4 Tex. Intell. Prop. L.J. 57

Texas Intellectual Property Law Journal
Fall, 1995

Symposium: The Emerging Law of Computer Network

FINDING OUT WHAT'S THERE: TECHNICAL AND LEGAL ASPECTS OF DISCOVERY

James H.A. Pooley[a1] David M. Shaw[aa1]

Table of Contents

I. Introduction

Computer technology and electronic communications are pervasive in our society. It is the rare business transaction that does

not in some way involve computerized data transfer or analysis. It is the exceptional document that is now typed on a typewriter and corrected with correction fluid. Even as far back as 1973, courts were cognizant of the fact that "computerized record keeping is rapidly becoming a normal procedure in ***58** the business world."[1] It is estimated that, in the modern business world, at least thirty percent of electronic data never realize embodiment in ink on paper.[2] It is reasonable to anticipate that most business information will eventually be stored exclusively in various electronic media.

As a result, computers and electronic data have become vastly important sources of information and, for attorneys, evidence in the ever-competitive world of litigation. This paper is designed to introduce the reader to the subject of acquiring that information and to provoke some thought into the best means of doing so.

II. The Law

Rule 34 of the Federal Rules of Civil Procedure was amended in 1970 to address changing technology, thereby indisputably bringing the Federal Rules into the computer age and evidencing that electronically-stored information is discoverable.[3] The rule now states that "[a]ny party may request to inspect and copy, any designated documents (including other data compilations from which information can be obtained, translated, if necessary by the [[[responding party] through detection devices into reasonably usable form)."[4] The change clarified that discovery of information stored in new and different media, including punched data cards, computer tapes, floppy and hard disks, and computer memories, even though that information is not as accessible as the traditional tangible form of information (paper), is nevertheless both necessary and proper.[5] The information provided, however, must be in a "reasonably usable form," and courts will ensure that the party requesting the information is able to access the data.[6]

*59 III. The Practice of "EMD" (Electronic Media Discovery): Finding the Smoking Disk

To the extent that information and evidence are available only in the traditional sense--in documentary and other tangible forms--resort to discovery of electronically-stored data is unavailable. To the extent that documentation and other evidence are available in both types of media, however, it generally is desirable to seek the electronic data over the "harder" evidence because of the greater amount of information that can be learned from such electronic evidence.

For example, remarks that are associated with a document but which are not normally seen when a document is viewed, and certainly are not present when the document is printed, can be quite telling. Comments in a "remarks section" that are used to help the reader to recall quickly the substance of the document, comments in headers and footers, short entries to aid in indexing, or even something as simple as a filename can reveal more about the document than would be learned simply by reading the text. It also may be revealing to learn when a document was last accessed and updated, especially if it occurs during the litigation when the document was otherwise quite old. Perhaps recognizing this, the *Manual of Complex Litigation* views production of computerized information in machine-readable form as the primary mode of responding to discovery requests in complex cases, with the production of printouts a secondary alternative.[7]

This position is not surprising for another reason. Handling large numbers of documents by computer is much more efficient than doing so manually. A study advocating the use of electronic storage had a person attempt to locate and retrieve twenty paper documents from a group of 20,000 stored in a single location. After sixtyseven hours of effort, only fifteen had been recovered. When the same task was run on 20,000 electronically stored documents, however, it took under three seconds to retrieve all twenty.[8]

A. Potential Gold Mine or Genuine Mine Field?

How electronically-stored information is viewed typically depends on which party has control of the information. Plaintiffs are beginning to treat such data as a gold mine ***60** in which to search for the devastating memorandum or other piece of evidence that supports the allegations leveled. Until potential defendants realize that uncontrolled and unshepherded use of computer systems can foster a breeding ground for evidence which threatens a company's well-being, the likelihood of a litigation disaster is ever present.

