

The Pitfalls of Electronic Discovery: What You Don't Know Can Hurt You

Christopher C. Ross, Esq.¹

Computers are everywhere - they are in our homes, in our cars and in our law offices. The business community has long been moving toward the fabled paperless society, but while industry continues to generate volumes of paper – paper now represents the outcome of a digital process that includes magnetic media, routers, meta-data, e-mail, cyberspace and more.² Too few lawyers, unfortunately, take the time to keep abreast of the latest trends and tools of the digital frontier. Attorneys who could once marginalize this “digital divide” must now face the effects of recent amendments to the Federal Rules of Civil Procedure that extend discovery to include electronic forms of data.³ Failing to understand the subtle nuances of electronic discovery can be detrimental to the unwary attorney.

The Expanding Scope of Discovery

Electronic discovery is a category of information gathering made possible by amendments to the Federal Rules of Civil Procedure in 1983, 1993 and 2000.⁴ The Federal Rules, as amended, force attorneys to discuss and implement the most efficient and economical means of conducting discovery while investing judges with the authority to see that discovery is conducted fairly and openly. Mandatory initial disclosure, perhaps the most dramatic change to the Federal Rules, compels disclosure whether or not the opposing party has requested the materials in question. Parties may obtain materials regarding any matter that is relevant to the claim or defense of any party to the action. Attorneys who file discovery requests must work both with the judge and with opposing counsel to establish realistic discovery goals and an

implementation plan. Failure to comply with these discovery obligations, whether by accident or design, may result in harsh sanctions.⁵

When a Document Is Not a Document - Formulating Electronic Discovery Requests

Electronic discovery involves a multi-step analysis for both the attorney requesting discovery and for the attorney who must respond. At the onset of litigation attorneys of both parties should consult with those specialists who understand the scope and types of electronic data maintained by either party.⁶ Decisions made at this stage will influence the success of future discovery.

Computer files are often searched by use of dates and key words allowing an attorney to tailor a discovery request that focuses on records that contain key words and phrases pertaining to specified individuals or subjects created during a fixed period of time.⁷ When forming a discovery strategy it is important to understand the types of electronic data that typically exist in a computer system.⁸ The four most important types of data to be aware of for these purposes are: active data, replicant data, residual data and meta-data.⁹

“Active data” is data that is current and readily accessible from the computers of the key actors in a case (i.e., managers, employees, etc.). This data is found in the typical locations that one would expect to find electronic data such as e-mail messages, word processing files and database records.¹⁰ Active data, consequently, is the easiest type of data to retrieve.

“Replicant data” is data that exists as digital archives and automatic backups routinely performed while users create, edit or modify electronic documents. Replicant data will often consist of file fragments or multiple and time-lapsed versions of computer files.¹¹ The importance of this type of data lies in the

ability to demonstrate the thought process that went into the development of the document from first draft to finalization.

“Residual data” is data that has been deleted or otherwise purged from a computer. A computer file does not disappear upon the pressing of the delete command key. The action of deleting a file merely allows the computer to write over the physical space that a particular file occupies. A computer expert can reconstruct the file to its original integrity until new data are written over the space containing the deleted file. An attorney attempting to retrieve residual data should hire specialists, such as data recovery experts, to perform this task.¹²

“Meta-data” is data that is automatically added to electronic documents to facilitate greater accessibility within computer systems. Examples of meta-data include information about when a document was created, modified, copied or deleted; the path that an e-mail traveled as it moved between computers to reach its destination; and the list of websites or files that an employee may have accessed during work hours. Meta-data is often invisible and may not be included in hard copy versions of electronic documents unless specifically requested.¹³ Examination of meta-data can uncover tampering and spoliation by revealing when a document has been accessed and by whom.¹⁴ Absence of certain meta-data can demonstrate that a party has deleted files, logs or other data that should exist in the normal course of operating a computer system.

