DISCOVERING AND PROTECTING ELECTRONIC FILES

STEPHEN A. COZEN, ESQUIRE
CHRISTOPHER C. FALLON, ESQUIRE
JAMES P. CULLEN, JR., ESQUIRE
COZEN AND O'CONNOR
1900 Market Street
Philadelphia, PA 19103
(215) 665-2000
scozen@cozen.com
cfallon@cozen.com
jcullen@cozen.com

Atlanta, GA
Charlotte, NC
Cherry Hill, NJ
Chicago, IL
Columbia, SC
Dallas, TX
Los Angeles, CA
New York, NY
Newark, NJ
Philadelphia, PA
San Diego, CA
Seattle, WA
W. Conshohocken, PA
Westmont, NJ

The views expressed herein are those of the author and do not necessarily represent the views or opinions of any current or former client of Cozen and O'Connor. These materials are not intended to provide legal advice. Readers should not act or rely on this material without seeking specific legal advice on matters which concern them.

Copyright (c) 2000 Cozen and O'Connor
ALL RIGHTS RESERVED

I. INTRODUCTION

A. The Nature of Electronic Information

Electronic information is invisible, it can not be perceived by human sense alone. Yet, in the past two decades, it has come to redefine the way we interact. Electronic data on every aspect of our daily lives is compiled and stored not only in computers, but also in our automobiles, microwaves and ATM cards. The business world, in particular, has embraced the electronic revolution, with computers now handling most, if not all, record analysis, data retention, word processing, communication and mail.

As electronic information continues to permeate business practices, it has inevitably become the subject of pretrial discovery disputes. Electronic data can and does exist, even when the author believes it is deleted. Most of the information stored is not viewable with common applications found on the average home or business computer. Even when an opponent believes that they have successfully concealed or destroyed electronic evidence, 'smoking guns' are often waiting to be found. The potential for abuse of discovery has never been easier, and, although litigators need not become computer experts, they must begin to understand the technology in general.

B. Differences Between Electronic and Paper Information

A paper printout of an electronic document is not an identical copy of the electronic original. Indeed, "the two documents cannot accurately be termed "copies" -- identical twins -- but are, at most, "kissing cousins"… perhaps distant ones at that."[1] For example, where a paper copy of an e-mail may contain the author, the recipient, the date and the message content, the electronic original will contain far more, including chain of custody,

[1] Armstrong v. Executive Office of the President, 1 F.3d 1274, 1283 (D.C. Cir. 1993), *rev'd on other grounds*, 90 F.3d 553 (D.C. Cir. 1996), *cert denied*, 520 U.S. 1239 (1997).

veracity of the copies, the document history, the identity of those who received copies of the mail and information on prior versions and revisions. Furthermore, at least 30% of electronic data in the business world never materializes on paper.[2] Obtaining copies of computer printouts, therefore, can never truly be considered complete discovery of all relevant data.

Electronic and paper information differs in a number of important aspects. Initially, electronic information allows for storage of a far greater quantity of information. By way of example, just one gigabyte of text data, a typical storage capacity for most average home computers, printed on 8 ½ x 11 size paper would stack about eighty five feet tall. Handling large numbers of documents by computer, therefore, is much more efficient than doing so manually.[3]

More importantly, given the vast amounts of data that can be stored in relatively small amounts of space, there has been little incentive for businesses to manage, and delete, old records. Unnecessary saving of outdated and obsolete information is now the norm. Consequently, old, unnecessary and potentially damaging electronic data has developed a knack of surfacing in litigation.

Electronic data is also far more pervasive and much more easily disseminated then paper information. Where, just a decade ago, there may have been ten copies of a document in existence, today there may well be hundreds of copies, produced in a matter of minutes, and these copies will probably be spread throughout the world. Accordingly, greater access to such copies is available than ever before.

---

[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] John H. Jessen, *Electronic Data Discovery: A Powerful Tool for a New Environment*, LAW TECHNOLOGY 19, 21 (3d Quarter 1992) (*citing The Legal Market: Making a Case for Optical Storage*, RESELLER MANAGEMENT 106-110 (Nov. 1990)): One study found that it took one person 67 hours to find 15 of 20 documents, stored amongst 20,000, in one location. It took a computer under 3 seconds to recover all twenty.

Electronic data is peculiarly more durable, but, at the same time, more frangible then its hard copy counterpart. It can be destroyed without trace of its former existence, but it can also be far more easily overlooked, and remain in perfect condition indefinitely.

C. Growing Importance of Electronic Information

In 1982, International Business Machines [IBM] launched its first version of the business computer. This early model, soon to become the industry standard, was never intended for mass use, and consequently lacked sufficient security protocols. By 1997, it was estimated that Americans spent 200 million hours a day using computers,[4] a number that has steadily increased ever since.

Modern operating systems such as Windows, in an effort to remain compatible with the original DOS operating system and industry standards, still lack sufficient security for business use. Consequently, most discovery today is possible due to the inherent security weaknesses of the original DOS and Windows operating systems.[5] Given the huge amount of information being processed through business computers, and the lack of sufficient security, "discovery has never held more potential rewards then it does now and increasingly will in the future. There are going to be fewer and fewer secrets that can be kept from *skilled* practitioners of digital discovery."[6]

---

[4] *see* G. Lardner, Jr., *Panel Urges U.S. to Power Up Cyber Security*, Washington Post, Sept. 6, 1997.
[5] Michael R. Anderson, *Electronic Document Discovery: Computer Forensics with a New Twist*, <http://www.forensics-intl.com/art8.html>.
[6] Jerry Saperstein, *Uncovering Electronic Evidence: The Use and Abuse of Discovery in the Age of Technology*, at 4. The author may be reached at <jerry@dsl.telocity.com>.

D. Discoverability of Electronic Data

The Federal Rules of Civil Procedure 34(a) states that "[a]ny party may serve on any other party a request (1) to produce…any designated documents (including…data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form)…"[7]

1. "Documents"

The Federal Rules of Civil Procedure were revised in 1970. The Advisory Committee's Note to the changes explains that the "inclusive description of 'documents' [was] revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices…" Courts have held that discovery of electronic information is both necessary and proper, even if the data is not as easily accessible as traditional forms of information, such as paper documents.[8] In1993, the Seventh Circuit finally laid to rest the question of whether "document" included electronic data. [9] "Today it is black letter law that computerized data is discoverable if relevant."[10]

2. "Reasonably Usable Form"

The Federal Rule of Civil Procedure 34(a) provides that discoverable data must be produced in a "reasonably usable form", and courts will therefore ensure that the party requesting the information is able to access the data. As early as 1978, the Supreme Court ordered a litigant to extract and produce relevant data from its own databases, even though this may have required the respondent to create a new program to retrieve the data.[11] Two years later,

---

[7] FED. R. CIV. PRO. 34(a).
[8] Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222 (W.D. Va. 1972).
[9] Crown Life Ins. Co. v. Craig, 995 F.2d 1376 (7th Cir. 1993), *reh'g denied,* 1993 U.S. App. LEXIS 15995 (7th Cir. 1993).
[10] Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y. 1995)
[11] Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978).

a Pennsylvania court followed suit by ordering a party to cause its computer experts to create a computer-readable tape containing data furnished by them in answer to interrogatories. [12] The Court reasoned that this would be no different from ordering the party to make a photocopy. Subsequent courts have held that, absent a showing of extraordinary hardship, "[t]he normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent."[13]

II. WHAT CAN BE DISCOVERED

A. Types of Electronic Data

1. E-mail

Discovery of electronic mail, or e-mail, is one of the most contentious areas of modern litigation. A recent survey has 98.7% of businesses reporting the use of e-mail, representing a larger number than those using the telephone.[14] The Yankee Group, a market research firm, estimates 263,000,000 e-mail addresses exist worldwide, and that the average white collar worker sends 30 e-mails per day. In 1998, 3.4 trillion e-mail messages were sent worldwide, compared with just 107 billion pieces of first class mail.[15] Thirty two million American workers can now access the Internet from work and thirty seven million American adults access the Internet from home.[16] The result is a deep well of electronic information just waiting to be discovered.