Of interest to a plaintiff, a company's database may contain an earlier and safer design of a product that is the subject of a product liability suit; an earlier draft of a sensitive document to prove intent in a fraud claim; altered spreadsheets in an

investor fraud case; company strategies to eliminate competitors in an antitrust case; employment records in a discrimination case; memoranda evidencing willful infringement in a patent case; and, of course, financial records useful in just about any case. Such paperless evidence includes computer-stored records in a variety of media, electronic mail messages (e-mail), voice-mail and electronic bulletin boards. Some documents or memoranda are stored only by electronic means precisely because of their sensitive nature. Realizing that this untapped wealth of evidence is waiting to be quarried is half the battle.

One of the reasons such information is lying around waiting for a lawsuit is because electronic data maintains a low profile, unobtrusively accumulating for years on the unassuming computer in the office corner. Imagine a company with just ten employees, each having an office with a computer. Think of ten paper documents--memoranda, messages, drafts--being created in each office every day. After six months, it would be abundantly clear that there is a problem with file management and unnecessary retention of documents. Perhaps it would trigger instituting a document retention/destruction policy to facilitate a periodic house-cleaning of unneeded paper.

It is another matter entirely, however, when all of the documents are stored magnetically or electronically and are, therefore, invisible to the company's employees until the storage capacity of the system is finally reached, at which time more memory is added and/or old information is off-loaded to tapes.

Rarely is it necessary to save old drafts of memoranda and contracts, previously digested messages and outdated strategies. Yet saving such obsolete information is the norm. In fact, the odds are that the reader is guilty of this same offense--even in paper form, never mind electronic form--and probably has no supportable reason for doing so. It is our job and duty as our clients' representatives to take advantage of others' sloppy management of records and retrieve the "smoking disk."

B. Electronic Information Can No Longer Be Ignored

For a modern litigator to ignore intangible, electronic data is to risk losing otherwise winnable cases, to risk exposing clients to expensive and otherwise avoidable ***61** judgments, and to risk the imposition of sanctions for failure to produce,[9] or for destruction of, available files.[10] Attorneys also risk charges of malpractice by frustrated clients for failing to represent their interests adequately by not using modern technology to discover the otherwise obvious and critical electronically-stored evidence.[11]

C. Requisite Skills for Effective Discovery

Litigation counsel must be versed in the appropriate terminology and technology. Using the correct lingo may more accurately define exactly what is being sought by the request. Moreover, carefully crafting the discovery request may aid in avoiding an otherwise effective "unduly burdensome" objection by the opposing party.[12] Even if a generally-worded request results in the production of some evidence in whatever form, the attorney must know how to follow that production with questions sufficient to determine whether the information produced is all that she is entitled to receive. To that end, the attorney should be able to explore adequately the nature and extent of the computer system, methods of storage, automated document retention programs (backups), etc. The computer system's degree of complexity will dictate the attorney's required competence in handling various lines of questioning.[13]

When a discovery dispute occurs, an attorney is generally able to approach the judge, lay out his position, and let the judge decide whether he has a right to get what he has requested. Often, the issues are quite clear if the dispute concerns a single document, or a box of evidence, or a room full of files. It is easy to envision the work necessary to prepare such documentation for production. But what about a request for access to the other party's computer system to hunt for the smoking gun? Should that be allowed? Not only is this an issue of educating the judge, if necessary, on the pertinent law in the area, but it is also an issue of the technology. It certainly would be helpful to the court to hear an explanation of the technology in order fully to fathom the true scope of the request. Once an objection is lodged, the judge will have to understand how magnetic records are created, maintained and accessed in order to ***62** render an intelligent and informed opinion. An attorney seeking electronic discovery thus has the added burden of familiarizing the judge with the technology in use.

D. Obtaining Discovery

The first step in approaching the issue of electronic discovery is to move quickly to preserve the evidence. A company that enters into litigation as either plaintiff or defendant has an obligation to preserve evidence. Yet a company, by simply continuing to use its computers after the lawsuit has been filed without safeguarding the data present in its system, can destroy otherwise valuable evidence that should be available to the adversary. It may be necessary to get the court involved at an early stage to ensure that the other side preserves its electronic information.

