

349. Wade v. Mississippi Coop. Extension Serv., 64 F.R.D. 102, 107 (N.D. Miss. 1974).

early in conducting discovery of electronically stored data—although they offer little practical advice on how to do so.[350] Yet standard discovery procedures are not geared toward such immediate action. Under Rule 26(d), the parties may not commence discovery until they have conferred to develop a proposed discovery plan.[351] As with most procedural tasks, the parties are unlikely to join in such a conference until the deadline, which is fourteen days before a scheduling conference is held or a scheduling order is due.[352] The scheduling order, however, only needs to be issued within ninety days after the appearance of a defendant and within 120 days after the complaint has been served on a defendant.[353]

Even when the parties are free to commence discovery, standard procedures do not provide for the immediate production of important evidence. Within ten days of the date on which the parties confer to develop a discovery plan, each party must serve an initial disclosure.[354] Although these disclosures might include information pertinent to computer-related discovery such as identities of individuals with relevant knowledge and categories of relevant documents and data compilations, there is no requirement at this stage to produce information contained in computer storage media.[355] Nor can opposing counsel be relied on to know the existence of or to disclose all potential sources of relevant information, such as computer storage media.

After the conference for developing a discovery plan, a party can pursue computer-related discovery more directly by serving interrogatories and requests for production and inspection of documents and tangible things, but the opposing party will have thirty days to respond to such discovery requests.[356] At the end of that thirty day period, where a request for production or inspection is served, the responding party need only provide a written response at the end of the thirty day period.[357] Indeed, where either interrogatories or requests for production or inspection are employed, the responding party may only end up serving objections, without producing the discovery sought.[358] In such instances, the discovering party must wait until objections have been resolved by negotiations between the parties or by a motion to compel presented to the

350. *See* Brill, *The Secret Life of Computer Data, supra* note 13, at 32; Davis, *supra* note 6, at 61; Dunbar, *supra* note 3, at 34; Johnson-Laird, *supra* note 5, at 7; Thomas R. Galligan, *Pursuing Electronic Documents in Discovery,* 25 MASS. LAW. WKLY 2644 (Aug. 11, 1997); Pooley & Shaw, *supra* note 2, at 62.

351. FED. R. CIV. P. 26(d).

352. FED. R. CIV. P. 26(f).

353. FED. R. CIV. P. 16(b).

354. FED. R. CIV. P. 26(a)(1).

355. *See id.*

356. FED. R. CIV. P. 33(b)(3), 34(b).

357. FED. R. CIV. P. 34(b).

358. FED. R. CIV. P. 33(b)(1), 34(b).

court.[359]

During all of this time, communications and data contained in computer storage media may be deleted in the ordinary course of business and deleted files may be overwritten from nothing more than ordinary usage of the computer system. More troubling still, where a party has used its computer system for an illicit or fraudulent purpose, once that party has been given notice that a lawsuit is pending and that discovery of computer-related materials is sought, that party may tamper with the computer system to evade detection of any wrongdoing. Thus, because of the delay entailed by standard procedures for conducting discovery, a party seeking discovery of computer-related evidence must consider extraordinary procedures. Several options are described below.

1. Ex Parte *Seizure Orders*

Of all the options available for obtaining expedited access to an opponent's computer system, none is so alluring as the *ex parte* seizure order. If the court will order the seizure of computer-related information, before the opponent has notice that the lawsuit even exists, the opponent has no opportunity to conceal or destroy evidence. Indeed, in taking the opponent by surprise and using a procedure that does not allow the opponent to select the materials to be produced, an *ex parte* seizure order may increase the likelihood of uncovering evidence of wrongdoing. Yet, of all the options available for obtaining such expedited access, none is more perilous. For the power of the court to seize a party's property without notice and an opportunity to be heard, is strictly limited by rule, by statute, and by the United States Constitution.

a. Constitutional Restrictions

Under the Constitution, any order that a party's property be seized must comport with due process.[360] In a series of cases beginning in 1969, the Supreme Court held that the due process clause forbids a wide variety of *ex parte* prejudgment remedies.[361] Although these decisions each turn on their own facts, at a general level at least three considerations govern whether such a procedure comports with due process: (1) the nature of the private interest that will be impacted by the remedy sought; (2) the risk that the remedy sought will erroneously deprive a party of its property right, particularly in light of additional or alternative safeguards that could be used in connection with the proposed rem-

359. FED. R. CIV. P. 33(b)(5), 34(b), 37(a)(2)(B).

360. U.S. CONST. amends. V & IV.

361. *See* Connecticut v. Doehr, 501 U.S. 1 (1991) (attachment); North Georgia Finishing, Inc. v. Di-Chem, Inc., 419 U.S. 601 (1975) (garnishment); Fuentes v. Shevin, 407 U.S. 67 (replevin); Sniadach v. Family Fin. Corp., 395 U.S. 337 (1969) (garnishment).

edy; and (3) the interest of the party seeking a prejudgment remedy, with regard for any ancillary interest of the government in providing the remedy sought or foregoing remedies that would entail greater protections.[362]

Some *ex parte* prejudgment remedies, however, will meet this threshold. For example, in *Mitchell v. W.T. Grant Co.*,[363] the Supreme Court upheld a statute allowing the *ex parte* sequestration of personal property under several restrictive conditions. To protect the defendant against an erroneous deprivation of property, the statute in question required that such an order be issued by a judge. The judge could only issue such an order upon an affidavit alleging specific facts showing a right to possession of the property. Under these circumstances, this procedure adequately protected against an erroneous deprivation, because the right claimed in the property was capable of determination from documentary proof and without resort to any complicated factual inquiry. Moreover, as an additional layer of protection, the statute required an immediate post-seizure hearing in which the party subjected to the remedy could challenge it. In the event that any seizure should prove to be erroneous, the statute also required the party seeking the remedy to post a bond first to protect the opponent from potential damages. Balanced against this minimized risk of erroneous deprivation, the plaintiff's interest in seizing the property at issue was strong. At issue were goods that were likely to deteriorate from daily usage. In addition, there was a real risk that the defendant would conceal or transfer the goods. Finally, balanced against the plaintiff's strong interest in seizing the goods, the defendant's interest in the goods was minimized due to the fact that the defendant's title was encumbered by a vendor's lien, which was held by the plaintiff to secure payments for the purchase of the goods—payments on which the defendant was in default.[364]

Thus, provided there are sufficiently protective conditions, *Mitchell* recognizes the preservation of property in dispute as a proper subject of prejudgment remedies. In a similar vein, the Supreme Court recognized that a summary seizure may be appropriate where there was an "immediate danger" that a party would "destroy or conceal disputed goods."[365] More broadly, the Supreme Court has recognized that *ex parte* temporary restraining orders may be issued to preserve the *status quo* and, thereby, prevent irreparable harm to a party, provided: (1) that such orders are narrowly tailored to that purpose; (2) that the party seeking the order demonstrate its irreparable injury by facts contained in sworn

362. *See Doehr,* 501 U.S. at 11.

363. Mitchell v. W.T. Grant Co., 416 U.S. 600 (1974).

364. *See id.*

365. *Fuentes,* 407 U.S. at 93.

statements; (3) that this showing include a demonstration that the threatened harm could not be protected by a procedure under which the opposing party was served with notice and an opportunity to participate; and (4) that the restraining order is of temporary duration such that it merely preserves a state of affairs until a hearing can be held on preliminary injunctive relief which the party subjected to the restraining order can be participate.[366]

In addition to the due process clause, courts must also follow the restrictions governing searches and seizures contained in the fourth amendment.[367] According to the fourth amendment, searches and seizures must not be "unreasonable" and may only be conducted upon sworn statements demonstrating "probable cause" and "particularly describing the place to be searched, and the persons or things to be seized."[368] Thus, any "search [must] be carefully tailored to its justifications and [must] not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit."[369] These protections apply in civil cases, as well as criminal cases, and to commercial premises, as well as private homes.[370]

Over and above these due process and search and seizure protections, the first amendment's protection of speech may also be implicated by seizures of materials containing expressive content.[371] Although the first amendment's protections do not apply to such unlawful materials as obscenity or copyright infringements, before such a seizure can be implemented, the first amendment requires safeguards against the seizure of materials that are, in fact, protected.[372] Nonetheless, even in the context of potentially protected content, the Supreme Court has held that a narrowly tailored *ex parte* seizure that merely seeks to preserve evidence

366. *See* Granny Goose Foods, Inc. v. Teamsters, 415 U.S. 423, 439 (1974); Sampson v. Murray, 415 U.S. 61, 88-89 (1974); Carroll v. President and Commr's of Princess Anne, 393 U.S. 175, 180 (1968).