This well is not only deep, it is also wide. Despite evidence to the contrary, most employees still use e-mail under the mistaken assumptions that e-mail can be permanently

[12] National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1262 (E.D. Pa. 1980).
[13] Daewoo Elec. Co. v. United States, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986), *aff'd in part, rev'd in part*, 6 F.3d 1511 (1993).
[14] Saperstein, *supra* n.6, at 23.
[15] eMarketer, Internet marketing group, *see also* Saperstein, *supra n.6 at 24* .
[16] The Strategis Group, *see also* Saperstein, *supra n.6 at 24.*

deleted, and that e-mail is private. To the contrary, e-mail is rarely effectively deleted.[17] E-mail is not subject to an independent privilege,[18] and is also not private if sent over an employer's e-mail system.[19] One court has gone as far as to say that there is no reasonable expectation of privacy in e-mail transmitted over an employer's computer system, even where the employer has told its employees that e-mail communications will remain confidential.[20]

Given these commonly held misconceptions, the content and grammar of e-mail communications is usually very different from paper documents. E-mails are not signed and are rarely reviewed before being sent.[21] They often contain comments or messages that one would not typically memorialize in written correspondence. [22] As a result, e-mails often contain conversations that would previously have been left at the office water-fountain.

E-mails can also be easily taken out of context. As words appearing on a flat screen, without accompanying facial expressions, vocal inflections and body language, they can often lead to misinterpretation. In an e-mail it is very easy for baseless opinion to appear like fact.[23] Unnecessary e-mail communications have become the bane of modern attorneys.

2. Network Logging Records

The last decade has seen the exponential growth of the Internet, and business networks. Proxy servers, attached to the networks, generate detailed logs showing which machine and user accessed which sites and what data was returned to them. Access to these

---

[17] *See infra.* at p.7.
[18] S*ee* In Re Brand Name Prescription Drugs Antitrust Litigation, 1995 WL 360526 (N.D. Ill. 1995).
[19] S*ee* Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).
[20] Restuccia v. Burk Tech., Inc., 1996 WL 1329386 (Mass. Super 1996).
[21] *See* B. A. Olmsted, *Electronic Media Management and Litigation Issues When Delete Doesn't Mean Delete*, 63 DEF. COUNS. J. 523-524 (Oct. 1996).
[22] *Id.*
[23] S*ee* Jeremy D. Mishkin, *The Paper It's Written On,* Vol. 25, 4 LITIGATION 17 (Summer, 1999); *See also* S.C. Gwynne and John F. Dickerson, *Lost in the E-mail,* (Apr 21, 1997) <http://www.time.com/time/magazine/1997/dom/970421/business.lost_in_the_e.html>.

logging records can prove fertile information, particularly in sex discrimination cases where, for instance, discovery can lead to evidence that a party regularly visited pornographic web sites.

Networks may also contain very personal and candid profiles on users. It is dangerous to assume what sorts of relevant information may be stored on a network. Unfortunately, network-logging records can become quite large and are routinely discarded by network administrators. Therefore, you should attempt discovery early and often.

3. Application Data

When running a typical application, including human resource applications, such as Word, Access and Excel, the computer will store much more information than what you see on the screen, or in a printout. This information can include evidence of earlier versions or revisions of a document, or even previous authors and recipients - which can prove invaluable when attempting to prove spoliation[24] or impute knowledge upon a particular party.

B. The "Lazarus Phenomenon"[25]: The Myth of Erased, Deleted, Destroyed and Lost Electronic Evidence

In the absence of specialized software designed expressly to extirpate data, when a person deletes or erases a document or object through the use of their operating system, or application, the actual data is neither erased nor deleted.[26] Essentially, 'deleted' data gets marked as a space that may be written over, and remains on the disk or hard drive until overwritten. "Imagine a document-destruction policy that only requires 'destroyed' to be marked at the top and side edges of document to be destroyed. Obviously the documents still exist and are perfectly readable. The same is true of deleted files until they are overwritten."[27]

---

[24] *See infra* at p.30.
[25] Jean Marie R. Pechette, *Electronic Records are Discoverable in Litigation*, THE NATIONAL LAW JOURNAL, Monday, June 27, 1994.
[26] Saperstein, *supra* n.6.
[27] J. H. A. Pooley and D. M. Shaw, *Symposium Article, The Emerging Law of Computer Networks: Finding Out What's There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57 (1995).

Even if written over, or scrubbed clean with special permanent deletion software, the old data can still sometimes be recovered with chemical and electron microscopy techniques.[28] At the very least, it may be possible to prove deliberate spoliation of relevant information. Electronic discovery has already led to the recovery of supposedly 'deleted' smoking guns in a number of cases.[29] Consequently, if, in response to a discovery request, you are met with a 'deleted' files excuse, it is wise to immediately request inspection of an adversary's computer system.

C. Sources of Hidden Data

1. Hard Drives

Federal Rule of Civil Procedure 34(b) permits a party to inspect documents "as they are kept in the usual course of business." This includes the inspection of documents in their electronic source. Often counsel, and sometimes their clients, will not know the full extent of their organization's technology resources. Researching the extent of such resources, however, is the responsibility of all careful litigants. It is important to make sure all responses to production requests include every place the information you seek may be found, including the electronic copy of information. Unlike paper discovery, a party wants the "dump truck" response wherever possible - this is often the best way to find the 'smoking gun'.

So far, courts have been willing to allow broad discovery of electronic data. In *Gates Rubber Co. v. Bando Chemical Industries Ltd.*,[30] the court ordered a site inspection and directed that no records be destroyed. The court permitted discovery of all computerized files, and access was granted to the opponent's entire hard drive. The court later criticized the

[28] *See* David S. Bennahum, *The Daemon Seed*, (May 1999)<http://www.wired.com/wired/archive/7.05/e-mail.html>.
[29] S*ee* Lexis-Nexis v. Beer, 41 F. Supp. 2d 950 (D. Minn. 1999).
[30] 167 F.R.D. 90 (D.C. Cir. 1996).

plaintiff's computer expert for not cloning[31] the drive, noting that a party has "a duty to utilize the method which would yield the most complete and accurate results."[32]

2. Backups and Archives

Ensuring the safety of electronic data by making regular backups of all, or significant parts, of the computer system is now standard business practice. Generally speaking, most organizations backing up to tape use between three or ten tapes that are rotated on a regular, scheduled basis, with a few offsite copies for disaster recovery. Immediate discovery, or a protective order, may prove vital as the oldest backup you may hope to recover may only be between ten and twenty-one days old.

