DISCOVERY OF ELECTRONIC DATA

James P. Cullen, Jr., Esq.
COZEN O'CONNOR
1900 Market Street
Philadelphia, PA 19103
(800) 523-2900
(215) 665-2000
jcullen@cozen.com

Atlanta
Charlotte
Cherry Hill
Chicago
Dallas
Las Vegas
Los Angeles
London
New York
Newark
San Diego
San Francisco
Seattle
Washington, D.C.
West Conshohocken
Wichita
Wilmington

These seminar materials are intended to raise questions concerning current issues in the law. They 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.

DISCOVERY OF ELECTRONIC DATA

By James P. Cullen, Jr.

I. INTRODUCTION

Twenty five years ago, computers were used as oversized calculators, to quickly perform complex mathematical analysis, and as glorified filing cabinets, given their ability to store vast amounts of data. Over time, the business world's use of and reliance upon computers has dramatically increased.

Today, computers are used in almost all record analysis and retention, word-processing, and communication functions. Computers also serve as mail carriers, with the use of electronic mail and the Internet. Some companies even have moved to "paperless" offices, thereby entrusting all document creation and record retention to computer technology.

Given the ever-expanding reliance upon computer technology, parties have begun to recognize the value of seeking discovery of computerized or electronic data.[1] While the parameters of permissible discovery and the responsibility for the costs that result from discovery requests for electronic data still are being defined, "today it is black letter law that computerized data is discoverable." Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y.).

Accordingly, parties must recognize both the extent of information that may be discovered through electronic data requests and the potential issues created by requests for their electronic data. This paper will discuss the discoverability of electronic data, the unique issues created by discovery of electronic data, including the "spoliation" of computer records, and the special concerns that arise from the use of e-mail.

II. ELECTRONIC DATA IS DISCOVERABLE

Federal Rule of Civil Procedure 34 allows a party to serve a request for production of designated "documents." The commentary to Rule 34 states that the term "document" was intended to evolve with changing technology. The commentary allows that hard copies of computer records and even the "electronic source itself" may be discovered.

Given the expansive definition of the term "document" under the federal rules, electronic data is subject to discovery. Indeed, any question concerning whether the term "document" encompassed electronic data was laid to rest by the Seventh Circuit Court of Appeal's decision

---

[1] Electronic data exists in many forms, including computer files, hard drives, and backup tapes.

in Crown Life Ins. Co. v. Craig, in which the court expressly rejected an insurer's attempt to characterize electronic data as outside the definition of a document for purposes of the discovery rules. 995 F.2d 1376 (1993); See also Linnen v. A. H. Robins Co., 1999 WL 462015 (Mass. Super.).

Accordingly, there is no question that parties may obtain electronic data through discovery. In fact, parties have sought to compel their adversaries to create computer applications to facilitate discovery requests. Although Federal Rule 34 speaks of producing documents that are already in existence, courts nonetheless have required parties to create computer applications, so that their adversaries may effectively access and utilize their electronic data. National Union Electric Corp. v. Matsushita Elect. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980); See also Orlowski v. Dominick's Finer Foods, Inc., 1995 WL 516595 (N.D. Ill); In Re Air Crash Disaster, 130 F.R.D. 634 (E.D. Mich. 1989). In addition, courts also have granted parties access to or copies of their adversary's entire hard drive. Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); Gates Rubber Co. v. Bando Chemical Industries Ltd., 167 F.R.D. 90 (D. Colo. 1996).

Although electronic data is discoverable, requests for such information are subject to the same controls and limitations as any other discovery request. Parties may seek protection from unreasonable discovery requests under Federal Rule 26. Courts will not allow discovery requests for electronic data to circumvent the protections afforded to privileged materials, nor will they require parties to respond to requests that are not reasonably calculated to lead to the discovery of admissible evidence. Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); See also, Shipes v. Bic Corp., 154 F.R.D. 301 (M.D. Ga. 1994).

III. UNIQUE ISSUES RAISED BY DISCOVERY OF ELECTRONIC DATA

A. Production of "Hard Copies" May Not Fully Discharge Discovery Obligations.

As most important decisions are memorialized in writing, parties typically have sought discovery of documents, in order to establish paper trails and uncover admissions. Parties obtain documentary evidence by propounding Requests for Production, which require the responding party to produce designated materials. In the past, parties generally were satisfied if they received hard copies of what they understood to be all properly responsive information.

Given the widespread use of word-processing applications, very few documents are now handwritten or manually typed. Instead, most documents are generated through the use of computer based word processing programs. The expanded use of computers to generate documents has created new forms of evidence and opened new discovery avenues.