367. U.S. CONST. amend. IV.

368. U.S. CONST. amend. IV.

369. Maryland v. Garrison, 480 U.S. 79, 84 (1987).

370. *See* Soldal v. Cook County, 506 U.S. 69, 67 & n.11 (1992); Donovan v. Dewey, 452 U.S. 594, 598-99 (1981); Marshall v. Barlow's, Inc., 436 U.S. 307, 311-13 (1978); *see also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT §§ 1.7(a) & (g), 2.4(b) (3d ed. 1996).

371. U.S. CONST. amend. I.

372. *Compare* A Quantity of Books v. Kansas, 378 U.S. 205, 208 (1964) ("We conclude that the procedures followed in issuing the warrant for seizure of the books, and authorizing their impoundment pending hearing, were constitutionally insufficient because they did not adequately safeguard against the suppression of non-obscene books.") *with* Dealer Adver. Dev., Inc. v. Barbara Allan Fin. Adver., Inc., 197 U.S.P.Q. 611, 614 (W.D. Mich. 1977) ("Constitutional objections to a writ of seizure similar to those raised by defendants have been considered and rejected by other courts. The first amendment was not intended to protect infringers of copyrights or misappropriators.") (citations omitted).

and that does not seize all copies of the content in question will pass constitutional muster.[373]

These constitutional protections have been applied in the context of civil *ex parte* seizure orders.[374] The cumulative effect of these constitutional protections is: (1) that a party seeking an *ex parte* seizure must be ready to demonstrate through specific, sworn statements that it has a right to the remedy sought and a need for the remedy to prevent the concealment, or destruction of evidence; (2) that the party seeking the seizure must be prepared to show that the harm that would be remedied by such an *ex parte* seizure could not be prevented by a less drastic remedy such as an order requiring that evidence be preserved pending an adversary hearing; (3) that the party seeking the seizure must be ready to persuade a judicial officer; (4) that the party seeking the seizure must propose specifically what that party intends to seize and where it shall be seized; (5) that the party seeking the seizure must be prepared shortly after the seizure to justify the continued seizure through an adversary hearing; and (6) that the party seeking the seizure must be prepared to post a bond that would compensate the opponent for damages that would be incurred if the seizure proves to be wrongful. It has also been held that these constitutional requirements demand that any seizure be conducted by governmental officers such as United States Marshals, rather than by the party seeking the seizure.[375] In the case of complex computer technology, however, courts have held that the law enforcement officers may be aided by a computer expert affiliated with the party seeking the seizure, as long as, the criteria for the seizure are sufficiently objective that the expert's role is restricted to applying specialized knowledge so as to identify predetermined materials.[376]

---

373. *See* Heller v. New York, 413 U.S. 483, 492 (1973) ("But seizing films to destroy them or to block their distribution or exhibition is a very different matter from seizing a single copy of a film for the bona fide purpose of preserving it as evidence in a criminal proceeding, particularly where, as here, there is no showing or pretrial claim that the seizure of the copy prevented continuing exhibition of the film.").

374. *See, e.g.*, Time Warner Entertainment Co. v. Does Nos. 1-2, 876 F. Supp. 407, 411-13 & nn. 3-4 (E.D.N.Y. 1994); Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 86-91 (E.D.N.Y. 1993); Warner Bros., Inc. v. Dae Rim Trading, Inc., 677 F. Supp. 740, 765-67 (S.D.N.Y. 1988), *aff'd*, 877 F.2d 1120 (2d Cir. 1989); *but see* Reebok Int'l Ltd. v. Su Youn Pak, 683 F. Supp. 929, 930 (S.D.N.Y. 1987) (rejecting fourth amendment challenge to seizure because seizure was implemented pursuant to statutory authority).

375. *See* Warner Bros., Inc. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1126 (2d Cir. 1989); *Time Warner Entertainment*, 876 F. Supp. at 412.

376. *See* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1264 (N.D. Cal. 1995); State v. Wade, 544 So.2d 1028, 1030-31 (Fla. Dist. Ct. App.), *rev. denied*, 553 So.2d 1168 (Fla. 1989) (table).

b. Rule 65

In addition to these constitutional restrictions, a party may only obtain an *ex parte* seizure order where authorized by statute or rule. One potential source of authority is Rule 65 of the Federal Rules of Civil Procedure, which provides for *ex parte* temporary restraining orders.[377] This rule expressly incorporates several procedural protections designed to comply with the constitutional restrictions on *ex parte* relief.[378] For instance, to ensure that the moving party has a legitimate interest in obtaining *ex parte* relief and to ensure that this interest could not be accommodated by less drastic remedies, the moving party must proffer sworn statements containing specific facts clearly demonstrating immediate and irreparable injury that would be suffered before the opponent could be afforded a hearing and must certify what efforts have been made to provide notice to the opponent and the reasons for which notice should not be required. Rule 65 further protects against an erroneous deprivation by limiting the duration of restraining orders to ten days, unless extended by another ten days for good cause shown.[379] Thus, the rule places the onus on the moving party to convert the temporary restraining order into a preliminary injunction upon notice and an adversarial hearing, where the responding party can assert its interests and challenge the process.[380] In the event the *ex parte* remedy should be found improper, the rule requires that the moving party first provide adequate security for any costs and damages that the opponent incurs.[381] Finally, in addition to the express requirements of the rule, most courts will balance the competing interests of parties and nonparties by considering factors typical of those that govern motions for preliminary injunctive relief, including the likelihood that the movant will prevail on the merits of its claim, the severity of the injury that the movant is likely to incur without temporary relief, the balance of harms between the parties, and the impact on the public interest of granting or withholding the relief sought.[382]

Fundamentally, any such preliminary or temporary injunctive relief should be designed to preserve the *status quo* pending trial.[383] Some courts, however, have held that seizure orders do not maintain the *status quo*.[384] Nonetheless, where seizure is the only way to prevent the de-

377. *See* FED. R. CIV. P. 65(b).
378. *See* 11A WRIGHT, *supra* note 65, § 2953.
379. *See* FED. R. CIV. P. 65(b).
380. *See* FED. R. CIV. P. 65(a) & (b).
381. *See* FED. R. CIV. P. 65(c).
382. *See* 13 MOORE, *supra* note 94, § 65.36[2]; 11A WRIGHT, *supra* note 65, § 2951.
383. *See* 13 MOORE, *supra* note 94, § 65.20; 11A WRIGHT, *supra* note 65, §§ 2947, 2948.
384. *See* Vuitton v. White, 945 F.2d 569, 573 n.3 (3d Cir. 1991); Warner Bros., Inc. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1125 (2d Cir. 1989) (citations omitted).

struction of crucial evidence, a seizure order may be seen as preserving the *status quo*.[385] Thus, a number of courts have issued seizure orders under Rule 65 in cases involving counterfeit goods that are susceptible to surreptitious disposal.[386] To ensure that such *ex parte* seizures do not overstep the *status quo* preservation purpose of Rule 65, courts will generally require a party seeking such an order to demonstrate that its opponent would likely disobey a court order requiring preservation of the evidence in question.[387] The moving party need not go so far as to show that its opponent has actually violated court orders in the past. Rather, the moving party can simply demonstrate that others who have been similarly situated have had a history of disposing of evidence or violating court orders.[388] Ultimately, to assure the court that an *ex parte* seizure order is necessary to preserve the *status quo*, a party seeking a temporary restraining order should be able to demonstrate to the court that there are no less drastic means that would protect the moving party's rights.[389]

c. *The Trademark Counterfeiting Act of 1984*

Another source of authority for *ex parte* seizures that is more specifically targeted to trademark counterfeiting was added to the Lanham Act in 1984. Specifically, the Trademark Counterfeiting Act of 1984 provides for seizure orders in cases where a party has used a counterfeit mark in connection with selling, offering for sale, or distributing goods or services.[390] This provision incorporates many of the same protections that apply to seizure orders under Rule 65, as well as other protections. These protections include, among others:

- The applicant must give the United States attorney such notice as is reasonable.