Sometimes an organization may only back up the new files in its system, therefore old files may remain untouched for years. With tape backups, the ends of tapes may remain uncovered for significant periods of time and this "off the end" data may prove invaluable.[33] The possibility of old, yet still valuable, information being stored on an old or supposedly damaged computer should not be overlooked. If there is a problem with a computer's drive reading mechanism, the drive itself, and the information on it, may still be viable.

3. Desktop Computers and Workstations

An employee's personal computer, or standalone workstation, may store information that has been deleted off the network. Employees tend to develop a habit of copying files onto their personal hard drives, or onto floppy disks for transportation. This can provide a useful source for information that has been deleted, as often employers will remain completely unaware of its existence.

---

[31] i.e., providing an exact replica.
[32] 167 F.R.D. 90 (D.C. Cir. 1996).
[33] Pooley and Shaw, *supra* n.27.

4. Laptops, Palm Tops and Home Computers

In *Northwest Airlines, Inc. v. Local 2000, International Brotherhood of Teamsters, et al.*,[34] a Minnesota court ordered the search of NWA employees home computers to find evidence of an organized 'sick out.' Other courts have also accepted that even personal hard drives may be the subject of discovery orders.[35] Home computers, laptops and palmtops are all potential storage devices for information that may have been purged from an organization's network. Laptops and palmtops can be, and frequently are, used to send and receive potentially damaging e-mails.

5. Telephone (Voice Messaging) Systems

Modern telephone systems are computer based. In many cases, messages may remain undeleted for months, or years, even though the intended recipient has 'deleted' the message. However, the process of recovery can be labor intensive and quite expensive. In some cases, employees working from home, or temporary offices, have created their own messaging systems.

6. Internet, WAN's, LAN's, Third-Party Repositories, Service Providers

A WAN, wide area network, or LAN, local area network, is essentially any network of interconnected computers, of which the Internet is probably the largest example. Understanding the topography of a network may lead to discovery of information that an adversary claims to have deleted long ago. Recently, there has been an increase in storage of files offsite on the world wide web [WWW], or in third party repositories. Organizations will rarely volunteer the existence of these offsite storage facilities unless specifically requested.

[34] 2000 WL 20881 (D.Minn. 2000).
[35] S*ee* Playboy Enterprise v. Welles, 60 F. Supp.2d 1050 (S.D. Cal. 1999).

Information may be inadvertently stored in offsite repositories. For instance, e-mails are often copied as they pass through service providers. Offsite newsgroups or chat rooms can be ripe with relevant information,[36] and conducting a quick search is relatively inexpensive. Service providers and mail carriers, such as America On Line [AOL], can be subpoenaed to produce copies of emails, or discussions conducted through its service. AOL, in particular, keeps backups of activities on its system and is known for prompt compliance with process.[37]

III. HOW TO DISCOVER ELECTRONIC FILES

A. Knowing the Adversary's Electronic Information System and Software

The overall nature of repositories of electronic data is determined by the operating system used. Microsoft Windows 95 and 98 are promiscuous in automatically writing certain kinds of information onto the hard drive. They may also automatically delete relevant information.[38] "With electronic evidence, you must start with a thorough understanding of what information technology resources are employed by the other side."[39] Without this initial inquiry, you simply won't know where to look, and valuable information may be missed.

Initial use of interrogatories and depositions is, therefore, advisable. You should identify the hardware and software used for different functions, identify all the persons with access to the computer systems of interest and determine how records are generated, maintained and removed. If access to the hard drive is sought, then it is advisable to combine the request for production with a deposition, so you can question the computer expert as to how he is copying or manipulating the data as he does it.

---

[36] <www.deja.com>: maintains archives of thousands of news groups, going back several years.
[37] Saperstein, *supra* n.6.
[38] Saperstein, *supra* n.6.
[39] Saperstein, *supra* n.6, at 10.

Once the response is received, it is vital that you know how to follow production with questions sufficient to determine whether the information produced is all that you are entitled to receive.[40] This too will require adequate knowledge of the adversary's electronic information system and software.

B. The Importance of Timeliness

Given the speed with which electronic information may be processed, and deleted, a litigant can not afford to delay in requesting discovery. Important information may be inadvertently, or purposefully, destroyed in a matter of moments. A company, simply by 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.

You should strongly consider filing some initial discovery requests as early as possible, perhaps coincident with serving the complaint or responsive pleading. You should also seek appropriate protective orders early on and stress the need for true clones to prove the authenticity of any data produced. In certain cases, it may be wise to seek an *ex parte* seizure order.[41]

C. Discovering Evidence

In order to comply with Federal Rule of Procedure 34(b) and to ensure maximum production of relevant information, a request for production which seeks electronic information should be expressed so that there can be no misunderstanding. It should specify the form of storage (tapes, disks or memory), the condition of the information (including back-up and

[40] Pooley and Shaw, *supra* n.27, *see also* Pechette, *supra* n.25.
[41] *See* First Technology Safety Sys., Inc. v. Depinet, 11 F.3d 641 (6th Cir.(Ohio) 1993), *reh'g denied*, 1996 U.S. App. LEXIS 7492 (6th Cir. 1996): Trial court has judicial discretion to grant *ex parte* seizure order to preserve electronic evidence.

deleted files) and the possible locations (on-site and off-site). The requesting party should also be careful to specify that drafts, and revisions, are to be considered new documents, also subject to discovery.[42]

If possible, engage a computer forensic expert to make a 'mirror image' of the hard drive. Otherwise, the expert should take an inventory of the files present. The requesting party should make sure the expert understands the issues in question, and should help to select potential targets or areas of interest. An expert can also help in the drafting of specific term searches.

1. E-mail

The cardinal rule of e-mail discovery is that a requesting party should never settle for hard copies of e-mails. A hard copy may contain five or six fields of information; for example, the date and time of production, the sender's name, the recipient's name, the subject and the message content. The RFC 822, which established the standards for Internet e-mail, describes approximately thirty fields in each electronic version of an e-mail, including the important BCC which notes the additional parties that may have received the e-mail. The BCC field may be used in litigation to impute knowledge of an email's contents to a third party. Furthermore, the potential for and ease of alteration is too great to take e-mail at face value. An electronic copy is the only way to verify authenticity, and avoid repeated discovery requests.

In general, a requesting party should always maintain a healthy skepticism toward the authenticity of a paper copy, and should always insist on production of exact duplicates (clones), preferably of the data stores in which the individual messages are contained. Failure to

[42] Peter V. Lacouture, Esquire, *Discovery and the Use of Computer Based Information in Litigation*, 45-Dec R.I. B.J. 9 (Dec. 1996).

produce the electronic originals should make the requesting party mindful of possible exclusions and spoliation motions.