The Costs of Electronic Discovery

The Federal Rules of Civil Procedure encourage judges to apply a proportionality analysis to limit discovery abuse, redundancies and overall litigation costs. Judges often participate in pretrial discovery planning conferences to minimize the costs and burden of discovery.¹⁵ As discovery costs continue to

escalate, judges must face the challenge of deciding not just the scope of discovery but also how to allocate the costs and burdens of extensive electronic discovery requests.¹⁶ Judges have begun to employ creative measures such as appointing neutral computer experts to carry out court ordered discovery protocols and dividing discovery costs between the several parties to a suit.¹⁷

Companies retain more information than ever before now that volumes of documents can be recorded on electronic media. A single eight-millimeter computer backup tape can store more than 1,500 boxes of paper documents. Sorting through these piles of tapes and computer logs can be time consuming and costly. Requesting documents in electronic form rather than in the traditional paper form reduces these costs significantly. Such requests carry additional benefits in that parties can produce 500,000 pages of e-mail, network logs and word processing files much easier in electronic form than by the truckload in paper form. Parties can also search electronic media through the use of keywords in ways that would be impossible with traditional discovery methods.¹⁸

Electronic mail (e-mail) is one of the most popular forms of communication in the business world. E-mail is the technological equivalent of first class mail in that e-mail may contain messages, notes and other attached files transmitted with the message. E-mail potentially represents a rich source for electronic discovery because users of e-mail tend to communicate informally and candidly, thus allowing an injection of personal motivations and opinions that can serve as the proverbial “smoking gun” in a case based largely on circumstantial evidence.¹⁹

A crucial step to commencing electronic discovery is the preservation of relevant data. Many operators of computer networks have established data retention policies to routinely purge archival data and backup logs on a scheduled basis. In addition to requesting a copy of an opposing party’s retention

policy, counsel should request that relevant information be preserved and secured for possible discovery.²⁰ Attorneys should not rely on the opposing party to discern what data to preserve and protect from periodic purging but rather should identify word processing documents, databases, spreadsheets, e-mail, voicemail, system records and logs, downloaded disk copies of files, Internet usage logs and any other data or systems that may contain information relevant to pending litigation and discovery requests.

Courts are increasingly directing attorneys to conduct on-site inspection of documents to reduce the burden on the opposing party to produce voluminous archives of data. In the realm of electronic discovery attorneys should employ computer specialists or should request court appointment of specialists to direct data retrieval efforts. Experts can safeguard against damage to the information sought and can protect the trade secrets and confidential data of the party granting access to sensitive electronic systems.²¹

Enough Is Enough - How to Reply to Electronic Discovery Requests

A party responding to an electronic discovery request has the same defenses as those applicable to traditional discovery. A reasonable discovery request must be relevant and must not place an undue burden or expense on the producing party. Discovery may not apply to matters protected by the privileges of confidential attorney-client discussions or attorney work product. Responding parties should seek protective orders to protect trade secrets and other confidential materials. Confidential data may be difficult to protect if the client has a poorly managed computer system. Attorneys, therefore, must advise their clients about the perils of electronic discovery. Clients who maintain computer systems should establish uniform protocols governing the use and functions of each system including how to respond to litigation and discovery requests. Clients should implement electronic data retention policies to allow for the systematic review, retention and destruction of documents received or created in the course of business. As part of

this review the client should categorize and keep separate official business records, routine business records, privileged material and trade secrets. Clients who have workplace e-mail and Internet capabilities should also devise and implement employee usage policies. The establishment of clear policies governing the use of company computers and resources can aid clients in the task of monitoring the conduct of subordinates and can place clients in a better position to respond to discovery requests.

Clients risk inadvertently waiving privileges through accidental disclosure unless confidential and privileged matters are treated separately and with greater care than routine business activities. The first step to address confidentiality and privilege in communications is to treat e-mail correspondence with the same care afforded to letter, fax and telephone correspondence. Confidential e-mail correspondence should be labeled as such and should include additional labels or disclaimers as are necessary.²² Similarly, data and correspondence lacking privileged status should not be labeled or treated as such, thus establishing a clear line between what is subject to discovery and what must be protected from discovery.²³ Security measures such as digital encryption, firewall protection and the abstention from transmitting sensitive data across wireless networks will help to ensure that privileged communications and stored data remain confidential and protected.