---

385. *See* Note, *Developments in the Law: Injunctions*, 78 HARV. L. REV. 994, 1060 (1965).

386. *See, e.g., In re* Vuitton et Fils S.A., 606 F.2d 1 (2d Cir. 1979); Brockum Int'l, Inc. v. Various John Does, 551 F. Supp. 1054 (E.D. Wis. 1982); Fimab-Finanziaria Maglificio Biellese Fratelli Fila S.P.A v. Kitchen, 548 F. Supp. 248 (S.D. Fla. 1982); Moon Records v. Various John Does, 217 U.S.P.Q. 46 (N.D. Ill. 1981); *see generally* J. Joseph Bainton, *Seizure Orders: An Innovative Judicial Response to the Realities of Trademark Counterfeiting*, 73 TRADEMARK REP. 459, 460-63 (1983).

387. *See* First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 650-51 (6th Cir. 1993); Am. Can Co. v. Mansukhani, 742 F.2d 314, 323 (7th Cir. 1984); *Vuitton et Fils*, 606 F.2d at 2-5.

388. *See First Tech. Safety Sys.*, 11 F.3d at 651; *Vuitton et Fils*, 606 F.2d at 2.

389. *First Tech. Safety Sys.*, 11 F.3d at 650 (citation omitted); *Am. Can*, 742 F.2d at 323.

390. *See* 15 U.S.C. § 1116(d)(1)(A). *See generally* J. Joseph Bainton, *Reflections on The Trademark Counterfeiting Act of 1984: Score a Few for the Good Guys*, 82 TRADEMARK REP. 1, 19-23 (1992); Neil A. Smith, *Obtaining Early and Effective Relief Against Trademark Counterfeiting*, 10 HASTINGS COMM. & ENT. L.J. 1049, 1059-62 (1988).

- The applicant must provide an affidavit or verified complaint setting forth sufficient facts to support the findings needed for the seizure order.
- The applicant must give a particular description of what is to be seized and where the seizure is to occur.
- The applicant must provide adequate security to compensate any person entitled to recovery as a result of a wrongful seizure.
- The court must determine that there is no other means adequate to achieve the purposes of the Lanham Act.
- The court must find that the applicant would be irreparably harmed without the seizure and that this harm outweighs the harm that would occur to the party who would be subject to the seizure.
- The court must find that the party who would be subject to the seizure would be likely to dispose of the matter to be seized if given notice.
- The court must issue a protective order governing the confidentiality of matters seized.
- The seizure must be carried out by federal law enforcement officials.
- The court must hold a prompt post-seizure hearing at which the applicant has the burden of proving that the order should remain in effect.[391]

Notably, the statute authorizes the seizure not only of goods and counterfeit marks, but also of "the means of making such marks, and records documenting the manufacture, sale, or receipt of thing involved in such violation."[392] Accordingly, this seizure remedy is broad enough to encompass relevant computer records.

Although the Lanham Act's seizure remedy is broad enough to encompass relevant computer records, the restrictions and protections incorporated into this remedy will limit its utility in obtaining expedited access to an opponent's computer evidence. For instance, the remedy only applies to counterfeiters, and, as in Rule 65 counterfeiting cases, the requirement of demonstrating that the defendant would likely violate a court order is generally satisfied by showing that the goods in question are easily disposable and have been surreptitiously disposed by similarly situated defendants in the past.[393] Congress has warned, however, that absent unusual circumstances this requirement is not likely to be satisfied where the party that would be subject to the seizure is a reputable business person.[394] Similarly, one court found the evidence inadequate to conclude that the defendants were likely to violate a court order requiring the preservation of evidence where the defendants were "not

391. *See* 15 U.S.C. § 1116(d)(2)-(11).

392. 15 U.S.C. § 1116(d)(1)(A).

393. *See* 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 30:38 (4th ed. 1997).

394. *See* Senate-House Joint Explanatory Statement on Trademark Counterfeiting Legislation, 130 CONG. REC. H12076 at 12081 (Oct. 10, 1984).

street vendors but manufacturers, with printing equipment and machinery that presumably cannot be easily moved or destroyed."[395]

d. The Copyright Act

Another source of authority for *ex parte* seizure orders may be found in the Copyright Act. Specifically, the Copyright Act authorizes a court "[a]t any time while an action . . . is pending" to impound "all copies or phonorecords claimed to have been made or used in violation of the copyright owner's exclusive rights."[396] Notably, this provision does not enable a court to impound books or records that serve as evidence of infringement, but are not themselves infringing articles.[397] This limitation obviously restricts parties' ability to use the Copyright Act to seize key computer-related evidence of infringement. On the other hand, infringing copies may well reside in computer storage media, thereby making such forms of computer storage media proper targets for impoundment. In addition, the Copyright Act authorizes the impoundment of "all plates, molds, matrices, masters, tapes, film negatives, or other articles by means of which such copies or phonorecords may be reproduced."[398] In some cases, computer equipment, including some forms of computer storage media, may fall within the broad sweep of this language. The fact that such equipment can be put to legitimate use will

395. Time Warner Entertainment Co. v. Does, 876 F. Supp. 407, 414 (E.D.N.Y. 1994).

396. 17 U.S.C. § 503(a).

397. *See* First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 649 n.10 (6th Cir. 1993); 4 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 14.07 (1997). One appellate court reacted quite harshly to a plaintiff's attempt to defend an *ex parte* seizure order as a form of "accelerated discovery." *See* Warner Bros., Inc. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1124, 1126 (2d Cir. 1989); *but see* Marc Alexander, *Discretionary Power to Impound and Destroy Infringing Articles: An Historical Perspective,* 29 J. COPYRIGHT SOC'Y 479, 494 (1982) (suggesting that courts consider, among other things, how well seizure order would promote obtaining key evidence in exercising its discretion to determine scope of order); Paul S. Owens, *Impoundment Procedures Under the Copyright Act: The Constitutional Infirmities,* 14 HOFSTRA L. REV. 211, 223-24 & n.71 (1985) (describing obtaining evidence as "perhaps most significant" purpose of seizure orders and collecting older cases in which seizure orders were issued to obtain business records and advertising or promotional materials). It seems clear that the impoundment procedures necessarily serve some discovery-related function of gathering evidence and preserving it for trial. The question, however, is the proper scope of that discovery-related function. To comply with the constitution, any seizure must be directed only to works already identified as likely infringing and to articles by which such infringements are produced to the extent one can determine what types of such articles were likely used to create the infringing works. While this evidence will be obtained and preserved, it should merely confirm what the applicant already has reason to suspect, although it may also increase the applicant's knowledge as to the extent of the infringing activity with respect to these previously identified works.

398. 17 U.S.C. § 503(a).

not necessarily prevent its seizure if it has been used to infringe.[399]

Unlike the Lanham Act, the Copyright Act does not include detailed procedures governing impoundment orders, although such orders are obviously subject to constitutional restrictions on the court's authority. Rather, the Copyright Act gives the district court substantial discretion by providing that the court "may" issue such orders "on such terms as it may deem reasonable. . . ."[400] This discretion may be constrained by several rules that the Supreme Court promulgated under an earlier version of the Copyright Act.[401] These rules require, among other things:

- An applicant must file an affidavit identifying the number and location of the items to be seized and their value.
- An applicant must file a bond as security in an amount not less than twice the reasonable value of the items seized.
- The seizure must be undertaken by the United States Marshals.
- The items seized shall be maintained in the custody of the United States Marshals or of the court.
- Within ten days after serving notice to the opponent, the applicant must justify to the court the amount of the bond.
- The party subjected to the seizure may apply to the court for return of the items seized upon filing an affidavit showing that the seizure was improper.[402]

Courts have disagreed over whether these rules remain intact.[403] Although the copyright rules contain some protections against overly in-

399. *See* Time Warner Entertainment Co. v. Does Nos. 1-2, 876 F. Supp. 407, 410 (E.D.N.Y. 1994) (citation omitted); Century Home Entertainment, Inc. v. Laser Beat, Inc., 859 F. Supp. 636, 639 (E.D.N.Y. 1994). For a discussion of how to interpret the phrase "other articles by means of which such copies or phonorecords may be reproduced and of constitutional protections implicated by this phrase," *see* Alexander, *supra* note 397, at 492-96. In exercising their discretion to issue seizure orders, Alexander suggests that courts consider four factors in determining the scope of such orders: (1) how the order would promote enforcement of the copyright laws through deterrence, discovery of evidence, and punishment; (2) how the breadth of the order correlates to the seriousness of the infringement; (3) how necessary the seizure of any particular item is to preventing further infringement; and (4) how probable it is that the item to be seized would be put to a legitimate noninfringing use in the future. *See id.* at 494.