It is also important to enter the electronic discovery game early because of the amount of detail involved in discovering another's electronic files. First, find out what kind of databases they have. How can the data be manipulated? What software applications are involved (commercially-available, custom, or a combination)? If custom software applications are involved, the attorney will need to prepare an inquiry into the command structure of the system in order to pose the right questions and to understand the responses. This will most likely require the aid of someone familiar with management of databases.[14]

Once the ground work has been laid by learning about the system in question, a litigator can then go after the targeted information that is stored within the system, being careful to consider all of the sources about which he has just learned.

Suggestions for discovering electronic information include:
1. Request production of documents in computer-readable form. If the documents are produced in "native" form, there may be problems in accessing the information. Production in generic form (e.g., ASCII) would facilitate processing but would result in loss of some of the file "indicia" that would be available in the "native" form--thus, make sure your request corresponds to your case strategy.

2. Offer to share the costs of production of the data in electronic form, or demonstrate undue financial hardship if the data are not so produced. Anticipate the downside to such an offer--it may become inordinately expensive as the plaintiff, or, alternatively, the party offering to pay may want to intrude to an intolerable extent into the defendant's attempts to comply with the discovery requests so as to ensure the money is being wellspent.

3. Decide whether to craft the requests in such a manner that your adversary is immediately alerted to the presence of damaging evidence or to information that it would rather not produce. Do you, for example, want to demonstrate that your opponent has a real fight ***63** on its hands in the hopes of fostering settlement, or do you want to surprise your opponent with the incriminating evidence at the last moment?

4. Seek any electronic data referenced by a testifying expert.[15]
Also, consider the propriety of combining a deposition with a request for production, so that the discovering attorney can observe the use of the company's computer system while it is producing the responsive documents and examine the system user on exactly what he is doing to manipulate the data.

E. Electronic (E-) Mail

With the advent of the Internet and the World Wide Web, electronic mail (e-mail) has come of age. Due to its growing and generally uncontrolled use, e-mail can provide a wealth of information about a company's thought processes that would otherwise be unavailable. The overarching problem with, or beauty of, e-mail, depending on your point of view, is that messages are typically written in an informal manner. Compare this to the almost ceremonious process of authoring a real document, which itself stresses the importance of the document and its potential use as evidence. Employees say things in e-mail messages that would never be stated directly to a person or consciously memorialized in a writing.[16] E-mail messages may also contain personal thoughts and notes to remember, as well as unwise and inappropriate comments about another person.

This lack of reluctance to speak one's mind is partially due to the anonymity afforded by the medium of communication and the seeming privacy with which the message is communicated--if it is addressed to [Bob] only, how can anyone else get to it? Yet off-the-cuff remarks can be dangerous if taken out of context in litigation. That e-mail messages can provide damning evidence really has yet to dawn on the collective societal and legal psyche.[17] Oliver North, however, knows full well about the damage e-mail can do. During the Iran-Contra affair, "deleted" messages were retrieved from the government e-mail system and used as evidence against him.

***64 F. Discovery of "Lost" or "Erased" Data**

One commentator has used the term "shadow data" to describe information that is thought to have been deleted.[18] When a computer file is "deleted" or "erased," the group of data merely is marked to be overwritten. That it is marked, however, does not mean that it is immediately unrecognizable. Indeed, if the computer were not used thereafter, the "deleted" information would survive forever. When and how data are ultimately overwritten depends entirely on the type and frequency of use of the computer after the file in question is marked: the actual erasure may occur in the next few seconds of use, or perhaps not until some weeks or months later.[19]

There are sophisticated computer programs that can retrieve e-mail messages and computer files from the guts of the computer system long after those messages and files were thought to have been forever deleted. So why ignore this information? Imagine a document-destruction policy that only requires "destroyed" to be marked on the top and side edges of documents to be destroyed. Obviously the documents still exist and are perfectly readable. The same is true of deleted files until they are overwritten.