Correspondence by e-mail creates additional considerations as ethical rules prohibit disclosure of privileged client information by an attorney. The American Bar Association formally recognizes e-mail as confidential correspondence so long as the attorney and client possess a reasonable expectation of privacy.²⁴ The ABA recommends that attorneys consider additional security measures, discuss the use of e-mail with clients and refrain from transmitting highly sensitive information via e-mail. Many state bars have issued opinions similar to that of the ABA.²⁵

Covering Your Bases - Other Considerations

Many other technology issues exist that may merit consideration depending on the circumstances of a particular case. Once litigation moves beyond discovery and into the actual courtroom a myriad of evidentiary problems potentially arises.²⁶ Where the federal government is a party to litigation, opposing parties may use the Freedom of Information Act to obtain records in electronic rather than traditional formats. Parties may encounter privacy issues where litigation involves employer monitoring of employee e-mail and Internet use, particularly when the employer has not established a clear policy regulating employee use of company resources. The Electronic Communications Privacy Act often applies in cases involving eavesdropping or wiretapping. In cases involving contract disputes or identity issues the Uniform Electronic Transactions Act may be persuasive authority. The Computer Fraud and Abuse Act may apply in cases where rouge employees or hackers break into client computer systems. Lastly, an expanding sphere of intellectual property laws, including the Anticybersquatting Consumer Protection Act, apply to protect client websites and the data maintained therein from cyberpiracy and infringement.

In conclusion, the digital age has expanded the scope and realm of the business community. New advances in technology continue to pervade the modern workplace faster than lawmakers can promulgate new laws to address the ever expanding sphere of cyberspace law. As electronic discovery continues to grow and develop more attorneys will face technological challenges. Clients want the benefits of cyberspace and expect their attorneys to keep them clear of the perils and pitfalls of poorly conceived business rules and computer policies that can lead to costly litigation. Electronic discovery has become more than a distant possibility – it has set a new standard for competent legal practice.

Bibliography

Armen Artinyan, Comment, *Legal Impediments to Discovery and Destruction of E-mail*, 2 J. Legal Advoc. & Prac. 95 (2000)

Nicholas A. Barone, *Computer Discovery*, SG007 ALI-ABA 539 (July 12-13, 2001)

John L. Carroll, *Discovery Disputes and Electronic Media*, SG045 ALI-ABA 421 (August 23-24, 2001)

Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 Wash. & Lee L. Rev. 257 (winter, 2000)

Jay E. Grenig, *Electronic Discover: Making Your Opponent's Computer a Vital Part of Your Legal Team*, 21 Am. J. Trial Advoc. 293 (Fall 1997)

Brett R. Harris, *Counseling Clients Over the Internet*, 18 No. 8 Computer & Internet Law 4 (August, 2001)

Jacob P. Hart & Anne Marie Plum, *Litigating The Production of Electronic Media: "Disk-covery" Issues for the 21st Century*, SG007 ALI-ABA 169 (July 12-13, 2001)

Debra S. Katz & Alan R. Kabat, *Electronic Discovery in Employment Discrimination Cases: As Employers Step More Boldly into the Computer Age, Plaintiff Lawyers must Embolden Themselves to Conduct More Sophisticated Discovery*, 34-DEC Trial 28 (December, 1998)

Carey Sirota Meyer & Kari L. Wraspir, *E-Discovery: Preparing Clients For (And Protecting Them Against) Discovery in the Electronic Information Age*, 26 Wm. Mitchell L. Rev. 939 (2000).

Christopher C. Miller, Note, *For Your Eyes Only? The Real Consequences of Unencrypted E-mail in Attorney-Client Communication*, 80 B.U.L. Rev. 613 (April, 2000)

Frank C. Morris, Jr., *The Electronic Platform and Employer Privacy and Other Risk Management Concerns in the New Millennium*, SG016 ALI-ABA 1197 (July 26-28, 2001)

Christopher D. Payne, *Discovery of Electronic Evidence*, 1 Ann.2001 ATLA-CLE 441 (July, 2001)

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

Endnotes

1. Christopher C. Ross is a staff attorney with the Fair Housing Law Clinic associated with the Cleveland-Marshall College of Law at Cleveland State University. Christopher is also employed with The Housing Advocates, Inc. and is an associate attorney with Kramer & Associates, LPA in Cleveland, Ohio. The author wishes to thank Jonathan D. Byrne, Jeffery Dillman, Tamara Stanford, Agnes Stucke and Tom Deep for editorial assistance. The author would like to extend special thanks to Edward G. Kramer for providing the opportunity to make this article a reality.