400. 17 U.S.C. § 503(a). *See First Tech. Safety Sys.*, 11 F.3d at 647.

401. *See* Rules of Practice as Amended, 17 U.S.C. foll. § 501.

402. *See id.*

403. *Compare* Warner Bros., Inc. v. Dae Rim Trading, Inc., 877 F.2d 1120, 1124 (2d Cir. 1989) ("The consensus of knowledgeable authorities is that the Supreme Court's Rules have not been repealed.") (collecting authority), *with* Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 87 (E.D.N.Y. 1993) ("[The Copyright Rules'] mandatory provisions are clearly inconsistent with the discretionary powers conferred on this Court by the Copyright Act of 1976. Moreover, a literal reading of the rules would result in procedures of dubious constitutional validity in light of Supreme Court decisions handed down since the time of the rules adoption.") (collecting authority), *and with* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1261 (N.D. Cal. 1995) ("Although neither the Supreme Court nor the 1976 Act explicitly repealed the Copyright Rules, . . . , courts

vasive and unwarranted seizures, these protections alone may not be sufficient to comply with the Constitution, because the rules do not require the applicant to demonstrate its likelihood of success on the merits by showing that the articles to be seized are actually infringing the applicant's copyrights, because the rules are not limited to situations where the defendant is likely to conceal or destroy the infringing materials, and because the post-seizure hearing contemplated by the rules is left to the discretion of the court.[404] Accordingly, in exercising the discretion afforded by the Copyright Act to impound materials, many courts follow a procedure much like the Rule 65 procedure, whereby they require an applicant to demonstrate, among other things, a likelihood of success in proving infringement and an imminent danger of being irreparably harmed by the likely disposal of the materials that are subject to statutory impoundment.[405]

e. Applications to Computer-Related Evidence

Thus, while Rule 65, the Lanham Act, and the Copyright Act, all enable a district court to issue *ex parte* seizure orders, the many restrictions on the court's authority to issue such orders limit the utility of such devices in obtaining expedited access to an opponent's computer system. Generally, a party seeking such a seizure must be prepared to come forward with sworn testimony setting forth specific facts that demonstrate a strong likelihood of prevailing on the merits of its claim, as well as a strong likelihood of irreparable harm, usually in the form of the likely disposal of evidence. The applicant should be prepared to post an appropriate bond and propose a narrowly tailored, particularized seizure order. These requirements are particularly difficult to meet at the commencement of the case when a party has limited information regarding its opponent. In addition, the applicant should be particularly sensitive to the nuances in the scope of judicial authority to issue seizure orders under Rule 65, the Lanham Act, and the Copyright Act.

One example of the difficulties in using an *ex parte* seizure order as a device to conduct accelerated discovery of computer-related evidence can

---

and commentators have questioned the Rules' continuing validity, both as a matter of statutory construction and constitutional law.") (collecting authority).

404. *See Paramount Pictures,* 821 F. Supp. at 87-88; *see generally* 4 NIMMER, *supra* note 397, § 14.07; Owens, *supra* note 397, at 230-49; Raoul A. Renaud, Comment, *Pretrial Remedies in Infringement Actions: The Copyright Holder's Impound of Flesh?,* 17 SANTA CLARA L. REV. 885, 901-08 (1977).

405. *See, e.g., Religious Tech. Ctr.,* 923 F. Supp. at 1262-63; Columbia Pictures Indus., Inc. v. Jasso, 927 F. Supp. 1075, 1076-77 (N.D. Ill. 1996); *Paramount Pictures,* 821 F. Supp. at 88-89 (collecting authority); WPOW, Inc. v. MRLJ Enters., 584 F. Supp. 132, 135 (D.D.C. 1984). *See generally* 4 NIMMER, *supra* note 397, § 14.07; Owens, *supra* note 397, at 226.

be seen in the case of *First Tech. Safety Sys., Inc. v. Depinet.*[406] In that case, the plaintiff sued three former employees and a competing company they had formed. The plaintiff claimed the defendants had misappropriated the plaintiff's trade secrets and infringed the plaintiff's copyrights by improperly copying from the plaintiff's computer storage media certain information pertaining to costs, customers, and marketing, as well as software used to manufacture the plaintiff's products.[407] The plaintiff sought and obtained an *ex parte* seizure order, which authorized the seizure and impoundment of electronically stored evidentiary materials relating to the claimed wrongdoing.[408] When the district court refused to vacate this order, the defendants appealed, and the Sixth Circuit reversed. The Sixth Circuit found that the only purpose for the seizure of the defendants' business records was to preserve evidence and held that there was no basis for such a seizure under the Copyright Act.[409] The appellate court further found that the plaintiff could not justify such a seizure under Rule 65, because the plaintiff failed to demonstrate a likelihood that the defendants would dispose of these records if given notice.[410] Notably, in reaching this result, the court rejected the argument that there was a danger that evidence would likely be destroyed, merely because that evidence resided in computer storage media and was, therefore, more susceptible to destruction, as well as the argument that there was a danger that the evidence would likely be destroyed because the defendants were accused in the complaint of having engaged in unlawful conduct.[411]

Although it seems clear that *ex parte* seizure orders will not serve as a device for expediting access to computer-related evidence in garden variety cases, one potential area for the use of these orders to obtain such evidence may be that of Internet-related trademark and copyright infringement. Trademark and copyright infringement over the Internet is a widespread problem.[412] Some forms of this infringement, such as the distribution of unauthorized video games or the distribution of services, through knock-off web sites, may qualify as counterfeiting.[413] Indeed,

406. First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641 (6th Cir. 1993).

407. *See id.* at 644-45.

408. *See id.* at 645-46.

409. *See id.* at 649.

410. *See id.* at 650-51.

411. *See id.* at 651.

412. *See generally* Ian C. Ballon, *Pinning the Blame in Cyberspace: Towards a Coherent Theory for Imposing Vicarious Copyright, Trademark and Tort Liability for Conduct Occurring Over the Internet*, 18 HASTINGS COMM. & ENT. L.J. 729 (1996).

413. *See, e.g.*, Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 933 (N.D. Cal. 1996) (in case where access to defendant's computer and memory devices was obtained pursuant to seizure order, summary judgment awarded to plaintiff on claims of copyright infringement and trademark counterfeiting arising out of distribution of unauthorized copies of video

even software programs have been counterfeited.[414] In addition, video games, text, graphics, and software programs distributed and displayed over the Internet may contain content that infringes copyrights.[415] Much like street peddlers of cheap knock-off goods, trademark and copyright violations over the Internet are often difficult to detect and remedy, and perpetrators of such violations may not be well established business enterprises. As one court observed: "Computer files can be easily uploaded and copied from one location to another and are easy to transport, conceal, or delete. The ability of users to post large amounts of protected works nearly instantaneously over the Internet makes it a rather dangerous haven for copyright infringers."[416] On the other hand, such violations occur by using computer equipment, which might be analogized to printing equipment and machinery that is not easily secreted and destroyed. Ultimately, which analogy prevails may depend upon how easy the discovery and the destruction of evidence residing in the computer are determined to be. There is, however, growing evidence of the use of such orders in Internet cases.[417]

Where intellectual property laws do not apply, the likelihood of prevailing with an *ex parte* seizure application will generally rise or fall with the applicant's ability to demonstrate an imminent likelihood that evidence will be destroyed. As *First Tech. Safety Sys.* demonstrates, courts

---

games through defendant's electronic bulletin board). The term "counterfeit mark" is defined, in pertinent part, as "a counterfeit of a mark that is registered on the principal register in the United States Patent and Trademark Office for such goods or services sold, offered for sale, or distributed and that is in use, whether or not the person against whom the relief is sought knew such mark was so registered. . . . " 15 U.S.C. § 1116(d)(1)(B).