2. Rule 26, Relevance and the Burden-Benefit Analysis

Courts have proven very willing to provide access to electronic data. A requesting party, however, must still pass certain threshold criteria, such as relevance, and, perhaps, a burden-benefit analysis. In *Playboy Enterprise v. Welles*,[43] a California court applied Rule 26(b)(2),[44] and found that the likely benefits of discovery outweighed the burden it would place on Welles of having her personal computer searched. Playboy was required to provide expert testimony that recovering some deleted e-mail would be just as likely as recovering nothing of relevance. The court appointed its own expert, specializing in electronic discovery, to make a 'mirror image' of Welles' hard drive. Only Welles, her attorney and the court appointed expert were allowed at the recovery procedure. Ms. Welles' attorney was then allowed to review the documents to find the responsive, relevant, and non-privileged information.

3. Counter-Arguments

There are four main objections to the discoverability of electronic evidence: that discovery would place an undue burden on the requested party, that the requested information is irrelevant, that the requested information is confidential, and that the requested information constitutes a trade secret. Each of these will be discussed in greater detail later.[45] Courts have been increasingly reluctant to deny accessibility to electronic data, and each of these objections has been consistently countered with ease.

When the requested party argues that producing the data would impose an undue burden on the party, a requesting attorney should argue for the necessity and potential relevance

[43] 1999 WL 669114 (S.D. Cal. 1999), *supra* n.35.
[44] FED. R. CIV. PRO. 26(b)(2).
[45] *See infra* at pp.22-27.

of an inclusive search. It may be useful to get an expert declaration regarding realistic burden of producing relevant records.

Where a requesting party is accused of engaging in a 'fishing expedition', it may be essential to educate the judge on the nature of electronically stored information. The requesting party should provide an expert declaration of how computers store data, and explain how relevant records may be identified through expert forensic analysis. The requesting party should also show the focus of the request, and possibly consider narrowing the scope of the search.

If the requested party argues that material is privileged or confidential, it may be possible to negotiate a protective order, with protocols for review and production of information. Similarly, with a party claiming protection of trade secrets, pre-discovery negotiation may lead to production of the necessary information without infringement of protected data.

If the requested party claims that a requested document is lost, then the opponent should seriously consider seeking exclusion of any adverse hard copy evidence for lack of authentication. Alterations, prior versions and authenticity can only be discovered through examination of the electronic original.

4. When Not to Seek Discovery

Before seeking discovery of electronic evidence, it is important to consider whether a request for production will be in the best interests of the client. In commercial disputes requests for production of electronic evidence are somewhat "analogous to nuclear deterrence: once one side pushes the button, there is little downside to the other side seeking the same information."[46] A client who has significant technological resources may be uncomfortable with risking exposure of his own electronic sources, and may prefer a limited form of electronic

[46] James K. Lehman, *Tips for Discovery of Electronic Information*, 8, THE PRACTICAL LITIGATOR, 6 (1997).

discovery, particularly given the potential cost of discovery - which often involves six-figure expenses.

IV. HOW TO PROTECT ELECTRONIC FILES

A. Methods to Prevent Unwanted Accumulation of Files

1. 'Knowledge Management', Records Retention Program

"The best defense is to plan long in advance of the discovery request for the contingency of litigation and the likelihood that computer-based evidence will be discoverable. It would be prudent to have in effect a systematic plan for the management of records."[47] The increase in litigation over discovery of electronic evidence has led a growing number of organizations to admit that they do not know what information they possess, or where it is kept. A number of industries now advocate the use of 'knowledge management.' The concept is for the organization to create a process by which all electronic information possessed is eventually identified, indexed and made available as a cohesive entity.

The first step is to learn how the system works, and the locations in which the data is stored. The second step is to create a valid records retention program. A carefully constructed and implemented program ensures that unwanted documents are not inadvertently, or unnecessarily, stored. A valid program has the added advantage of avoiding the implication that harmful documents have been destroyed in order to prevent damaging production in response to pending litigation.[48] An organization embarking on a records retention program, however, must be careful not to conduct the program on an *ad hoc*, or selective destruction, basis -- as either could result in adverse negative inferences.[49]

---

[47] Pechette, *supra* n.25.

[48] "The best way to avoid any appearance that documents have been destroyed in order to avoid production in litigation is to establish a document retention program that is designed for the selective retention and destruction of documents."L. Youst & H. Koh, *Management and Discovery of Electronically Stored Information*, COMPUTER L. REV. AND TECH. J. at 86 (Summer 1997).

[49] Youst & Koh, *supra* n. 48, at 86-7.

a) Fundamental Components of a Valid Records Retention Program

1) Systematically develop the records retention program.
2) Address all your records in the records retention schedules, including reproductions.
3) Address all media in the records retention schedules, including microfilm and machine-readable computer records.
4) Obtain written approvals for the records retention schedules and the program procedures.
5) Systematically expunge records when permitted by the records retention program.
6) Control and manage the operation of the records retention program.
7) Stop expunging the records, even when permitted by the program, when litigation, a government investigation or an audit is pending or imminent.
8) Maintain documentation supporting the development and implementation of the records retention program, including records retention schedules, procedures, changes in procedures, approvals, legal research and listing of records expunged.[50]

b) Guidelines for Developing a Records Retention Policy

1) Preserve, for as long as necessary, in any event for a term not to exceed a specified number of years, all documents maintained in accordance with applicable laws and regulations.
2) File, in a systematic and accessible manner, all documents required for the conduct of business.
3) Identify and preserve all documents relevant to foreseeable or pending litigation and other judicial or governmental investigations or proceedings.

[50] *See* D. Skupsky, *Recordkeeping Requirments,* §§2-10 (1991).

4) Catalogue and reduce to electronic media all documents required to be permanently maintained, for convenient and economical storage and access.
5) Purge all other documents.
6) Conduct regular audits of all electronic data to assure compliance with the retention policy provisions.
7) Establish a mechanism which assures the immediate suspension of data destruction occurring pursuant to provisions of the retention policy.
8) Always resolve any uncertainty as to the application of the retention policy in favor of retention of documents.[51]

c) E-mail

E-mail provides particular concern for a record retention policy. "It is important for companies to train their employees to understand that e-mail is a business document -- that you should keep it only while you need it, destroy it when you don't and don't destroy it if you've been ordered by the court to retain those records."[52] Email should be organized and archived so that important and potentially privileged information can be easily retrieved.[53] Finally, a company wide e-mail policy should be instituted, and employees should be trained in its use.

1) The e-mail system is the property of employer.
2) E-mail is to be used only for valid business purposes.
3) E-mail must not be used for personal matters or comment about others.

[51] *See* W.F. Reinke, *Limiting the Scope of Discovery: The Use of Protective Orders and Documentation Retention Programs in Patent Litigation*, 2 ALB. L. J. SCI. & TECH. 175 (1992).
[52] *See* Roberta Fusaro, *Cases Highlight Need for E-mail Policies*, Computerworld, Oct 5, 1998 (*quoting* Theodore Banks, general counsel at Kraft Foods, Inc., Northfield, Michigan).
[53] Heidi L. McNeil, *Discovery of E-Mail: Electronic Mail and Other Computer Information Shouldn't Be Overlooked*, 56 OR. ST. B. BULL. 21, 23 (1995).