Indeed, the mere fact that files were destroyed, perhaps systematically, could prove to be more valuable information than the actual files retrieved, especially if such fact is used to prove a cover-up, for example. Deletion of whole blocks of data, which is detectable though various modern computer tools when such activity is not the norm, raises the issue of motive, and may provide circumstantial evidence of a "guilty mind" through a concerted effort to eliminate any document vaguely related to the area of sensitivity.

G. Areas Not to Be Overlooked

Backups and archival tapes are used mainly as precautionary measures to preserve information in case the main computer system suffers some mishap. Various operating systems, other than DOS, often create logs of data files and system users that were at one time present on the system. Both sources can provide valuable information.

Do not overlook "off the end" data stored on magnetic tapes. "Off the end" data essentially consist of old information originally stored on a tape but not overwritten when the tape was reused to store other information. Because it has not been overwritten, the information is as viable as when it was stored, and may provide information that the company thought was long dead.

Do not neglect the "broken" hard disk that contains otherwise valuable information. If the only part of the hard disk that failed is the electronic controller, then ***65** the information on the disk is viable. In essence, it is like a locked box that can be opened only with a new key. One would not ignore a locked box of documents just because the owner could not find the key. Consider treating a broken hard disk likewise.

In discovering a company's computers, one may become focused on the mainframe and the points of mass storage. Do not forget PCs connected in a LAN, but which may have independent storage capacity, or the office's portable PCs used by employees while away from the office. Also, floppy disks or diskettes lying around in various locations may contain documents never transferred to the main system because the disks were used to transfer files between home and office.[20]

Finally, this paper has discussed electronic information containing words and numbers and the discoverability thereof. Think about searching for other evidence stored on the computer that could prove just as valuable--e.g., diagrams and designs, digitized images, motion pictures and audio recordings. For example, you file suit against Disney for copyright infringement of your cartoon character, and you want to verify that all digitized images of the development of the cartoon character in question have been produced. How do you do it? Experts will have to be involved to guide an attorney through this constantly developing field.

IV. Resisting Electronic Discovery

A. What's a Business to Do?

In this age of electronic information, a business needs to take steps to be prepared for discovery of its electronic systems. If the company waits until it is embroiled in litigation before it closely analyzes exactly what is stored in its files, it will be too late. Any review needs to be conducted by both technical and legal personnel to sensitize the company to the risks involved in its conduct.

Steps a company can take include:
• learning how its systems work (hardware and software) and the locations in which data are stored (mainframe, LANs, PCs, tapes, disks, etc.);

• creating a system or series of rules for creating, storing, locating and retrieving different types of information;

• establishing and implementing an information creation/retention/destruction policy or plan;

***66** • educating its employees on any implemented plan and on potential liability of the company based on electronic information, including the use and abuse of e-mail; and

• periodically inspecting the policy or plan to determine its strengths/weaknesses and employees' compliance.
From the company's point of view, it would prefer to learn sooner rather than later that potentially damaging information is being retained unnecessarily in the normal course of affairs when no suit is pending, because this can be dealt with through adoption of a document/data retention schedule. If a company does not have some sort of retention/destruction policy and suddenly destroys a group of documents on the eve of contentious litigation, the trier of fact is likely to draw an adverse inference from such conduct.

Be aware, however, that absent a reasonable business purpose, destruction of information solely to frustrate a subsequent suit not only reflects badly on the company involved, but can also provide a basis for sanctions, adverse evidentiary presumptions, and even tort liability for spoliation.[21]

In light of increasing discovery of electronic information, a company should encourage employees to draft all documents, especially e-mail messages, with the expectation that they may be subject to the scrutiny of a judge or jury at some later date in the context of an adversarial proceeding. Sensitize employees through education to the notion that e-mail is not always an appropriate substitute for old-fashioned conversation.