414. *See* Smith, *supra* note 390, at 1049.

415. Copyrightable subject matter is defined as "original works of authorship fixed in any tangible medium of expression, including literary works and pictorial and graphic works." 17 U.S.C. § 102(a). Literary works may be "expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as . . . tapes, disks, or cards, in which they are embodies." 17 U.S.C. § 101. In addition, the Copyright Act expressly limits the types of copying that may constitute infringement of copyrights inhering in computer programs. *See* 17 U.S.C. § 117.

416. Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1262 n.36 (N.D. Cal. 1995).

417. *See, e.g.*, Sega Enters., Ltd. v. MAPHIA, 948 F. Supp. 923 (N.D. Cal. 1996). This is not to say that such applications for *ex parte* seizure orders in this context have met with unqualified success. *See* Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 923 F. Supp. 1231, 1260-65 (N.D. Cal. 1995) (vacating *ex parte* seizure order due to failure to satisfy requirements of Rule 65 and the constitution, including because of failure to show likelihood that evidence would be destroyed and because of overbreadth of seizure); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1353, 1358-61 (E.D. Va. 1995) (vacating *ex parte* seizure order due to finding that plaintiff had unclean hands, in part, because of manner in which seizure order was implemented); Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1528 (D. Colo. 1995) (contempt proceedings in connection with plaintiff's failure to return seized materials as ordered by court).

will probably hesitate to find such a likelihood from hazards of losing evidence that are attributable solely to the general nature of computer storage media. What type of proof is required to show a likelihood that evidence will be destroyed, however, remains unclear. In the leading case of *Vuitton et Fils*, the plaintiff offered an attorney's affidavit recounting the plaintiff's experience with similar defendants accused of counterfeiting who had maintained little documentary evidence and had disposed of the counterfeit merchandise in question upon receiving notice of the lawsuit.[418] Certainly, any party seeking to avoid running afoul of constitutional requirements will want to ensure that any such affidavits are based on personal knowledge or offer expert opinions with proper foundational testimony.[419] One way to persuade a court that there is a likelihood that the opponent will dispose of computer-related evidence may be by referring to cases involving similarly situated targets of computer-related discovery where tampering or destruction was found.[420] Another approach would be to offer expert testimony of a computer technician who has worked on similar cases and has found other instances of tampering or destruction. Where the party from whom discovery is sought is accused of having falsified or antedated a document, inquiry into whether that party is likely to tamper with or destroy evidence in computer storage media related to that document may entail some of the same problems associated with determining whether invasive discovery of such a party's hard drive should be permitted.

Finally, where a party seeks discovery of computer-related evidence, before applying for an *ex parte* seizure order, that party must consider the tactical consequences of such a motion. There are several possible adverse consequences from such a motion. First, the motion might be denied, and the denial might be accompanied by a judicial decision questioning the moving party's likelihood of succeeding on the merits. Second, the motion might be granted, and the seizure might yield either nothing of probative value or, worse, evidence tending to support the opponent's position. In that instance, the adverse impact of such evidence is likely to be magnified in the mind of a judge who has just devoted

418. *In re* Vuitton et Fils S.A., 606 F.2d 1, 2 (2d Cir. 1979).

419. *See* FED. R. EVID. 602 (witness must have personal knowledge to testify); FED. R. EVID. 703 (expert testimony may be based on facts or data of type reasonably relied on by experts in field).

420. *See, e.g.*, Cerruti 1881 S.A. v. Cerruti, Inc., 169 F.R.D. 573 (S.D.N.Y. 1996), discussed in text accompanying notes 178-79, *supra*. One potential source of cases where parties have been found to have tampered with or destroyed evidence is the law of spoliation. *See supra* notes 45-57 and accompanying text. One court cited *Vuitton et Fils* and its progeny as support for the proposition that "those who deliberately traffic in infringing merchandise" are likely to dispose of evidence, thus supporting the use of analogous caselaw to help establish the likelihood that a party may dispose of evidence. *See* Columbia Pictures Indus., Inc. v. Jasso, 927 F. Supp. 1075, 1077 (N.D. Ill. 1996).

extraordinary efforts and resources towards granting expedited relief that has constitutional implications. Third, the motion might be granted, but the resulting seizure order might subsequently be successfully challenged in an adversarial hearing. Thus, the dangers of having the motion denied or of seizing evidence having little or no probative value are heightened by the challenges of persuading the court of the need for relief and of targeting a seizure order on the right evidence when the moving party has not yet had an opportunity to learn basic facts about the case and about the opponent's computer storage system through discovery. Of course, an additional and ever-present factor is the expense of both obtaining relief from the court and providing any technical support for the seizure and examination of the evidence. Therefore, before seeking an *ex parte* seizure order a party must consider the relative importance of the evidence sought, whether there is a real need for *ex parte* relief, whether there is sufficient information to meet the evidentiary hurdles to obtaining such relief, and what such a seizure is likely to yield.

2. *Preservation Orders*

Because of the daily deterioration of evidence residing in computer storage media, if such evidence is not immediately seized it becomes imperative to consider ways to ensure that this evidence is preserved. If a party believes that an opponent may actively tamper with or dispose of such evidence but does not wish to incur the risk of an *ex parte* seizure application, one alternative is an *ex parte* temporary restraining order requiring that such evidence be preserved until appropriate actions can be taken. Indeed, where courts have denied *ex parte* seizure orders, they have often done so on the ground that the applicant has failed to demonstrate that a less intrusive *ex parte* preservation order would not suffice to prevent the threatened harm.[421]

If the party seeking preservation of an opponent's computer storage media is concerned about giving undue emphasis to the evidence that may be found in that media, preservation might be sought in a setting less dramatic than the context of injunctive relief. The source of judicial authority best suited to such an effort is Rule 16 of the Federal Rules of Civil Procedure, which empowers the court, among other things, to issue orders "control[ing] and scheduling discovery, including orders "affecting disclosures and discovery," orders "adopting special procedures for managing potentially difficult or protracted actions that may involve complex

421. *See, e.g.*, First Tech. Safety Sys., Inc. v. Depinet, 11 F.3d 641, 650 (6th Cir. 1993); Am. Can Co. v. Mansukhani, 742 F.2d 314, 323 (7th Cir. 1984); Time Warner Entertainment Co. v. Does Nos. 1-2, 876 F. Supp. 407, 414 (E.D.N.Y. 1994); Paramount Pictures Corp. v. Doe, 821 F. Supp. 82, 89 (E.D.N.Y. 1993).

issues . . . or unusual proof problems," and orders relating to "such other matters as may facilitate the just, speedy, and inexpensive disposition of the action."[422] According to the *Manual for Complex Litigation*, in crafting case management orders, courts should consider whether to order the preservation of records, including of computer-related evidence.[423]

Not only does Rule 16 serve as a useful vehicle to preserve such evidence due to the subject matter of the rule, but it is also useful for preserving evidence due to the stage in the proceedings when courts must act under the rule. Specifically, Rule 16 requires the court to conduct a conference addressing such matters before issuing a scheduling order within four months after service of the complaint.[424] Although this early stage of the proceedings makes this procedure useful for preserving evidence, the need to persuade the court of an appropriate form of order governing the manner and extent of preservation may be difficult before a party has had the ability to discover essential information about the opponent's computer system. Accordingly, a party seeking to address the preservation issue at a Rule 16 conference should take as many steps as possible to learn the nature of an opponent's computer system and computer storage practices and should enlist a competent technician to help present all relevant concerns to the judge, who may be unfamiliar with the technological issues presented by the discovery sought.[425] If insufficient information can be obtained, the party seeking preservation may seek to have the court require the expedited disclosure of certain necessary information so that the court can revisit the issue.

Alternatively, a party seeking to overcome informational obstacles and to prevent the court from entering an insufficiently protective preservation order may attempt to negotiate such an order with the opponent. Rule 29 empowers the parties to enter written stipulations that "modify . . . procedures governing . . . discovery . . . ."[426] The parties can also seek to have the court enter such a stipulation as a court order. The process of negotiating such a stipulation, however, is susceptible to getting bogged down, particularly if sensitive or damaging information is involved, or if one or both of the parties are hampered in their technological understanding.