4) E-mail correspondence and messages are to be kept confidential by the employee/user.
5) The employee agrees, and is aware, that e-mail may be monitored and disclosed by the employer.
6) Employees should be educated to recognize common email misconceptions. Humor and sarcasm should not be communicated in e-mail, it can be easily misinterpreted and offensive.
7) Do not compose e-mail messages when angry.
8) E-mail message recipient lists and text should be thoroughly reviewed by the composer for accuracy before being sent.
9) Employees should archive important and critical messages by subject, and delete groups when no longer used or needed.
10) Archived and current messages will be subject to review and production in litigation.
11) E-mail messages that are not archived will be deleted in a specified number of days after being sent.[54]

Approximately 40% of U.S. Corporations now have policies deleting e-mail after 30, 60, or 90 days.[55] A further option, employed by a number of large corporations, is the use of investigative e-mail software that is capable of catching "hot words" and phrases.[56]

[54] Sheila J. Carpenter and Shaundra A. Patterson, *Discovery of Electronic Documents, Practical Tips*, COMMUNICATION NEWS, Winter 2000, at 5. *See also* Lacouture, *supra* n.13.
[55] *See* Roberta Fusaro, *CasesHighlight Need for E-mail Policies*, COMPUTERWORLD, Oct 5, 1998 (*quoting* Michael R. Overly of Foley & Lardner, San Francisco).
[56] *See* Thomas Hoffman, *Brokers Can Monitor E-mail More Easily*, COMPUTERWORLD, July 20, 1998, at 39.

d) Inadvertent Deletion of Relevant Data Through Application of a Records Retention Program: 'Reasonableness Standard'

If a document is destroyed according to a document retention policy, the court will look to see how reasonable the retention policy was given facts and circumstances, how relevant the information was, and how foreseeable the need for the requested documents would be. The court may also consider the frequency and magnitude of other complaints against the party, and whether the party acted in bad faith.[57]

e) Argument Against Knowledge Management

It should be noted that whilst a knowledge management policy makes detection of unwanted, unnecessary and potentially harmful information easier, it also makes detection of illegal deletion or alteration easier, and may help your opponents find the critical document invaluable to their case.

2. Employee Education

A survey of 800 corporate human resource managers in November 1997 found that only 52% had written policies on e-mail use, of these only a quarter were enforcing them. 51% were training workers in appropriate e-mail use, but only 15% of e-mail users treat it the same way as paper documents.[58] Despite a growing number of companies implementing record retention policies, therefore, only a small minority have yet to make them effective. Once a knowledge management plan has been developed, it is essential to educate employees in its use.

Identify employees unnecessarily copying files onto disk, or desktop hard drive. In particular, a company should be aware of unnecessary e-mail retention. Employees should be educated on the potential liability of the company resulting from the misuse of electronic

[57] Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir.(Mo.) 1988).
[58] Business Week - June 8, 1998, *Office E-mail: It Can Zap You -- In Court*.

information, including abuse of e-mail. One New York firm[59] uses an artificial intelligence program called MailCop that warns employees when they send or receive e-mail that may violate company rules. In general, it is worth reminding employees that e-mail is not always a good alternative to an old-fashioned conversation.

3. Automatic Deletion

Software that will really 'delete' electronic data when you tell it to is now readily available.[60] Large corporations, including Citibank, Lockheed Martin and General Electric have begun using Cipher Logics Corp.'s Secure Delete, an electronic shredding program, on all company laptops.[61] Also, a San Francisco based company has developed an encryption code for e-mail that destroys the message, and any copies, after a period of time set by the sender.[62]

A foreseeable problem with automatic deletion programs is that, unless stopped, they will continue after a party has been served with a request for production, possibly leading to sanctions for inadvertent destruction of evidence. A safer way to ensure deletion of records, perhaps, may be deletion as part of a valid records retention policy.

4. Encryption

Encryption is essentially a way of putting e-mails inside an electronic envelope which can only be opened by the intended recipient. The most internationally popular encryption device is called "PGP", or "pretty good protection," invented by Mr. Philip Zimmerman, though using it may be illegal within the United States. The United States government currently classifies the device, which may be downloaded off any number of sites, as

---

[59] Hughes Hubbard & Reed, LLP.
[60] *See* Electronic Evidence Discovery, Inc.
[61] *See* Stepanek, *E-mail: It Can Zap You -- In Court.*
[62] Jacob P. Hart and Anna Marie Plum, *Your Opponent's Electronic Media: Some "Disk-Covery" Disputes for the 21st Century,* ALI-ABA COURSE STUDY MATERIALS, Vol. II Course No. SE63, Dec.1999.

weapons or "munitions" under 22 U.S.C. § 2778 (1995), and Zimmerman has faced serious charges.

Some form of encryption should definitely be considered in the context of avoiding waiver of privilege,[63] particularly if the e-mail involves communication between attorney and client. If an encryption device is used then the organization should be careful not to loose the password to the code, or they should ensure that someone maintains a master key. Without a valid password the data will become useless, and the organization may face sanctions for spoliation.[64]

B. The Importance of Pre-Discovery Negotiation

The court's pragmatism in dealing with e-mail discovery issues offers parties opportunities to be creative in tailoring discovery protocols to minimize adverse legal and financial impacts.[65] Creating discovery databases, and electronic compilations of evidence has become common place in modern litigation. Pre-discovery negotiation has the added advantage of avoiding the cost of implementing an expensive database, only to have it turned over to the opposition at a later point in discovery. The parties may negotiate to create a joint database of information, or may choose to limit the scope of discovery at an early stage. Flexibility is far less likely in an adversarial context.

C. Methods to Prevent Discovery by an Adversary

1. Undue Burden

Federal Rule of Civil Procedure 26 provides protection from unreasonable discovery requests. Under Rule 26(b)(2) the court can shift costs by reference to certain criteria,

---

[63] *See infra* at p.24.
[64] *See infra* at p.30.
[65] Harold C. Hirshman *et al., Developments in the Law Concerning the Discovery of Electronic Mail (*on file with author).

including whether the information sought "is obtainable from some other source that is more convenient, less burdensome, or less expensive," and whether the expense of production "outweighs its likely benefits." Under Rule 26(c) the court can limit the scope of discovery "to protect a party or person from…undue burden or expense." The undue burden objection is the most common approach used to avoid discovery. However, it rarely succeeds.[66]

Courts will probably not require a company to submit to burdensome, intrusive or expensive discovery, where the burden is not justified by the relevance of the evidence likely to be discovered, the size of the case, and the availability of less burdensome alternatives for obtaining the information.[67] Yet discovery requests for electronic data involving six figure expenses have become increasingly common and, in most cases, an electronic discovery request can cause further financial hardship resulting from the interruption of business. Courts have consistently held, however, that merely because a request is costly or time consuming does not render discovery impossible,[68] and courts have been reluctant to find an undue burden on a requested party.