A company also should be on the lookout for employees who unnecessarily save e-mail messages and other documents that otherwise would be discarded through the regular document retention program. Such unauthorized retention can be just as damaging as not having any retention program at all. Moreover, if normal procedure requires systematic destruction of old documentation on paper, then be sure to do the same to electronic information.

On the opposite side of the issue, a company should also be aware that by storing extremely sensitive documents only on electronic media, it risks losing the valuable information more so than if the files were stored in a cabinet off-site. Simply due to the dynamic interrelationship among data stored on a disk, loss of one document most likely will compromise others, rendering them useless as exculpatory evidence. Also, it is foreseeably easier simply to misplace several 3.5" disks than it is to lose a file ***67** cabinet full of documents, although both may contain the same amount of information. Thus, to the extent that a company has critical documentation that it simply cannot afford to lose, it should consider maintaining both electronic and hard copies.

One final, emerging option is that of encryption. Encryption provides the possibility of securing electronically stored data. It is essentially a way of putting information inside electronic envelopes which can only be opened by the recipient. However, there are problems with this option.

National Public Radio recently carried a story about Mr. Philip Zimmerman, a computer consultant, who made available on the Internet, free of charge, a rather effective encryption program for e-mail named "Pretty Good Privacy" or "PGP."[22] The U.S. government, however, currently classifies encryption techniques as weapons or "munitions" under 22 U.S.C. § 2778 (1995), thereby placing severe restrictions on the distribution of such information. Zimmerman thus faces serious legal troubles as a consequence of his actions, even though PGP is now recognized as the main choice of Internet e-mail users

worldwide.[23]

If encryption becomes popular, a party discovering the information will need to either acquire the "key" or "crack" the code--a real problem if the employee who protects the file has "forgotten" the code, either as a matter of fact (because he changes the code regularly) or because he is simply unwilling to cooperate. Moreover, if the code is truly forgotten, a defendant may not be able to access its own information that would otherwise prove to be exculpatory.

B. Attorney-Client Privilege/Work Product Doctrine

The attorney-client privilege and the work product doctrine, codified in Rule 26(b)(3) of the Federal Rules of Civil Procedure, apply as much to electronic data as to paper documents, and thus should be used to their fullest extent when document production during discovery is requested.[24] Concerning waiver of these privileges, beware of instant retrieval. Computers have enabled massive amounts of information to be almost instantly recalled from the depths of storage for perusal and analysis. While most view this capability as an enormous blessing for document handling, an attorney required to produce electronic evidence cannot ignore the dangers of such access. The attorney may be tempted to "data-dump" the memory's contents and let ***68** opposing counsel sift through the contents. Yet to do so would be to risk providing more information to the other side than it has a right to see.

The laborious business of going through every document to determine whether any contain material that should not be produced under the attorney-client privilege cannot be ignored. Moreover, waiver of the privilege covering a single electronically-stored file can lead to waiver of the privilege for many other documents concerning related subject matter, including other electronically-stored information as well as traditional documentation thought to be safe because previously found and designated privileged.[25] Because of the danger of waiver, the recommended practice, if one is ever the subject of organized electronically-stored information discovery, is to stipulate that any inadvertent production of documents does not waive any privilege.

The issues of work product are more subtle. A database may contain no document that, by itself, or even in combination with other documents, constitutes work product that can be withheld. But the mere method of storage or organization of certain documents--organized by legal issue, importance of issue, attorney handling the issue or potentially in any order other than alphabetical--can reveal the thought processes of an attorney or agent sufficiently to constitute work product.[26] Do not overlook this possibility in seeking to oppose production of otherwise discoverable materials.