Finally, for a party wishing to ensure preservation while not drawing undue judicial attention to the nature of this evidence and not getting bogged down in negotiations over the scope of the duty to preserve, there is one more alternative. In this instance, a party may consider

422. FED. R. CIV. P. 16(c)(6), (12), and (16).

423. *See* MANUAL FOR COMPLEX LITIG., *supra* note 67, §§ 21.442 & 21.446.

424. FED. R. CIV. P. 16(b) & (c).

425. *See* Johnson-Laird, *supra* note 5, at 3 & 13.

426. FED. R. CIV. P. 29.

simply sending a letter to the opponent giving notice that particular computer-related information will be material to the litigation and warning that any failure to preserve such evidence will be dealt with under the law of spoliation.[427] Although this approach may enable a party to act early and to avoid conceding ground in negotiations over the scope of required preservation, this approach may leave considerable uncertainty. For instance, it is unclear to what extent the law of spoliation would require a party to take steps to preserve computer-related information that is the subject of daily usage in the ordinary course of business.[428]

3. *Expedited Discovery*

One additional weapon in the litigator's arsenal of procedures to obtain early access to computer-related evidence is expedited discovery. Under Rule 26(d), the court can accelerate the time when the parties are permitted to commence discovery.[429] In addition, under Rules 33(b)(3) and 34(b), the court can accelerate the thirty-day periods for responding to interrogatories and requests for inspection and production.[430]

Courts frequently allow expedited discovery when the request is made in order to obtain information needed in connection with a motion for a preliminary injunction.[431] Indeed, the Advisory Committee Note to Rule 26(d) contemplates expedited discovery in such instances.[432] Thus, not surprisingly, the standard followed by most courts for determining whether or not to grant expedited discovery loosely tracks the standard for obtaining preliminary injunctive relief. In particular, such courts require the applicant to show: "(1) irreparable injury; (2) some probability of success on the merits; (3) some connection between the expedited discovery and the avoidance of the irreparable injury; and (4) some evidence that the injury that will result without expedited discovery looms greater

427. *See* Dunbar, *supra* note 3, at 34; Kashi, *How to Conduct On-Premises Discovery, supra* note 4, at 42; Lacouture, *supra* note 3, at 10.

428. *See supra* notes 52-54 and accompanying text.

429. FED. R. CIV. P. 26(d).

430. FED. R. CIV. P. 33(b)(3); FED. R. CIV. P. 34(b).

431. *See, e.g.*, Ellsworth Assocs., Inc. v. United States, 917 F. Supp. 841, 844 (D.D.C. 1996) (citations omitted); Advanced Portfolio Techs., Inc. v. Advanced Portfolio Techs. Ltd., 1994 WL 719696, *3 (S.D.N.Y. 1994) (citations omitted); Onan Corp. v. United States, 476 F. Supp. 428, 434 (D. Minn. 1979); Karmel v. Great Lakes Chem. Corp., 1981 WL 15078, *3 (Del. Ch. Ct. 1981), *reargument denied*, 1981 WL 15143 (Del. Ch. Ct. 1981). On the other hand, with preliminary injunction proceedings looming, courts may look with disfavor on an attempt to obtain overly broad discovery on an unrealistic schedule from an opponent who is concentrating its efforts on the preliminary injunction proceedings. *See* Irish Lesbian and Gay Org. v. Giuliani, 918 F. Supp. 728, 731 (S.D.N.Y. 1996) (denying motion for expedited discovery).

432. FED. R. CIV. P. 26(d), advisory committee note (1993 amendment).

than the injury that the defendant will suffer if the expedited relief is granted."[433]

Courts often allow expedited discovery in intellectual property cases, given the urgency with which such cases are litigated and the resulting frequent use of motions for preliminary injunctive relief.[434] Similar concerns may be present in constitutional cases.[435] Where, however, expedited discovery is sought to ensure preservation of evidence, the moving party can invoke at least one decision expediting discovery to expose alleged steps taken by the defendants to hide assets and cover up their fraud.[436] Such expedited discovery can be sought in addition to, or in the alternative to such other preliminary relief as *ex parte* seizures, temporary restraining orders, and preliminary injunctions.[437]

A party should not, however, presume that expedited discovery will be allowed. A substantial record must be prepared to satisfy the four-part standard for relief. As with other forms of accelerated judicial relief, the applicant must be prepared for a court that may be unfamiliar with the technological issues involved in conducting discovery of computer-related evidence. In addition, the applicant must be wary of proposing overly broad expedited discovery that sweeps beyond the reach of

433. Notaro v. Koch, 95 F.R.D. 403, 405 (S.D.N.Y. 1982); *accord Irish and Gay Org.*, 918 F. Supp. at 730 (quoting *Notaro*); *Advanced Portfolio Techs.*, 1994 WL 719696, at *3 (quoting *Notaro*); Crown Crafts, Inc. v. Aldrich, 148 F.R.D. 151, 152 (E.D.N.C. 1993) (quoting *Notaro*).

434. *See, e.g., Advanced Portfolio Techs.*, 1994 WL 719696, at *4; Sports Design and Dev., Inc. v. Schoneboom, 871 F. Supp. 1158, 1167 (N.D. Iowa 1995); Fox v. Mow Trad. Corp., 749 F. Supp. 473, 475 (S.D.N.Y. 1990); Fimab-Finanziaria Maglificio Biellese Fratelli Fila S.P.A. v. Helio Import/Export, Inc., 601 F. Supp. 1, 3 (S.D. Fla. 1983) ("*Fimab I*"); Fimab-Finanziaria Maglificio Biellese Fratelli Fila S.P.A. v. Kitchen, 548 F. Supp. 248, 250 (S.D. Fla. 1982) ("*Fimab II*"); 6 NIMMER, *supra* note 397, § 34.06.

435. *See Ellsworth*, 917 F. Supp. at 844 (collecting authority).

436. *See* Merrill Lynch Futures, Inc. v. Kelly, 585 F. Supp. 1245, 1259-60 (S.D.N.Y. 1984). Analogous concerns relating to preservation of evidence are present where courts expedite discovery to provide for a witness who is about to leave the jurisdiction or who is infirm. *See* Gibson v. Bagas Restaurants, Inc., 87 F.R.D. 60, 62 (W.D. Mo. 1980) (quoting Babolia v. Local 456, 11 F.R.D. 423, 424 (S.D.N.Y. 1951)).

437. *See* Time Warner Entertainment Co. v. Does Nos. 1-2, 876 F. Supp. 407, 414 (E.D.N.Y. 1994) (denying *ex parte* seizure where, among other things, plaintiff failed to show why less intrusive injunction, coupled with expedited discovery, would not suffice); *Sports Design and Dev.*, 871 F. Supp. at 1167 (expedited discovery granted as alternative to *ex parte* seizure); *Fimab I*, 601 F. Supp. at 3 (expedited discovery granted in addition to *ex parte* seizure); *Fimab II*, 548 F. Supp. at 250 (expedited discovery granted in addition to *ex parte* seizure); Smith, *supra* note 390, at 1051 (discussing use of expedited discovery in combination with temporary restraining order and seizure order). Some courts actually order expedited discovery as a component of a temporary restraining order. *See* NEA Enters., Inc. v. Am. Horse Enters., Inc., 211 U.S.P.Q. 109, 111-12 (N.D. Cal. 1980); NEA Enters., Inc. v. Zacks, 209 U.S.P.Q. 566, 568 (S.D. Fla. 1980).

the harm to be avoided by accelerated procedures.[438] Indeed, in view of the fact that, at the outset of litigation, a party seeking expedited discovery may be in a poor position to conduct all necessary discovery on any particular issue, an applicant for expedited discovery may be well advised to limit such a request to the bare essentials and reserve its rights to conduct more fulsome discovery in later phases of an expedited discovery process and/or in the ordinary course of the litigation.[439]

B. Obtaining the Evidence

After resolving the timing of computer-related discovery, the discovering party must confront technological and procedural obstacles to obtaining the desired evidence. Specifically, the discovering party must determine where to look for relevant computer-related evidence and must determine how to find such information given the limitations that the rules of procedure place on a party's ability to conduct discovery.