In *Baine v. General Motors Corp.*,[69] the Alabama court expressed concern that reliance on technology should not create a shield or become a hindrance to the discovery of information. The cost inherent in electronic discovery is generally considered to be a necessary and foreseeable business expense, which a party assumes the risk of when it decides to utilize electronic data. "On the one hand it seems unfair to force a party to bear the lofty expense attendant to creating a special computer program for extracting data responsive to a discovery request. On the other hand, if a party chooses an electronic storage method, the necessity for a

[66] Saperstein, *supra* n.6.
[67] *See* Murlas Living Trust v. Mobil Oil Corp., 1995 WL 124186 (N.D. Ill. 1995).
[68] *See* Dunn v. Midwestern Indem., 472 F. Supp. 1106 (S.D. Ohio 1980).
[69] 141 F.R.D. 328 (M.D. Ala. 1991).

retrieval program or method is an ordinary and foreseeable risk… the costliness of the discovery procedure involved is a product of the defendant's record-keeping scheme over which the [plaintiffs have] no control."[70] A more effective way of couching the undue burden objection may be to suggest that the opponent party is attempting to increase the cost of litigation without any real hope of discovering useful information.[71]

2. Relevance: the 'Fishing Expedition'

Overly broad requests, especially where data sought is old and allegedly deleted, may face a relevance objection. In the context of paper storage, the Second Circuit noted that it is not enough to show relevance that the documents relating to the litigation may be somewhere hidden in the file cabinet.[72] The same argument may be applied to unfocused requests for hardware, where a request for individual files, or file categories, would suffice.

In In re Grand Jury Subpoena Duces Tecum Dated November 15, 1993,[73] a New York court quashed a subpoena issued by the grand jury for all computer hard disk drives and floppy diskettes. The court held that the subpoena was unreasonably broad, focusing on the failure to seek production of specific categories of information. Consequently, when facing an overly broad discovery request, the court may require the requesting party to show a "particularized likelihood of discovering appropriate information."[74]

In the majority of cases, however, a relevance objection will probably fail as courts favor broad discovery of electronic documents. In particular, authenticity, earlier

---

[70] 1995 WL 360526 (N.D. Ill. 1995); *see also* Linnen v. A. H. Robins Co., 10 Mass.L.Rptr. 189, 1999 WL 462015 (Mass. Super. 1999): "While the court certainly recognizes the significant cost associated with restoring and producing responsive communications from tapes,… this is one of the risks taken by companies which have made the decision to avail themselves of the computer technology now available to the business world."
[71] *See* Saperstein, *supra* n.6.
[72] In re Horowitz, 482 F.2d 72, 79 (2d Cir.(N.Y.) 1973), *cert. denied*, 414 U.S. 867 (1973), *reh'g denied*, 414 U.S. 1052 (1973).
[73] 846 F. Supp. 11 (S.D.N.Y. 1994).
[74] Fennell v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir.(Me.) 1996).

versions, and 'deleted' files may only be discovered through broad examination of the entire computer system. To such extent, the entire system is implicitly relevant to discovery.

3. Privilege and the Work Product Doctrine

Attorney-client privilege protects privileged electronic records to the same extent that paper documents reflecting similar-types of information are protected.[75] Consequently, it is possible to object to a broad hard drive search on the grounds that if files are to be provided in their native form then too much information would be revealed. Even the organization of files, or the method of storage may reveal attorney work product, by showing, for instance, which files the attorney considers important. As with the undue burden and relevance objections, however, the application of the attorney-client privilege and work product doctrines has been narrowly construed.

a) "Substantial Need" and "Undue Hardship" Exception

The work product doctrine is more of a qualified immunity than a privilege. Under Federal Rule of Civil Procedure 26(b)(3), a party seeking discovery can obtain certain work product upon a showing of substantial need of the materials in preparation of the case, and an inability to obtain the substantial equivalent of the materials by other means without undue hardship. Both "substantial need" and "undue hardship" have been broadly interpreted to allow discovery in most cases.

To show "substantial need", a party need only show that production of the requested evidence will save significant time and money in preparation of case.[76] "Undue hardship" is a relative term that depends on the financial abilities of the parties. Courts have held

[75] *See* National Employ. Serv. v. Liberty Mutual Ins. Co., 3 Mass.L.Rptr. 221, 1994 WL 878920 (Mass. Super. 1994).
[76] In re Chrysler Motors Corp. Overnight Evaluation Program Litig., 860 F.2d 844, 846 (8th Cir.(Mo.) 1988), *see also* Washington Bancorporation v. Said, 145 F.R.D. 274, 279 (D.D.C.,1992).

that it may be synonymous with extensive effort and cost, which the opponent, ironically, often proves by making objections to production on the basis of how much work went into compiling the electronic evidence.[77]

b) Accidental Waiver

A requested party must be very careful not to waive potentially privileged information. The temptation to "data-dump" the information on the opponent's desk in the hope of swamping the adversary should be avoided in the context of electronic discovery. "[W]aiver 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 to be privileged."[78]

In the majority of cases, courts have been quick to find inadvertent waiver of privilege where a requested party turns over electronic data sources without first doing an extensive check of the data produced.[79] In *CIBA-Geigy Corp. v. Sandoz*,[80] the defendants waived attorney-client privilege regarding certain documents by inadvertently producing them. The court held that, absent reasonable precaution to preserve confidentiality, there is a presumption that inadvertent disclosure of a document falling within the attorney-client privilege is the result of gross negligence or intentional conduct, thereby waiving the privilege.

Privilege may also be waived by sending confidential documents over e-mail, when outside parties can readily monitor the communication. A number of state bar

[77] *See* Michael Owen Miller and Brenden J.Griffin, *Computer Databases: Forced Production Versus Shared Enterprise*, 23 LITIGATION 40 (Summer 1997).
[78] Pooley and Shaw, *supra* n.27, at 11.
[79] One Ninth Circuit case does not follow the trend. *See* In re IBM Peripheral EDP Devices Antitrust Litigation, 459 F. Supp. 626 (N.D.Cal. 1978): the court was reluctant to find waiver resulting from inadvertent production of privileged electronic files. Given the changes in electronic discovery since 1978, and the trend towards broad discovery, it is unlikely that this case would have been decided the same way today.
[80] 916 F. Supp. 404 (D.N.J. 1995).

organizations, however, have determined that a lawyer does not breach client confidence by using e-mail,[81] as unauthorized interception of e-mail is generally illegal under the Electronic Communications Privacy Act.[82]

Finally, electronic data compiled by a testifying expert can be discovered.[83] If an expert relies on a party's entire database to support a claim, then the entire database may have to be turned over to the opposition, including any work product that the expert may have relied upon.

c) Decline of the "Strict Responsibility" Rule

The strict responsibility rule of cases such as CIBA is gradually being abandoned by a majority of courts in favor of a new approach to inadvertent disclosure that focuses on the facts surrounding the disclosure on a case by case basis.[84] Also, under the modern Rules of Professional Conduct, an attorney who receives e-mail that has been inadvertently sent to the wrong person, and realizes that she is not the intended recipient, should refrain from reading the document and should contact the sender regarding the return or destruction of the information.