During the creation of electronic files, pieces of the documents may be written to or stored in temporary files, swap files, and/or in file slack. When documents are revised or modified on a word processing program, the remnants of the original version often remain on the hard drive. As a result, through the discovery of electronic data, parties can locate initial drafts, which may not exist in a "hard copy" form, and also determine when and by whom a document

was revised. Fennell v. First Step Designs, Ltd. 83 F.3d 526 (1st Cir. 1996)(electronic discovery reveals dates on which document was revised).

It also should be noted that the delete function of a computer does not always destroy the document. Instead, the delete function moves the document to an undisclosed location on the hard drive. In addition, many companies routinely back-up their systems, including the deleted materials. Therefore, a file may remain on the computer system even after the user has deleted the document from the word processing application. Consequently, discovery of electronic data can result in the disclosure of items that the user may believe were destroyed and unavailable to be produced in litigation. Lexis-Nexis v. Beer, 41 F. Supp. 2d 950 (D. Minn. 1999)(electronic discovery reveals documents that were deleted by a party).

As parties recognize the additional information that is available from a computer system, they no longer are satisfied with merely obtaining the "hard-copy" of the final version of a document. Instead, parties are seeking both the hard copy and the underlying electronic data. Because certain information may only be discovered by review of the electronic data, courts have refused to accept the position that production of hard copies completely discharges a party's discovery obligations. Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934 (S.D.N.Y.); See also National Union Electric Corp. v. Matsushita Elect. Indus Co., 494 F. Supp. 1257 (E.D. Pa. 1980).

Parties must now be sensitive to the need to preserve both a hard copy and the electronic data. In addition, when the electronic data is produced, parties must be aware that prior edits or modifications to a document and deleted documents may be discovered.

Fennell v. First Step Design, Ltd. represents an example of the additional information that can be gathered through requests for electronic data. 83 F.3d 526 (1st Cir. 1996). In Fennell, an employee brought an action alleging that she was discharged in retaliation for filing a sexual harassment complaint. The company defended upon the grounds that the termination was not retaliatory, because it was planned prior to the report of harassment. In support of its position, the company produced a memo regarding the anticipated termination, which pre-dated the harassment complaint.

The discharged employee refused to simply accept the hard copy of the memorandum. The employee sought and obtained discovery of the underlying electronic data. By the use of forensic computer experts, the employee determined the document had been revised on several occasions. Unfortunately for the employee, all of the revisions pre-dated her complaint. While the employee's effort was ultimately not fruitful, the case demonstrates the lengths to which parties will go in seeking computerized data and the ability to determine when documents were revised or altered.

B. When Responding to Discovery Requests, Electronic Data Should Be Considered.

When a discovery request is received, the attorney and client typically consult regarding available responsive information. As set forth above, the responsive information can include more than the available hard copies of records. In order to fully explore the available responsive information, parties must be aware of the information that is available on their computer systems.

The failure to consider electronic data in formulating a response can result in miscommunications and may lead to discovery sanctions. By way of illustration, in American Bankers Ins. Co. of Florida v. Caruth, the defendant served document requests upon an insurer. 786 S.W.2d 427 (Tx. Ct. App. 1990). The insurer responded that the information requested was contained in excess of 30,000 boxes, which were located in an out-of-state warehouse. The insurer took the position that the only way to access the information was to manually inspect each of the files in its warehouse.

In response, defendant deposed a representative of the insurance carrier's information services department. Through the deposition, defendant learned that the insurer maintained a sophisticated database and its computer system could generate the requested information in approximately forty hours. During the resulting motion practice, American Bankers was forced to concede that it had not properly complied with the discovery requests. American Bankers was ultimately sanctioned for its conduct.

In order to avoid such circumstances, parties should consider the viability of utilizing their own information services department when served with valid discovery requests. Parties also must be prepared for depositions of their information services personnel, by lawyers who are assisted by forensic computer experts. Simply stating that documents are not readily available, without considering electronic data, may no longer be sufficient.

C. Significant Expenses Can Result From Requests For Electronic Data.

Electronic data allows parties to store significant amounts of information. However, producing the materials can be burdensome and costly. Parties often object to discovery requests for electronic data, due to the cost inherent in responding to such requests. Indeed, some have characterized electronic data requests as a form of blackmail, designed to induce settlement by forcing parties to incur substantial expenses to litigate a case. Discovery disputes involving requests for electronic data, which involve six figure expenses, are become increasingly common.

The Federal Rules provide parties with a mechanism by which to seek relief from onerous and unreasonable discovery requests. However, the fact that production of the data results in substantial expense does not, in and of itself, create an adequate basis for imposing the cost of production on the requesting party. In Re Brand Name Prescription Drugs, 1995 WL 360526 (N.D. Ill.).