Although, as discussed above, computer-related evidence clearly falls within the scope of discoverable subject matter, under the Federal Rules of Civil Procedure, a party cannot simply frame discovery requests for specific types of information and assume that an adversary will produce, either voluntarily or by court order, all forms of computer storage media likely to contain the requested information.[440] To begin with, whenever a party responding to a discovery request searches for responsive information, that party will always have to make a judgment about the scope of the search that should be undertaken in light of the likelihood of finding responsive information from various locations and in light of the burden of searching various locations relative to the importance of the information sought and the overall expense of the case. Beyond these basic impediments to a fulsome search for responsive information, in the area of computer technology, the responding party simply may not know all of the potential sources of computer storage media that may contain responsive information. Furthermore, opposing counsel—and, possibly, the court as well— may not understand why it is

438. *See Irish Lesbian and Gay Org.*, 918 F. Supp. at 730-31 (denying request for expedited discovery that court characterized as "overbroad, burdensome, and oppressive"); *Ellsworth Assocs.*, 917 F. Supp. at 844 (allowing expedited discovery that court characterized as "narrowly tailored"); *Onan*, 476 F. Supp. at 434 (allowing expedited discovery, as limited by court).

439. *See* Computerland Corp. v. Batac, Inc., 1988 WL 140816, *5 (S.D.N.Y. 1988) (limiting issues that will be subject of expedited discovery and allowing applicant to conduct full deposition at later stage of litigation).

440. *See* E.E.O.C. v. Gen. Dynamics Corp., 999 F.2d 113, 116-17 (5th Cir. 1993) (reversing lower court order imposing sanctions for failure to produce computer tapes in response to earlier court order, where earlier order did not clearly require production of computer tapes).

necessary to search in every form of computer storage media when one or more sources of what purports to be the requested information exist in other formats, such as hard copy.[441]

Accordingly, a party seeking discovery of computer-related information should frame discovery requests that seek information in specific media for computer storage and in specific locations.[442] Although the discovering party should consider employing an expert to help frame these requests, there are several areas that can be identified as potential candidates for discovery. These include systems, local area networks, desktop personal computers, online services, lap top computers, and computers used by employees at home.[443] The potential sources of evidence may include not only such broadly defined types of computer storage media as hard drives, floppy diskettes, magnetic tapes, and CD-ROMs, but also, more specifically, e-mail, system history files, back-up files, files containing drafts, deleted files, dormant files, data stored "off the end" of currently active sections of magnetic tape, partially overwritten file remnants, and broken hard drives.[444] The discovering party should further consider whether online services may have retained e-mail communications in their computer storage media even if such communications have been deleted from the user's computer and whether e-mail distribution lists may be retained on the sender's hard drive instead of on the network.[445]

Without knowing basic information about the types of computer systems used by an opponent, however, it may not be possible to know all potential sources of relevant evidence or to know all of the safeguards needed to inspect and copy data from an opponent's computer systems.[446] In addition, when framing discovery requests without such knowledge, there is a substantial danger of framing requests that have no applicability to the types of computer systems used by an opponent or that may not be reasonably calculated to lead to the discovery of admissible evidence.[447] Moreover, given the likelihood of an objection based on undue burden, it is particularly important that discovery requests for computer-related evidence be tightly focused.

Thus, before seeking discovery of substantive evidence, a party may wish to consider a preliminary phase of discovery aimed at learning basic

441. *See* Johnson-Laird, *supra* note 5, at 13.

442. *See id.;* Lacouture, *supra* note 3, at 9.

443. *See* Davis, *supra* note 6, at 60.

444. *See* Brill, *The Secret Life of Computer Data, supra* note 13, at 32; Davis, *supra* note 6, at 53-54; Johnson-Laird, *supra* note 5, at 8-9 & 13.

445. *See* Davis, *supra* note 6, at 60; Lacouture, *supra* note 3, at 9 n.4.

446. *See* Galligan, *supra* note 350, at 2644; Kashi, *How to Conduct On-Premises Discovery, supra* note 4, at 28.

447. *See* FED. R. CIV. P. 26(b)(1).

information about an opponent's computer system. This phase of discovery may include identification of basic information through interrogatories and obtaining background and follow-up information through depositions of appropriate computer personnel, followed by an inspection of the opponent's premises.[448] Moreover, the discovering party can learn the types of computer systems and equipment used at different levels of an opponent's organization, the procedures and media used for storage, what types of e-mail systems and subdirectories may exist, and what potential sources of back-up files may exist.[449] In addition, deposition questioning can yield such valuable information as ways to obtain information from computer storage that was believed to be unavailable, forms of information maintained only in computer storage that have not been produced in hard copy, and whether important computer files have been deleted.[450] Alternatively, the necessary background information might be obtained through an informal or stipulated exchange of information, preferably including a consultation between the technician who will inspect or copy data and the opponent's technician.[451]

Given the extent of the information needed to conduct effective discovery of computer-related evidence and the broad scope of potentially relevant computer-related evidence, this form of discovery is likely to strain the already scarce discovery resources allocated to each party as of right under the rules of procedure.[452] For instance, without leave of court, a party can only conduct ten depositions.[453] Similarly, without leave of court, a party can only serve twenty-five interrogatories.[454] Although there is no similarly explicit limit on the number of requests for the production of documents or for the inspection of premises that may be served, objections founded on undue burden and expense will impose limits on these forms of discovery.[455]

Accordingly, before seeking discovery of computer-related evidence, a party should consider addressing the type and scope of potentially

448. *See* Davis, *supra* note 6, at 60-61; Howie, *supra* note 7, at 72-73; Lacouture, *supra* note 3, at 9.

449. *See* Howie, *supra* note 7, at 72.

450. *See* State Farm Mut. Auto. Ins. Co. v. Engelke, 824 S.W.2d 747, 751 (Tex. Ct. App. 1992) (testimony revealing manner in which information sought by interrogatories could be obtained from computer system); Zapata v. IBP, Inc., 1994 WL 649322, *2 (D. Kan. 1994) (deposition testimony revealed that employee historical information not produced in response to discovery requests resided in computer storage); Gates Rubber Co. v. Bando Chem. Indus., Inc., 167 F.R.D. 90, 110-11 (D. Colo. 1996) (deposition testimony in which one of defendant's employees admitted deleting computer file).

451. *See* Kashi, *How to Conduct On-Premises Discovery, supra* note 4, at 28.

452. *See id.*

453. *See* FED. R. CIV. P. 30(b)(2)(A).

454. *See* FED. R. CIV. P. 33(a).

455. *Compare* FED. R. CIV. P. 34(a) *with* FED. R. CIV. P. 26(c).

needed discovery in the discovery plan that must be submitted pursuant to Rule 26(f) and at the scheduling conference to be conducted pursuant to Rule 16(b).[456] At the conference, the discovering party should be prepared to explain why the discovery sought is needed and to meet objections. The discovering party should also anticipate the possibility that broad requests for computer-related discovery will be met with equally broad requests for discovery from such sources by the opponent. In turn, a party targeted for such discovery should be prepared to articulate precisely how the requested discovery would be unduly burdensome or expensive and precisely what sorts of privileged or confidential information might be jeopardized by such discovery.

C. Evidentiary Issues

In addition to issues of timing and informational obstacles, discovery of computer-related evidence also presents evidentiary questions not present in other forms of discovery. Although a complete discussion of evidentiary rules governing the use of computer-related evidence at trial is beyond the scope of this Article, some evidentiary rules demand that computer-related evidence offered at trial be sufficiently accurate, trustworthy, and reliable. These rules must be considered when conducting discovery and preserving the evidence that is to be offered at trial.

First, a proponent of computer-related evidence must authenticate that evidence.[457] Specifically, Rule 901 requires as a prerequisite to admissibility "evidence sufficient to support a finding that the matter in question is what its proponent claims."[458] Rule 901 provides several illustrations of the types of authenticating evidence that will pass muster. For instance, with regard to processes or systems, the rule specifies as adequate "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."[459] Thus, this illustration serves as guidance for authenticating computer-related evidence.[460] As the text of the illustration indicates, accuracy of the system is central to admissibility.[461]

---

456. *See* Fed. R. Civ. P. 16(b); Fed. R. Civ. P. 26(f).

