

Discovery of Electronic Evidence

David Kerwin*

1

- I. A Beginning Word of Caution 2
- II. Initial Steps 5
 - A. Send a Notice of Litigation and Preservation of Evidence Letter 5
 - B. Ask the Court to Shape Certain Parameters of the Discovery Process 6
- III. Interrogatories and Requests for Electronic Documents 10
- IV. Objections and Their Resolution 19
- V. Rule 30(b)(6) Deposition of Opposing Party's IT Expert(s) 22
- VI. Other Important Things to Remember 24
 - A. Get Backups 24
 - B. Image-Copy Everything and Protect Data Integrity 28
 - C. Ask Everybody About Computer Usage 28
 - D. Work Closely With Your IT Expert 29
- VII. Allocation of Costs 30
 - A. Different Approach to Cost Allocation 34
 - B. Alterations to the *Rowe* Factors 36

* Mr. Kerwin is an attorney in the State of Washington. He was assisted by Jordan Rubinstein who contributed to the materials on cost-shifting. Mr. Rubinstein is practicing with the firm of Jones Day in New York City.

1. Factors Added by *Zubulake* to the *Rowe* Test 36
2. Factors Eliminated From the *Rowe* Test 37
- C. Test Sample Before Reallocating Costs 42
- D. Costs Related to the Resolution of Privilege Claims 42
- VIII. Proactive Measures Prior to Litigation 45
- IX. Additional Source of Income for Law Firms 46

The information provided in this chapter assumes a reader's familiarity with the discovery rules in the Federal Rules of Civil and Criminal Procedure. This chapter gives an understanding of what may be encountered when engaging in initial discovery concerning a party's document and data creation, location, maintenance, storage, and destruction. A sample document request is provided, and deposition and interrogatory questions are proposed.

I. A BEGINNING WORD OF CAUTION

Engaging in effective discovery of e-evidence can be exceedingly complex and technologically challenging. Few lawyers have the necessary expertise in information technology (IT) to be adequately prepared to handle the mountains of materials that usually must be sifted, organized, examined, and coordinated. As a consequence, lawyers attempting to "go it alone" in this computer age often discover that they are ill-equipped to compete with the IT experts advising those from whom discovery is sought. Most lawyers, particularly when they first encounter electronic discovery, find it helpful, if not necessary, to retain consulting firms specializing in IT to advise or even direct electronic discovery undertakings.¹

1. *See* *United States v. Lloyd*, 269 F.3d 228 (3d Cir. 2001) (computer forensics experts were critical in discovering evidence of digital "time bomb" placed in a company's computer system by saboteur); *Taylor v. State*, 93 S.W.3d 487, 502-03 (Tex. Crim. App. 2002) (holding that a criminal defendant has a right to have an expert analyze a hard drive entered into evidence against him, analogous to a drug case where a defendant has a right to have an independent expert analyze the contraband in question); *Munshani v. Signal Lake Venture Fund II*, 2001 WL 1526954 (Mass. Sup. Ct. 2001) (court-appointed computer forensics experts were able to determine that plaintiff fabricated e-mail in question and attempted to hide fabrication).

The last two decades have seen exponential growth in the amount of digital information involved in the normal business activity of most companies. Such data is now routinely requested during the course of litigation. A single backup tape or even a portion of a hard drive can easily contain the equivalent of millions of printed pages.

Just as e-mail has become critical to the operation of many businesses, it has become critical to the discovery process in both civil and criminal litigation. Due to the heavy dependence of many businesses on electronic communications, as much as 80 percent of discoverable communications will be in the form of e-mail because it is often the primary tool for business and personal communications. Retrieving such data, placing it within a useful context, and maintaining its integrity can be critical to its authentication and use at trial.²

In the past, there was a common misconception that when an e-mail or a file is “deleted,” it is gone forever. This, of course, is rarely the case.³ Computer operating systems use various methods for storing data. The most common types, used by Microsoft operating systems, are FAT (File Allocation Table) and NTFS (NT File System). When a file is deleted by a user, the name of the file is removed from the operating system’s file tracking table, but the data itself remains intact until overwritten or explicitly erased by some other method. An expert may be able to recover this information, in whole or in part, and also may be able to re-create the time line in which the information was created, utilized, and deleted. In order to facilitate discovery, a court usually will order a party, when making data available, to reveal any passwords or encryption systems that protect the data. Where this is not the case, an expert will be able to “hack” such information and gain access to the data for you.