2. This article endeavors to explain few of the technical terms that are peppered throughout. Those who have only a faint idea of how computer networks or Internet connections function should consult some supplemental reading. See ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa 1996), aff'd 521 U.S. 844 (1997) (this District Court decision regarding the 1996 Communications Decency Act provides a thorough fact finding regarding the development, nature and use of e-mail and the Internet.). See also Nicholas A. Barone, *Computer Discovery*, SG007 ALI-ABA 539 (July 12-13, 2001); Christopher C. Miller, Note, *For Your Eyes Only? The Real Consequences of Unencrypted E-mail in Attorney-Client Communication*, 80 B.U.L. Rev. 613 (April, 2000); and Frank C. Morris, Jr., *The Electronic Platform and Employer Privacy and Other Risk Management Concerns in the New Millennium*, SG016 ALI-ABA 1197 (July 26-28, 2001).

3. An example of an interrogatory definition of "electronic data" follows:

When used in this request, the term "electronic data" means the original (or identical duplicate when the original is not available), and any non-identical copies (whether non-identical because of notes made on copies or attached comments, annotations, marks, transmission notations, or highlighting of any kind) of writings of every kind and description whether inscribed by mechanical, facsimile, electronic, magnetic, digital, or other means. Electronic data includes by way of example only, computer programs (whether private, commercial or work-in-progress), programming notes or instructions, activity listings of electronic mail receipts and/or transmittals, output resulting from the use of any software program, including word processing documents, spreadsheets, database files, charts, graphs and outlines, electronic mail, operating systems, source code of all types, peripheral drivers, PIF files, batch files, ASCII files, and any and all miscellaneous files and/or file fragments, regardless of the media on which they reside and regardless of whether said electronic data consists in any active file, deleted file or file fragment. Electronic data includes any and all items stored on computer memories, hard disks, floppy disks, CD-ROMs, removable media such as Bernoulli Boxes and their equivalent, magnetic tapes of all types, microfiche, punched cards, punched tape, computer chips, including, but not limited to EPROM, PROM, RAM and ROM, on or in any other vehicle for digital data storage and/or transmittal. The term electronic data also includes the file, folder tabs and/or containers and labels appended to, or associated with, any physical storage device associated with each original and/or copy.

Barone, *supra* note 2.

4. See John L. Carroll, *Discovery Disputes and Electronic Media*, SG045 ALI-ABA 421 (August 23-24, 2001) (this article explains in detail the various Federal Rules changes affecting electronic discovery).

5. In Linnen v. A. H. Robins Co., 10 Mass. L. Rptr. 189 (Mass. Super. 1999) the plaintiff requested e-mail records and backup tapes from the defendant. Based on consultation with the client, counsel reported that defendant did not maintain e-mail messages for that time period. Months later defendant revealed that it did, in fact, have thousands of backup tapes. In imposing sanctions the court ordered that defendant must restore and produce the tapes at a cost of \$120,000. The court, additionally, compelled the defendant to pay the costs and fees of the discovery motion.

6. Due to their involvement in planning and implementing data storage policies and procedures, managers and system administrators are good initial sources for discovering this type of information.

7. An attorney requesting discovery may also wish to clarify, in detail, the definition of the data that is being sought. When an attorney seeks documents contained in an opposing party's computer system the attorney seeking discovery should specify that "computer system" includes: storage media such as hard drives, floppy disks, compact discs, and backup devices; workstations including laptop computers; PDAs (personal data assistants) such as Palm Pilots and handheld computing devices; network, internet, and mainframe servers and devices; and even the home computers of relevant employees who telecommute or who routinely take work home.