C. Litigation Support Systems

A litigation support system (LSS) is "a record of potentially relevant information developed in anticipation of litigation and stored in a computer. The computer allows lawyers quickly and efficiently to identify needed documents so that they may be retrieved out of voluminous files."[27] LSSs can take various forms, including simple objective-index systems, index-plus-partial text systems, and full-text retrieval systems, and can be viewed as fitting into a continuum. At the objective extreme of the continuum, LSSs consist solely of documents, without modification, stored in the system for ease of recall. LSSs at the subjective extreme consist entirely of attorney input of summarized documents, indices setting priorities, and theories of the case. The closer an LSS is to the subjective end of the continuum and the more input an attorney ***69** has in creating the LSS, the more discovery-proof it will be.[28] Note, however, that if a testifying expert relies on information in the litigation support system, the whole system may become the proper subject of discovery.[29]

A party might wish to discover an opponent's LSS not only because it would reveal trial strategies, but also because the documents are not otherwise electronically stored, forcing the party to have to input the documents at his own expense. Courts will attempt to avoid such needless duplication of effort if no privilege is violated.[30] This area is ripe for discovery disputes as LSSs are used more and more frequently.

V. Evidentiary Issues

Once electronic evidence has been discovered, there are issues of how one actually introduces the information into evidence. Consider the questions of authentication and identification, hearsay, and the best evidence rule.[31] Although this area of discussion is outside the scope of this article, the need to authenticate the information ultimately recovered is so important

that it should be considered before ever invading the opposing party's computer. If one is not careful to document fully all steps taken in acquiring electronic evidence--such as how the file was found, what tools were used to locate it, where it was found, and how it was transferred to its current format--one may confront problems in attempting to admit the evidence at trial when arguing that a document was found on the opponent's computer system.

In addition, one must ensure that the document is actually what it purports to be. One may face the argument that even though a document was found on the defendant's computer system, no one knows its true source. Although the danger of forgery of evidence is real, considering, for example, that computer hackers are able to forge e-mail messages, the problem presented as a result of such action is not insurmountable. Such activity would only be undetectable in the rarest of instances, and should leave traces that could be discovered through the methods discussed above.

If given access to another's computer system, one should take precautions to document every step taken to acquire the information so that admissibility is not ***70** affected by the search method used. One must be careful that a method used to search for data does not damage or change the original format of the stored electronic data. One should also be careful to avoid creating any basis for a charge of altering or tampering with data, of introducing a virus into the computer being searched, or of inadvertently "crashing" the system and damaging the competitor by losing valuable data besides that being sought. If certain documents need to be manipulated, make a working copy of the files using a foolproof copying process. Store originals in a secure place with limited and controlled access to avoid any possibility of the data being corrupted through alteration or destruction.

VI. Conclusion

Much of the law on electronic discovery is yet to be settled. For example, for a company to meet its obligations under discovery rules, will it have to sift through months of backed-up hard drives, cull and redact backup tapes, and attempt to "undelete" information that does not exist as far as it is concerned? Or will the burden or expense of such activity outweigh any likely benefit?[32] How does a party go about demonstrating sufficient need to gain the right to inspect deleted disks or erased files? These and related questions will provide the basis for much legal sparring in the years to come.

Footnotes

a1 Fish & Richardson, P.C., Menlo Park, Ca.

aa1 Fish & Richardson, P.C., Menlo Park, Ca.

1 Union Elec. Co. v. Mansion House Ctr. N. Redevelopment Co., 494 S.W.2d 309, 315 (Mo. 1973).

2 Jessen & Shear, *The Impact of Electronic Data Discovery on the Corporation,* Address at the National Conference of Am. Corp. Counsel Ass'n (May 1994).

3 FED. R. CIV. P. 34 (1970 Amendments).

4 FED. R. CIV. P. 34. *See* 8A CHARLES A. WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE & PROCEDURE: CIVIL 2D § 2218, at 449 (1994).

5 *See, e.g.,* Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972) (computer tapes proper subject of discovery); *accord* United States v. Davey, 543 F.2d 996, 999 (2d Cir. 1976).