457. *See* Fed. R. Evid. 901; *see, e.g.,* First Nat'l Bank of Jefferson Parish v. M/V Lightning Power, 851 F.2d 1543, 1548 (5th Cir. 1988) (holding that computer print-out of wage-related data was not self-authenticating).

458. Fed. R. Evid. 901(a).

459. Fed. R. Evid. 901(b)(9).

460. *See* Lory Dennis Warton, Note, *Litigators Byte the Apple: Utilizing Computer-Generated Evidence at Trial,* 41 Baylor L. Rev. 731, 733 (1989).

461. *See, e.g.,* United States v. Weatherspoon, 581 F.2d 595, 598 (7th Cir. 1978) (holding that computer print-out was properly authenticated by, among other things, testimony that input procedures and print-outs were accurate within two percent); United States v. Liebert, 519 F.2d 542, 547 (3d Cir. 1975) ("The introduction of a computer printout is admissible in a criminal trial provided that the offering party lays a foundation sufficient to warrant a

Second, because computer print-outs and even data contained in computer storage media are generally copies of information generated from another source, a proponent of computer-related evidence must anticipate an objection based on the best evidence rule, under which courts prefer originals to duplicates.[462] Whether computer-generated information will be treated as an original or as a duplicate, will depend upon the purpose for which the evidence is offered. The rule defines "original" to include any print-out or other output readable by sight of data stored in a computer.[463] In order to qualify as an original, however, a print-out or computer output must be "shown to reflect the data accurately. . . ."[464] While, in the proper circumstances, print-outs or outputs offered to prove the contents of data stored in a computer may qualify as originals, they will be treated as duplicates when offered to prove the contents of a record that originated elsewhere before being stored in the computer.[465] Even where the computer record is a duplicate, however, a duplicate will generally be admissible unless: "(1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original."[466] Thus, the keys to admissibility are, once again, accuracy and reliability.

Third, because computer records are out of court statements, the proponent of such records should anticipate a hearsay objection.[467] In ordinary civil litigation, computer-related evidence obtained from an opponent's computer system will often be admissible as an admission of a party opponent.[468] Where the evidence is obtained from a third party who is not an agent of the opponent, the proponent will have to satisfy one of the exceptions to the hearsay rule. For computer records, the most

---

finding that such information is trustworthy and the opposing party is given the same opportunity to inquire into the accuracy of the computer and its input procedures as he has to inquire into the accuracy of written business records.") (citation omitted), *cert. denied*, 423 U.S. 985 (1975).

462. *See* FED. R. EVID. 1002 ("To prove the content of a writing . . . , the original writing . . . is required except as otherwise provided in these rules . . . ."); *see, e.g.*, United States v. Foley, 598 F.2d 1323, 1338 (4th Cir. 1979) ("The computer print-outs qualify as duplicates of the diskettes within the meaning of Rule 1006."), *cert. denied*, 444 U.S. 1043 (1980). For purposes of this rule, the term "writings" includes "letters, words, or numbers, or their equivalent, set down by . . . magnetic impulse, mechanical or electronic recording, or other form of data compilation." FED. R. EVID. 1001(1).

463. FED. R. EVID. 1001(3).

464. *Id.*

465. *See* 6 WEINSTEIN, *supra* note 262, § 1001.11[4].

466. FED. R. EVID. 1003.

467. *See* FED. R. EVID. 802 ("Hearsay is not admissible except as provided by these rules . . ."). Hearsay is defined as "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted." FED. R. EVID. 801(c).

468. *See* FED. R. EVID. 801(d)(2); *see generally* Long, *supra* note 28, at 413.

likely candidate is the business records exception.[469] Here too, however, one of the essential criteria for admission is reliability of the system.[470]

In sum, accuracy and reliability are crucial determinants of whether computer records are admissible. Importantly, however, even where such factors do not preclude admissibility, they may, nonetheless, be considered by the finder of fact in determining what weight to afford computer-related evidence.[471] Thus, when conducting discovery, litigants must be careful to obtain and preserve evidence in a manner that is accurate and reliable. In addition, litigants must anticipate that computer-related evidence may be offered at trial by the opposing party and, accordingly, must conduct any needed discovery to undercut the accuracy and reliability of the opposing party's evidence. This type of discovery might explore such areas as errors or omissions in data entry, errors in output instructions, errors in programming, the integrity of computer storage media, loss in power supplying the computer systems, and malfunctions in computer systems.[472]

Some of the hazards relating to these concerns are illustrated by *Gates Rubber Co. v. Bando Chemical Industrial, Ltd.*[473] In *Gates Rubber*, the plaintiff hired a technician to copy the defendant's computer storage media in an effort to show that the defendant had wrongfully deleted material computer evidence after the commencement of litigation. The plaintiff's spoliation claim, however, was undercut by two mistakes made by the plaintiff's technician. First, in using a program to recover deleted files, the plaintiff's technician unnecessarily copied that program onto the defendant's hard drive, thereby randomly overwriting seven to eight percent of the information on that hard drive before any efforts could be made to recover the deleted files. Thus, it was impossible to determine what items were overwritten by the file recovery program. Second, instead of making an "image backup" that would have copied every bit of information contained on the hard drive, the plaintiff's technician merely performed a "file by file" backup, which only copied existing nondeleted files on the hard drive. By performing an inadequate backup, the plaintiff's technician failed to obtain the creation dates of

469. *See* FED. R. EVID. 803(6); *see generally* Fromholz, *supra* note 30, at 445-51; Long, *supra* note 28, at 413-17; Warton, *supra* note 460, at 736-38.

470. *See* 5 WEINSTEIN, *supra* note 262, § 803.11[3].

471. *See, e.g.* United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts, whether resulting from incorrect data entry or the operation of the computer program, as with inaccuracies in any other type of business records, would have affected only the weight of the printouts, not their admissibility."); United States v. Vela, 673 F.2d 86, 90-91 (5th Cir. 1982) (same holding for telephone billing data), *reh'g denied*, 677 F.2d 113 (5th Cir. 1982) (table).

472. *See* Warton, *supra* note 460, at 735 (listing these areas as potential avenues for attacking admissibility).

473. Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996).

certain files that overwrote deleted files. Without this information, the court could not determine whether files overwriting deleted files were created prior to the litigation, which would have shown that the deleted files were not improperly erased after the litigation began. The court weighed these factors against the plaintiff's claim that the defendant had spoliated evidence.[474]

Accordingly, before conducting computer-related discovery, it is often crucial to obtain a competent technician. Such a technician should be versed in chain of custody procedures.[475] In particular, consistent with *Gates Rubber*, commentators recommend obtaining multiple mirror image backups of the computer storage media in question, including a pristine copy to be used at trial and working copies to be used by the parties' technicians.[476]

VII. CONCLUSION

Although the Federal Rules of Civil Procedure and statutes governing procedure provide ample mechanisms to resolve most issues involving discovery of computer-related evidence, this new form of discovery will transform the way cases are litigated. To conduct and respond to requests for such discovery, litigators must grapple with unfamiliar technology and often must litigate in the context of unusual procedures. Even in the context of resolving traditional disputes over access and protective conditions, courts will often resort to discretionary safety valves provided by the rules. Until litigators and judges gain greater familiarity with these issues, disputes over computer-related discovery are likely to yield more fact-specific discretionary rulings that offer minimal guidance to the bar.

In this uncertain environment, a premium will be placed on a party's ability to map new technological terrain and to adapt existing procedures to overcome obstacles on that terrain. Although the procedural framework for discovery may remain much the same, discovery of computer-related evidence will take the existing procedural system into a new dimension.

---

474. *See id.* at 112-13.

475. *See* Brill, *A Lawyer's Place in Cyberspace, supra* note 18, at 10; Kashi, *How to Conduct On-Premises Discovery, supra* note 4, at 30; Middleton, *supra* note 10.

476. *See* Brill, *The Secret Life of Computer Data, supra* note 13, at 32; Howie, *supra* note 7, at 72; Johnson-Laird, *supra* note 5, at 9; Kashi, *How to Conduct On-Premises Discovery, supra* note 4, at 32; Leibowitz, *supra* note 10, at A13.