8. For further discussion on how to effectively formulate electronic discovery strategies and techniques see Barone, *supra* note 2; Carey Sirota Meyer & Kari L. Wraspir, *E-Discovery: Preparing Clients For (And Protecting Them Against) Discovery in the Electronic Information Age*, 26 Wm. Mitchell L. Rev. 939 (2000); Christopher D. Payne, *Discovery of Electronic Evidence*, 1 Ann.2001 ATLA-CLE 441 (July, 2001); Jacob P. Hart & Anne Marie Plum, *Litigating The Production of Electronic Media: "Disk-discovery" Issues for the 21st Century*, SG007 ALI-ABA 169 (July 12-13, 2001); and Debra S. Katz & Alan R. Kabat, *Electronic Discovery in Employment Discrimination Cases: As Employers Step More Boldly into the Computer Age, Plaintiff Lawyers must Embolden Themselves to Conduct More Sophisticated Discovery*, 34-DEC Trial 28 (December, 1998). & Katz & Kabat, *infra* note 8.

9. For further discussion on the types of electronic data see Meyer & Wraspir, *supra* note 8.

10. No special skills or tools should be needed to access active data. A quick search of computer system storage locations (i.e., the hard drive or network server) would show the active data that is currently accessible.

11. Most word processing programs continually create automatic back-up copies (also described as "file clones") while the computer user is creating, editing or otherwise working with the computer file. The purpose of such a process is to guard against loss of data should a catastrophic event, such as a power failure, cause the active document to be lost. Other types of file clones may be created by computer networks when the active file is e-mailed or sent to a network printer. Residual copies of any one document may reside on multiple computers, network servers and may even remain in the memory buffer of network printers long after the active file has been completed, archived and deleted from the original computer.

12. In Gates Rubber Co. v. Bando Chem. Indus., 167 F.R.D. 90 (D. Colo. 1996), the court imposed sanctions when one party used the commercially available "Norton's Unerase" program in an attempt to retrieve requested residual data. The process of installing the program overwrote 7 to 8 percent of the hard drive, thus permanently destroying data that was potentially subject to discovery. See also note 18, *infra*.

13. At least one court has ordered that printed versions of electronic documents must include all significant material contained in the electronic form to ensure the completeness of the evidentiary data. See Armstrong v. Executive Office of the President, 1 F.3d 1274 (D.C. Cir. 1993).

14. "Spoliation" refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. See Silvestri v. General Motors Corp., 271 F.3d 583 (4th Cir. 2001).

15. Several factors contribute to the rising cost of discovery: first companies retain greater quantities of data electronically than in the days when data was primarily retained on paper; second many companies do not have effective data retention policies and consequently retain vast amounts of data that become increasingly costly to search through; third even when companies have effective data retention policies many computer networks retain files and data in multiple and residual forms thus subjecting the parties to costly data retrieval; and fourth the Federal Rules compound the above factors by allowing virtually limitless discovery. See Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear The Costs of Discovery of Electronically Stored Data*, 57 Wash. & Lee L. Rev. 257 (2000) (this note reviews the above factors and explores the manner in which the federal judiciary has addressed these problems).

16. The producing party generally bears the cost of responding to a discovery request. In In re Brand Names Prescription Drugs Antitrust Litigation, 1995 WL 360526; 1995 U.S. Dist. LEXIS 8281 (N.D. Ill. June 15, 1995) the court ordered the producing party to pay the costs of producing approximately 30 million pages of information at a cost of \$50,000-\$70,000 because the court reasoned that the requesting party should not be forced to bear a burden caused by the producing party's choice of data storage. Other courts have allocated these discovery costs in differing ways. See *Giacobbe*, *supra* note 15.

17. In Playboy Enterprises, Inc. v. Terri Welles, Inc., 60 F. Supp. 2d 1050 (S.D. Cal 1999) the plaintiff requested access to the defendant's personal computer for the purposes of reconstructing certain e-mail messages that the defendant admitted to having deleted. The court granted the access to the defendant's hard drive through a court appointed computer expert and a detailed protocol designed to protect the defendant from invasion of private and privileged matters while allowing the plaintiff access to material that was rightfully subject to plaintiff's discovery requests.