In determining who should bear the cost inherent in producing electronic data, some courts have viewed the costs as a necessary and foreseeable business expense, which a party assumes the risk of when it decides to utilize electronic data. In Re Brand Name Prescription Drugs, 1995 WL 360526 (N.D. Ill.); See also Linnen v. A.H. Robins Co., 1999 WL 462015 (Mass. Super.). Under this rational, courts allocate the cost of production to the producing party, as reliance on technology should not create a shield or become a hindrance to the discovery of information. Baine v. General Motors Corp. 141 F.R.D. 328 (M.D. Ala. 1991).

In contrast to this bright line test, other courts seek to balance the equities of the situation. Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); see also, McPeek v. Ashcroft, 202 F.R.D. 31, 33 (D.D.C. 2001). Most recently, in Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002), a court utilized a "balancing approach", based upon eight factors. The Rowe factors are: (1) the specificity of the discovery requests; 2) the likelihood of discovering critical information; 3) the availability of such information from other sources, including production in alternate formats; 4) the purpose for which the responding party maintains the requested data; 5) the relative benefit to the parties of obtaining the information; 6) the total cost associated with production; 7) the relative ability of each party to control costs and its incentive to do so; and 8) the resources available to each party. 205 F.R.D. at 429-30; see also, Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 2002 W.L. 246439 (E.D.La).

Given such cases, parties must be sensitive to requests for electronic data and develop systems to efficiently manage such requests. In fact, most major corporations already have begun preparing for the issues created by the discovery of electronic data by instituting technology plans and electronic data policies. New York Law Journal, January 25, 1999, *Preparing for Electronic Discovery*.

D. Spoliation of Electronic Data.

As electronic data is discoverable, parties must take steps to ensure they do not inadvertently destroy or spoliate electronic data. Due to the means by which electronic data can be compromised, parties may inadvertently destroy or alter evidence and thereby expose themselves to the risk of sanctions. As is demonstrated by the recent Massachusetts Superior Court decision in Linnen v. A. H. Robins Co., even the inadvertent spoliation of electronic data can have severe consequences.

In Linnen, plaintiffs moved for an *ex parte* order requiring all computer records to be preserved at the time of filing their complaint. After defendant had answered, plaintiffs filed a request for discovery and the court lifted its order. During discovery, plaintiffs noticed the deposition of an information services person concerning the utilization and storage of electronic mail software.

Plaintiffs learned that defendant maintained backup systems, which were designed to recover lost data in the event of a computer crash or a catastrophic disaster. The backup system recorded all of the company's electronic data systems, including word processing files, spread sheets, models, and electronic mail. Defendant utilized what the court characterized as a "widely-accepted business practice" of recycling the backup tapes.

Despite the order and request for production, defendant did not begin removing the backup tapes from its normal recycling process until three months after the document request was received. Plaintiffs sought the restoration of the tapes and spoliation sanctions. Plaintiffs argued that spoliation sanctions were appropriate because the backup tapes could yield discovery of communications and documents that were deleted from the computer system and only available via the backup tapes. Defendant asserted that hard copies had been produced and plaintiffs' request represented a multi-million dollar fishing expedition, which was completely unwarranted.

Although the court recognized the recycling of the tapes was customary, given the pending discovery requests, the court held the recycling of the backup tapes constituted a "clear violation" of a party's obligation to preserve evidence. Defendant was made to bear the cost of restoring the tapes. The court also allowed an adverse inference instruction at trial concerning the destruction of the backup tapes.

By way of further example, in a particularly contentious patent infringement suit, Applied Telematic moved for spoliation sanctions against Sprint Communications, based upon their routine computer back-up procedures. No. Civ. A. 94-CV-4603 (E.D. Pa). After a request for production had been served, Sprint continued its weekly back-up practice, which resulted in the prior week's back-up data being overwritten. Applied alleged the back-up procedure resulted in the spoliation of electronic data. The Court agreed and found that Sprint should have altered its back-up procedures after receiving the document request.

Based upon Sprint's failure to alter its back-up procedure and preserve the data, the court imposed sanctions. Although the Sprint order was ultimately vacated as part of a settlement agreement, the warning concerning the need to preserve all forms of evidence remains. Parties must be aware of the steps that should be taken to preserve electronic data or obtain permission to delete the data in accordance with their existing technology plan. See Smith v. Texaco, Inc., 951 F. Supp. 109 (E.D. Tex. 1997) (allowing a party to delete its electronic data, in keeping with its existing business practice, in order to avoid the "high costs associated with electronic document storage").

IV. THE DISCOVERY OF E-MAIL

The New York Court of Appeals described e-mail as today's "evolutionary hybrid of traditional telephone lines communications and regular postal service mail." Lunney v. Prodigy Services, Co., 1999 WL 1082126 (NY). E-mail allows people to quickly transmit and/or receive informal electronic messages. E-mail increasingly has become a substitute for telephone conversations, meetings, and the exchange of correspondence. Indeed, in 2001, North American businesses e-mail generated over 2.5 trillion e-mail messages. Trial, January 2003*, Digging for e-data*.