6 *See, e.g.,* Greyhound Computer Corp. v. IBM, 3 Computer L. Serv. Rep. 138, 139 (D. Minn. 1971) (where defendant provided computer tapes that plaintiff was unable to read, court ordered defendant to assist plaintiff in accessing the information with

materials and personnel); Pearl Brewing Co. v. Joseph Schlitz Brewing Co., 415 F. Supp. 1122 (S.D. Tex. 1976) (court ordered delivery of entire system documentation to opposing party); *In re* Air Crash Disaster, 130 F.R.D. 634 (E.D. Mich. 1989) (after producing hard copy printout of simulation, party also required to produce data on computer-readable tape).

[7] MANUAL OF COMPLEX LITIGATION (CCH) (1981) § 2.715 at 153 (cited in National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1262 (E.D. Pa. 1980); *see also National Union,* 494 F. Supp. 1257 (requiring production of material in computer-readable format even after production of the same information in hard-copy); *compare* Williams v. Owens-Illinois, Inc., 665 F.2d 918, 933 (9th Cir. 1982) (court refused to order production of tapes after wage cards already provided), *cert. denied,* 459 U.S. 971 (1982) (described as a "shortsighted" ruling in Richard A. Horning, *Electronically Stored Evidence: Answers to Some Recurring Questions Concerning Pretrial Discovery and Trial Usage,* 41 WASH. & LEE L. REV. 1335, 1344 (1984)).

[8] *See* John H. Jessen, *Electronic Data Discovery: A Powerful Tool for a New Environment,* LAW TECHNOLOGY 19, 21 (Third Quarter 1992) (citing *The Legal Market: Making a Case for Optical Storage,* RESELLER MANAGEMENT 106-10 (Nov. 1990)).

[9] *See* American Bankers Ins. Co. v. Caruth, 786 S.W.2d 427 (Tex. Ct. App. 1990) (default judgment entered against party who failed to produce computer files--party alleged that requested information was stored among 30,000 boxes of materials, when a computer could have easily accessed same information).

[10] Cabnetware v. Sullivan, 22 U.S.P.Q.2d (BNA) 1686 (E.D. Cal. 1991) (destruction of source code used to write software provided ground for default judgment).

[11] *Cf.* Simon Chester, *Must Litigators Use Computers or Face Malpractice?* in WINNING WITH COMPUTERS, TRIAL PRACTICE IN THE 21ST CENTURY 40-43 (John C. Tredennick & James A. Eidelman eds., 1991).

[12] *Cf.* PHE, Inc. v. Department of Justice, 139 F.R.D. 249, 257 (D.D.C. 1991) (burdensome objection rejected where tax records sought were computerized, even though "no program presently exist[ed] to obtain the information requested").

[13] For a list of suggested questions, see Joseph M Howie, Sr., *Electronic Media Discovery: What You Can't See Can Help (or Hurt) You,* TRIAL 70, 73 (Jan. 1993).

[14] *See* MANUAL FOR COMPLEX LITIGATION, (CCH) § 21.461 at 75 (1985) (when obtaining information about systems and programs of the storage and retrieval of computerized data, a party "may need assistance in formulating precise questions and the answering party may need time and special guidance to respond").

[15] For more comprehensive coverage of suggestions for use when attempting either to obtain or avoid discovery of electronic data, *see* John T. Soma & Steven G. Austin, *A Practical Guide to Discovering Computerized Files in Complex Litigation,* 11 REV. LITIG. 501, 515-21 (Summer 1992).

[16] *See, e.g.,* Siemans Solar Indus. v. Atlantic Richfield Co., Cir. No. 93-1126, Fed. Sec. L. Rep. (CCH) ¶ 98, 167, 1994 WL 86368 (S.D.N.Y 1994) (series of e-mail messages alleged to demonstrate concealment of serious flaws in company's main solar energy product during purchase of company).

[17] In Borland Int'l, Inc. v. Symantec Corp., No. 123059 (Cal. Super. Ct. (Santa Cruz) filed Sept. 4, 1992), e-mail messages played a central role. Eugene Wang, a now former employee of Borland, allegedly sent some of Borland's confidential documentation to the president of Symantec using MCI's e-mail service while Wang was still a Borland employee. The messages, which only existed in electronic form on MCI's computers, were discovered by Wang's ex-colleagues shortly after he left Borland for Symantec. Mr. Pooley is counsel for Wang in that matter.