18. Plaintiff attorneys in the recent Fen-Phen litigation used computer programs to sort through and locate documents helpful to their side. See "News and Trends", 37-OCT Trial 12 at *105 (Oct. 2001) (providing a description of one electronic discovery software tool). See also *Payne*, *supra* at note 8 (providing website addresses for various electronic data services).

19. The court in Strauss v. Microsoft Corp., 814 F. Supp. 1186 (S.D.N.Y 1993) relied on a series of e-mail messages along with other evidence to reject the employer's motion for summary judgment. Another court found that an employee stated a claim for hostile work environment where she alleged that another employee used his work computer to access pornographic material and brought the images to her attention in an attempt to elicit a reaction. Coniglio v. City of Berwyn 1999 WL 1212190, 1999 U.S. Dist. LEXIS 19426 (N.D. Ill. Dec. 16, 1999). In 1995, Chevron Corporation paid \$2.2 million to settle a sexual harassment charge that it permitted its e-mail system to be used to distribute sexually offensive messages including one titled "25 Reasons Why Beer Is Better Than Women." See *Morris*, *supra* note 2. Another company settled a sexual discrimination suit for \$250,000 when an e-mail sent from the president to the head of personnel stating "Get rid of that tight-assed bitch" was discovered by the plaintiff. See id.

20. Clients may routinely destroy old data through a data retention policy so long as the policy is tailored to meet specific needs related to legitimate business objectives and not merely to thwart current or future litigation. Clients should be careful in deciding how to dispose of old data. In Danis v. USN Communications Inc., 2000 WL 1694325, 2000 U.S. Dist. LEXIS 16900 (N.D. Ill. Oct. 23, 2000) the court fined the defendant \$10,000 and instructed the jury that defendant had failed to produce key documents; documents that had been destroyed as a result that the defendant had delegated the task of data preservation to an inexperienced in-house counsel. Another court issued a \$1 million sanction against Prudential Insurance Co. for improperly destroying electronic data necessary for the establishment of a plaintiff's claims. In re Prudential Ins. Co. Sales Practices Litigation, 169 F.R.D. 598 (D.N.J. 1997). In Proctor & Gamble Co. v. Haugen, 179 F.R.D. 622 (D. Utah 1998) the court issued discovery sanctions of \$10,000 against defendant for discarding e-mail messages of employees identified during discovery who possessed knowledge relevant to the litigation.

21. For a discussion about the nature and type of specialized data recovery experts see *Payne*, *supra* note 8. See also note 17 *supra*.

22. An example of an e-mail disclaimer follows:

THE INFORMATION CONTAINED IN THIS E-MAIL COMMUNICATION IS INTENDED ONLY FOR THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENT NAMED ABOVE. This message may be an Attorney-Client communication, and as such is privileged and confidential. If the reader of this message is not the intended recipient, you are hereby notified that you have received this communication in error, and that any review, dissemination, distribution, or copying of the message is strictly prohibited. If you have received this transmission in error, please notify us immediately by telephone and/or reply email.

Brett R. Harris, *Counseling Clients Over the Internet*, 18 No. 8 Computer & Internet Law 4 (August, 2001).

23. Documents and data properly categorized by parties as “highly confidential” may be subject to a protective order. See Quotron Sys., Inc. v. Automatic Data Processing, Inc., 141 F.R.D. 37 (S.D.N.Y. 1992).

24. See ABA Comm. on Ethics and Professional Responsibility, Formal Op. 413 (1999).

25. See Harris, *supra* note 22 (for a state by state comparison of ethical opinions); and Miller, *supra* note 2.

26. Issues such as the best evidence rule, authentication of evidence and hearsay could render certain electronic documents inadmissible at trial. This should not deter the Attorney requesting electronic discovery because many documents are relevant and discoverable notwithstanding their potential for admissibility at trial. See Mark D. Robins, *Computers and the Discovery of Evidence - A New Dimension to Civil Procedure*, 17 J. Marshall J. Computer & Info. L. 411 (winter 1999).