4. Trade Secrets

Federal Rule of Civil Procedure 26(c)(7) expressly authorizes a court to protect trade secrets or other confidential information. In *United States v. IBM*,[85] the New York court held that certain specifications relating to computer systems need not be disseminated if the information rises to the level of trade secret. Where information may be protected under Rule

[81] For example, South Carolina Bar Assn., 97-08 (June, 1997); New York State Bar Assn., ADVISORY OPINION CPLR 4547 (January 24, 1997); Illinois State Bar Assn., ADVISORY OPINION 96-10 (1996).
[82] 18 U.S.C. §§ 2701(a), 2792(a).
[83] City of Cleveland v. Cleveland Elec. Illuminating Co., 538 F. Supp. 1257 (N.D. Ohio 1980).
[84] Hart and Plum, *supra* n.62; s*ee also* Alldread v. City of Grenada, 988 F.2d 1425, 1433 (5th Cir., 1993), *see also* United States v. Keystone Sanitation Co., 885 F. Supp. 672, 674 (M.D. Pa. 1994), *cert. denied*, 516 U.S. 928 (1995).
[85] 67 F.R.D. 40 (S.D.N.Y. 1975).

26(c)(7), the court will look to see if disclosure will work a clearly defined and very serious injury to the defendant.[86]

5. Arguing Under the ABA Civil Discovery Standards and Manual for Complex Litigation, Third

Both the Manual for Complex Litigation 3rd, and the ABA's August 1999 Civil Discovery Standards, in comparison to the courts, are more balanced in approaching discovery of electronic files. They are rarely cited by the courts,[87] but the ABA standards in particular are still relatively new. They may prove useful in pre-trial negotiation, and some of the points raised may provide some help in argument.

a) Scope of Discovery Under ABA Civil Discovery Standards: "Substantial Need" Standard

ABA Civil Discovery Standards §29(a)(iii) provides that:

> [u]nless the requesting party can demonstrate a substantial need for it, a party does not ordinarily have the duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory.

The ABA Commentary argues further that:

> [j]ust as a party ordinarily has no duty to create documents, or to re-create or retrieve previously discarded ones, to respond to a document request, it should not have to go to the time and expense to resurrect or restore electronic information that was deleted in the ordinary course of business.

Clearly, both these statements go against the trend of most modern decisions. There also appears to be a slight logical fallacy in the commentary's argument: given the nature of resurrecting or restoring electronic data it is difficult to provide a persuasive analogy to recreating or retrieving previously destroyed paper documents. It is difficult to imagine a court

[86] *Id.*
[87] 1995 WL 360526 (N.D. Ill. 1995), *supra* n.18: CIBA cited the Manual for Complex Litigation, this is one of the few cases.

refusing to order production of paper documents merely because the requested party had written the word "delete" on the top of every page.

b) Scope of Discovery Under Manual for Complex Litigation, Third

Unlike the ABA standards, the Manual for Complex Litigation, third, limits itself to a call for increased specificity in discovery plans. Section 21.446 suggests that a discovery plan should address issues such as the search for, location, retrieval, form of production and inspection, preservation, and use at trial of electronically stored evidence.

c) Allocation of Costs Under ABA Civil Discovery Standards

ABA Civil Discovery Standards §29(b)(iii) provides that:

> The discovering party generally should bear any expenses incurred by the responding party in producing requested electronic information. The responding party should generally not have to incur undue burden or expense in producing electronic information, including the cost of acquiring or creating software needed to retrieve responsive electronic information for production to the other side.

In suggesting that the responding party should not be forced to bear the costs of producing electronic information, §29(b)(iii) is clearly at odds with most modern case law, including *Linnen*[88] and *In re Brand Name*.[89]

d) Allocation of Costs Under Manual for Complex Litigation, Third

The Manual for Complex Litigation § 21.433 interprets the Federal Rules of Civil Procedure 26(b)(2) and 26(c). By reading the rules together, it infers that the court has broad authority to control the cost of discovery. Under the Manual's interpretation, the court may require a discovering party to pay all or part of the cost of discovery as a condition of permitting

[88] *supra* n.70.
[89] *supra* n.86.

it to proceed. This gives the parties an incentive to use cost-effective means of obtaining information.

The Manual also suggests a number of factors that a court should consider in allocating the costs of production in electronic discovery cases:

1) What is the most efficient and economical way of obtaining the requested information?
2) Is the information of sufficient importance to warrant the expense of production?
3) Can one party obtain the information with less time and expense than other?
4) Should some or all of the costs be shifted between the parties?

D. Reducing Expenses

In *Sattar v. Motorola, Inc.*,[90] the Court of Appeals upheld the lower court's plan to provide e-mails in electronic, as opposed to hard copy, format. If the electronic production was not sufficient, the court was to allocate the costs of production of hard copies equally between both parties. Providing only an electronic version of the information can result in substantial reduction of discovery costs.

There are a number of ways of reducing costs through careful planning of the discovery process. Parties can eliminate excessive duplication of information. If files have the same name, the same "byte size" and have nearly identical time stamps, then they are probably the same file. There are also a number of ways in which to reduce the scope, and thereby the cost, of the search. The time frame of the search, the number of users or departments searched and the types of file searched, for instance a search of only user-created files, may all be narrowed. Careful planning of a detailed search term list can significantly reduce time and expense.

[90] 138 F.3d 1164 (7th Cir.(Ill.) 1998), *cert. denied*, 516 U.S. 928 (1995).

E. The Possibility of Sanctions or Expenses

1. Incomplete Compliance with Discovery Request

Generally, a hard copy response to a request for production is no longer sufficient, and, in certain circumstances, may lead to the imposition of sanctions. In *American Bankers Ins. Co. of Florida v. Caruth*,[91] the ABI argued that the information requested was stored in over 30,000 boxes in an out-of-state warehouse. A subsequent deposition of an information services representative revealed that the information could be obtained in just forty hours from ABI's sophisticated database. ABI eventually admitted failure to comply properly with the discovery requests and the court entered default judgment.

In another similar case,[92] evidence was produced that one party maintained a database that it had failed to produce in response to a request for production. Again, the trial court imposed sanctions that were tantamount to default judgment. The court rejected the contention that "written documents" referred only to printouts and not to magnetic media.

2. Spoliation

Spoliation of relevant electronic information is a major risk for modern technologically advanced organizations. Inadvertent spoliation, in particular, is easy in the electronic context. Even turning on a computer will often modify dates and times of files on the hard drive, without keyboard input. Spoliation of relevant data will inevitably lead to sanctions. "[S]anctions may be imposed against a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and destroys such documents and information."[93]

[91] 786 S.W.2d 427 (Tex. App.-Dallas 1990).
[92] 995 F.2d 1376 (7th Cir. 1993), *supra* n.9.
[93] National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 556 (N.D. Cal. 1987).

a) Pre-Discovery Duty to Preserve

Federal Rule of Civil Procedure 26(a)(1)(B) requires initial disclosure, even before a discovery request, of "all documents, data compilations, and tangible things in the possession, custody or control of the party that are relevant to disputed facts alleged with particularity in the pleadings." A responding party, therefore, must anticipate having to produce relevant documents very early in the dispute, and must take pains to preserve them.[94]

> While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant to the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is the subject of a pending discovery request.[95]

All parties have a duty, therefore, to save all data that may be requested in the future, even if they haven't received a request for production.[96] Even inadvertent destruction may lead to sanctions.