Not suprisingly, most e-mail users view communicating by e-mail differently than the transmittal of paper documents. In fact, based upon recent surveys, only fifteen percent of e-mail users treat it the same way as paper documents. Business Week - June 8, 1998, *Office E-mail: It Can Zap You -- In Court*.

E-mail represents a distinct form of communication for several reasons. E-mail is typically created by the author typing at his or her own terminal. As a result, content and grammar, which would not be used in or survive the dictation and proof reading process, are commonly found in e-mail. E-mail also is not signed by the author, which results in many messages being sent prior to any review. Many people, who closely review any document they sign, quickly hit the send button without a second thought. As a result, e-mail often contains comments or messages that one would not typically memorialize in written correspondence.[2]

Moreover, the majority of users believe that e-mail can effectively be deleted. However, as with any other information that is on a hard drive, e-mail messages can remain indefinitely on a computer system. E-mail messages may be found on both the sender's and recipient's computer systems, which creates two means by which to discover the communication. E-mail also may exist on back-up tapes. Therefore, one should never assume the deletion of an e-mail means that it cannot be obtained at a later date, through a request for electronic discovery.

Many e-mail users mistakenly believe e-mail is private. However, courts have ruled that no reasonable expectation of privacy exists in e-mail transmitted over an employer's computer system. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa 1996); further, no independent privilege exists for e-mail communications. Indeed, e-mail is routinely discoverable, assuming it is not otherwise privileged. Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999); See also In Re Brand Name Prescription Drugs, 1995 WL 360526 (N.D. Ill.).

---

[2] In CFO: The Magazine for Senior Financial Executives, John Jensen, President of Electronic Evidence Discovery, Inc., offers examples of e-mails, that contain information which would not commonly be expected to be memorialized in writing, including: (1) "Yes, I know we shipped 100 barrels of [deleted], but on our end, steps have been taken to insure that no record exists. Therefore, it doesn't exist. I know you know what I mean. Remember, you owe me a game of golf next time I'm in town"; (2) "Did you see what Dr. [deleted] did today? If the patient survives it will be a miracle"; and (3) "Hi David, please destroy the evidence on the [litigation] you and I talked about today. Thx. Laura."

Accordingly, E-mail users must recognize that the messages are not private off-the-record communications but, rather, discoverable evidence which parties actively seek to obtain.

Playboy Enterprises, Inc. v. Welles illustrates the lengths to which parties will go in order to obtain discovery of their adversary's e-mail. 60 F. Supp. 2d 1050 (S.D. Cal. 1999). In this infringement case, defendant did not produce hardcopies or electronic copies of her e-mail communications. Even after a discovery request was served, defendant continued her "custom and practice" of deleting e-mail from her computer's "mailbox" and "trash bin," after it had been read or sent.

In the course of discovery, plaintiff received copies of e-mail generated by the defendant. As defendant asserted hard copies of the e-mail could not be produced, plaintiff sought an order compelling defendant to produce a "mirror image" of her hard drive, because it could lead to the discovery of the deleted e-mail communications. Defendant contended the request was improper as it would reveal privileged information, invade her privacy, and result in undue expense, since the creation of the mirror image of her hard drive would require her business to close for greater than four hours.

As defendant's action made the production of e-mail in a hardcopy form impossible, the Court ruled that a mirror image of the hard drive should be produced. However, in order to avoid disclosure of privileged attorney-client communications and/or an undue invasion of defendant's privacy, the Court did not allow plaintiff's expert to create the mirror image. Instead, the Court appointed a computer expert, as an officer of the Court, to retrieve whatever e-mail files were available. The Court directed the retrieval of the electronic data occur in the presence of defendant's counsel, who could review the materials obtained for purposes of asserting privilege or other objections. Although plaintiff was required to bear the expense of the expert's time, defendant was not compensated to her loss of business.

A number of clients utilize e-mail to provide Cozen O'Connor with early notification and/or adjustment reports. When used in this manner, e-mail is protected by the attorney-client privilege. However, the e-mail that is routinely exchanged between field adjuster and home office personnel, brokers, insureds, and/or experts may be discoverable. E-mail users must recognize their messages may one day be read to a jury, even if they have deleted the message.

V. CONCLUSION

Our increased reliance upon computer technology has created new avenues for discovery and new obligations in responding to discovery requests. As the applicable rules and case law provide that electronic data is discoverable, parties must recognize that retention of hard copies alone may be insufficient. Parties must prepare themselves to effectively utilize and respond to requests for electronic data. While use of electronic data does not compromise any of the existing privileges, electronic data requests can result in discovery of information that was previously thought not to be available, such as drafts that were discarded, and deleted items. Consultation with legal counsel is appropriate to design, implement and maintain an information services policy that is consistent with applicable legal obligations.