[18] Richard C. Reuben, *Shadow World: Searching Information Highway's Side Roads for Evidence,* 80 A.B.A. J. 115 (Apr. 1994).

[19] *Id.*

[20] For an excellent discussion of the technical side of discovering electronically stored information, see Andrew Johnson-Laird, *Smoking Guns and Spinning Disks,* 11 COMPUTER LAWYER 1 (Aug. 1994).

[21] *See generally* Kirby & Steele, *Consequences of Document Destruction in Commercial Litigation,* in DESTRUCTION OF EVIDENCE 335 (Gorelick et al., 1989 & Supp. 1995); Hill, *Judicial Activism & the Destruction of Evidence: Reconsidering Traditional Responses to Evidence Destruction in Civil Proceedings,* 23 LAND & WATER L. REV. 209, 212-17, 219-21 (1988); Rowse, *Spoliation: Civil Liability for Destruction of Evidence,* 20 U. RICH. L. REV. 191 (1985); FED. R. CIV. P. 37.

[22] *See Feds Say e-Mail Scrambler Is a Weapon* (NPR radio broadcast, Apr. 14, 1995) (available in LEXIS, News Library, Curnws File).

[23] *Id.*

[24] *See, e.g.,* IBM v. Comdisco, Inc., No. 91-C-07-199, 1992 Del. Super. LEXIS 67 (Mar. 11, 1992) (analyzing whether e-mail discussing attorney advice sent to company representative by business practices manager was privileged); Lawyers Title Ins. v. United States Fidelity & Guar. Co., 122 F.R.D. 567 (N.D. Cal. 1988) (denying discovery seeking information about opponent's computer storage, organization and retrieval systems to evaluate compliance with discovery, on ground of work product).

[25] *See, e.g.,* Alldread v. City of Grenada, 988 F.2d 1425, 1434-35 (5th Cir. 1993) (discussing various views of inadvertent waiver); Wichita Land & Cattle Co. v. American Fed. Bank, F.S.B., 148 F.R.D. 456 (D.D.C. 1992) (same). *Compare* Transamerica Computer Co. v. International Business Machs. Corp., 573 F.2d 646 (9th Cir. 1978) (no waiver of privilege for inadvertently produced document).

[26] *See, e.g.,* Santiago v. Miles, 121 F.R.D. 636 (W.D.N.Y. 1988) (files organized by lawyer's program constitute work product and are not discoverable).

[27] Stephen J. Krigbaum, *Computerized Litigation Support Systems and the Attorney Work Product Doctrine: The Need for Court Support Against Discovery,* 17 VAL. U. L. REV. 281, 284-85 (1983).

[28] *See, e.g., In re* IBM Peripherals, 5 Computer L. Serv. Rep. 878, 878-90 (N.D. Cal. 1975) (holding that trial-support system was not discoverable because it constituted data compiled for litigation and reflected counsel's mental impressions, theories, and thought processes); Hoffman v. United Telecommunications, Inc., 117 F.R.D. 436, 439 (D. Kan. 1987) (denying discovery of litigation support system as seeking the opposing party's "discovery plan").

[29] *Hoffman,* 117 F.R.D. at 439.

[30] *See, e.g.,* National Union Elec. Corp. v. Matsushita Elec. Indus., 494 F. Supp. 1257, 1259-60 (E.D. Pa. 1980).

[31] For a general discussion of the evidentiary issues involved, see John R. Thomas, Note, *Legal Responses to Commercial Transactions Employing Novel Communications Media,* 90 MICH. L. REV. 1145 (Mar. 1992); Richard M. Long, Note, *The Discovery and Use of Computerized Information: An Examination of Current Approaches,* 13 PEPP. L. REV. 405, 413-21 (1986).

[32] FED. R. CIV. P. 26(b)(1)(iii).