b) Inadvertent Spoliation

In *Linnen v. A. H. Robins Co.*,[97] a Massachusetts court held that inadvertent spoliation can have severe consequences for the requested party. The court initially granted an *ex parte* order requiring all computer records to be preserved at the time of filing. The plaintiffs subsequently learned that the defendant maintained backup systems, designed to recover lost data in event of a computer crash or catastrophic disaster. The defendant utilized a "widely-accepted business practice" of recycling tapes, which it continued after the court order resulting in the inadvertent destruction of information on the tapes. The court held that the spoliation was

---

[94] Pechette *supra* n.25.
[95] William T. Thompson Co. v. General Nutrition Corp., Inc., 593 F. Supp. 1443, 1455 (C.D. Cal. 1984) (*citations omitted*).
[96] *See* Capellupo v. FMC Corp., 126 F.R.D. 545, 551 (D. Minn. 1989), *but see,* Skeete v. McKinsey & Co., Inc., 1993 WL 256659 (S.D.N.Y. 1993).
[97] 10 Mass.L.Rptr. 189, 1999 WL 462015 (Mass. Super. 1999), *supra* n.70.

a 'clear violation' of the defendant's obligation to preserve evidence, and ordered that the defendant be made to bear the cost of restoring the tapes. The court also allowed an adverse inference instruction to be made at trial.

In *In re Prudential Insurance Co. Sale Practices Litigation*,[98] Prudential ordered employees to preserve information pursuant to a court order, but some information was still negligently destroyed due to a "haphazard and uncoordinated approach to document retention."[99] Consequently, the court fined Prudential $1 million and ordered the payment of plaintiff's attorney fees. The court then ordered Prudential to promulgate a formal, company-wide document retention policy.

As part of a valid document retention program, a party, when faced with pending litigation, should either take steps to preserve backup data or should seek permission to continue recycling in accordance with the existing technology plan.

3. Default Judgments

Although courts have been willing to impose sanctions in the event of inadvertent spoliation of electronic data, they are far more reluctant to find bad faith. The courts appear to be recognizing the complex nature of electronic discovery issues and, though they are keen to encourage careful management of electronic records, they have been willing to give parties the benefit of the doubt in most cases.

In *Proctor & Gamble Co. v. Haugen*,[100] the court could not determine on the record that Proctor and Gamble had acted in bad faith in destroying e-mails, but the company's failure to search for or preserve e-mails generated by five employees that Proctor and Gamble had identified as having relevant information was a sanctionable breach of their discovery duty

[98] 169 F.R.D. 598 (D.N.J., 1997), *rev'd on other grounds*, 133 F.3d 225 (3d Cir. (N.J.) 1998).
[99] *Id.* at 615.
[100] 179 F.R.D. 622 (D. Utah 1998).

to preserve relevant information. Proctor and Gamble was fined $10,000 per employee. In *In re Cheyenne Software, Inc. Securities Litigation*,[101] the defendant's destroyed documents stored in its desktop hard drives. The court refused to make a 'spoliation inference' as no prejudice to the plaintiff was shown. However, the court did fine the defendant $15,000.

Even absent a finding of bad faith, however, the court may award default judgment to a requesting party where the evidence destroyed was of a sufficiently important character.[102] In *Computer Assocs. Int'l, Inc. v. American Fundware, Inc.*,[103] the defendant's willful destruction of a computer program's source code rendered it impossible for the plaintiff to prove its claim that its own copyrighted program had been illegally copied by the defendant. The court entered a default judgment against the defendant.

In *Telectron, Inc. v. Overhead Door Corp.*,[104] the Florida court noted that "deeply rooted in the common law tradition is the power of any court to manage its affairs, 'which necessarily includes the authority to impose reasonable and appropriate sanctions upon errant lawyers practicing before it.'"[105] In particular, the court added, "courts have the inherent power to enter a default judgment as punishment for a defendant's destruction of documents."[106] The power to enforce a default judgment, therefore, can be found both within the Federal Rules of Civil Procedure and within the court's inherent powers.

4. How to Avoid Sanctions

A number of steps may be taken to ensure full compliance with a request for production, thereby avoiding sanctions and at the same time preserving privileged or sensitive information. Steps should be taken early on to assess client systems for possible relevance to

[101] 1997 WL 714891 (E.D.N.Y. 1997).
[102] *See* 995 F.2d 1376 (7th Cir. 1993), *supra* n.9, *and* 138 F.3d 1164 (7th Cir. 1998), *supra* n.90.
[103] 133 F.R.D. 166 (D.C. Cir. 1990).
[104] 116 F.R.D. 107 (S.D. Fla. 1987) (*citations omitted*).
[105] *Id.* at 126.
[106] *Id* at 126.

litigation. Attorneys should ensure preservation of evidence early, then collect client data responsive to discovery requests. Once collected, review the data for privilege, responsiveness and confidential information then prepare redacted sets of privileged information for production.

F. Preventing Use at Trial: the Hearsay Exception

Once produced, electronic documents, particularly e-mail, are often objected to on grounds of hearsay. Unfortunately, there are a number of ways in which a hearsay objection may be circumvented when considering electronic data.

The easiest way around the hearsay objection is to claim that the information produced, particularly e-mails, represent communications made and retained in the ordinary course of business, under the Federal Rules of Evidence 803(6). Printouts of general ledger are admissible as business records. "Fed. R. Evid 803(6), the business records exception, specifically allows for the admission of a 'data compilation, in any form,' which meet the requirements of the rule."[107] One 9th circuit case has held that, to the contrary, e-mail does not fit the business records exception. The court noted that ongoing electronic message and retrieval systems are far less of a systemic business activity than are record keeping printouts.[108] The case was decided in 1994, however, and came before the e-mail and internet revolution had really taken hold.

The business records exception has been broadly interpreted by the courts to include most electronic information. Where each point of data in an electronic source is made in the regular course of business, then the output from a computer is not hearsay even if it (a) was not printed out at, or near, the time of the events recorded, (b) was not prepared in the ordinary course of business (but, for example, for trial), and (c) is not in the usual form[109]

[107] United States v. Catabran, 836 F.2d 453 (9th Cir.(Cal.) 1988).
[108] Monotype Corp., P.L.C. v. Int'l Typeface Corp., 43 F.3d 443 (9th Cir.(Wash.) 1994).
[109] United State v. Russo, 480 F.2d 1228, 1240 (6th Cir.(Mich) 1973), *cert. denied,* 414 U.S. 1157 (1974).

Other possible arguments are that the documents represent admissions, present sense impressions, or declarations against interest, admissible under Rule 803(1), or public records, admissible under Rule 803(8). An attorney should also be aware that if an employee is typing something that he or she has been told then this may constitute hearsay within hearsay under Rule 805. Finally, even where no hearsay exception is applicable, then relevant data may still be admissible if the documents can be used as evidence that a communication was made.

V. CONCLUSION

Electronic evidence has become so pervasive in modern society, that to ignore its existence in any litigation context could prove disastrous. Even organizations that believe they have addressed the issue of electronic evidence can fall foul to embarrassing discovery through misapplication of records retention policies, or poor employee education. For the modern organization, it is essential to implement a valid records retention policy, and take steps to apply the policy to all usage of electronic data. For the modern lawyer, it is essential to seek electronic discovery as early and as often as possible. The use of electronic discovery in litigation is fast becoming the norm, not the exception.