2. See Chapter 6, Authentication, *infra*.

3. See *Arista Records, Inc. v. Sakfield Holding Co.*, 2004 WL 881851, at *5 (D. D.C. April 22, 2004) (“Plaintiffs’ computer expert recovered a small amount of information from the computer servers despite defendant’s attempts to destroy all the files. The information recovered showed partial lists of Puretunes users and a partial record of music file downloads. Using this information, plaintiff was able to extrapolate data showing that approximately 241 Puretunes users were located in the District of Columbia . . . and that these users downloaded approximately 20,000 music files from Puretunes.”). This is true of even self-deleting e-mail programs. Such programs only destroy the encryption key that opens them. A computer forensic expert will be able to retrieve such e-mails.

Forensic experts in computer science offer a number of advantages when engaging in electronic discovery:⁴

- They will have the experience and the equipment to handle the diverse array of software and hardware that you may encounter. Many companies from which you will take discovery will not have maintained their records in formats that are compatible with the equipment you may regularly use.
- They will be able to provide the bandwidth, disk space, and processing power necessary to analyze all of the relevant data.
- They will be able to assist in finding crucial data that may have been deleted or hidden.
- An expert will also be able to assist you with properly drafting interrogatories, depositions, and requests for document production and in maintaining the integrity of chains of custody. Such assistance in drafting discovery requests can be invaluable in jurisdictions that limit the number of discovery requests available to each party.

Because of the special characteristics of e-mail, experts are particularly helpful when attempting to discover those communications. For instance, e-mail messages often reside in several locations (for example, both on a network server and locally on a user's machine), making it very difficult to ascertain when an e-mail has truly been "deleted" or has ceased to exist in all recoverable formats. An e-mail often has a life span well beyond the original intention of its author. Any given message may be answered or forwarded any number of times. An expert will be able to assist in recovering e-mails by analyzing the route along which they have traveled. An expert will be able to dissect and analyze the various components of an e-mail message, such as its header, the message itself, and any embedded objects that may be attached to the e-mail. E-mails sent via the Internet will necessarily travel via "ISPs" (Internet Service Providers), in addition to any number of other minor stops and redirection points. Accessing and analyzing information from these ISPs can be an important link in putting together the overall picture.

4. This information was obtained from Ms. Joan Feldman, of Computer Forensics, Inc., in Seattle, Washington. She is a leading expert in the field of electronic discovery and has provided assistance to attorneys in many cases of varying size and complexity.

The fees that such an expert will charge will vary depending upon the services rendered. Simply having data recovered from a hard drive or a back-up tape will be less expensive, but will leave you to decipher the results yourself. In an amusing opinion by Judge Samuel B. Kent of the Southern District of Texas, the court issued a warning to those who would depend upon e-evidence of questionable origin. Judge Kent scolds a party for relying upon the “voodoo information taken from the Internet”⁵ and suggests they do a better job of searching the opposing party’s “hard copy” documents. His decision reinforces the importance of gathering and analyzing digital information in a knowledgeable and useful manner. The assistance of IT experts can ensure that.

II. INITIAL STEPS

A. *Send a Notice of Litigation and Preservation of Evidence Letter*

While in theory an opposing party in litigation is put on notice by the filing of the lawsuit to maintain pertinent documents for purposes of discovery and not to engage in spoliation of any kind,⁶ it is often helpful, and in some instances critical, in e-discovery cases to immediately send the opposition a letter requesting the preservation of certain digital evidence. Early notice is important not only to keep relevant data from being intentionally deleted, but also to keep data from being lost through the natural processes of computer usage.⁷

While such letters are often helpful with opposing parties, they may be critical to the preservation of evidence by parties not named in the complaint. You should send a prompt notice to all third parties who possess information that may be relevant to your litigation. With such notification, you can establish a clear point in time when their obligation to preserve

5. *St. Clair v. Johnny’s Oyster & Shrimp, Inc.*, 76 F. Supp. 2d 773, 775 (S.D. Tex. 1999).

6. *See* Chapter 2, Spoliation, *infra*.

7. *See* *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 651-52 (D. Minn. 2002) (granting plaintiff’s motion requesting expedited discovery, based on finding that “Defendants may have relevant information, on their computer equipment, which is being lost through normal use of the computer, and which might be relevant to the Plaintiff’s claims, or the Defendants’ defenses. This information may be in the form of stored or deleted computer files, programs, or e-mails, on the Defendants’ computer equipment.”).

potentially relevant information arose. You should consider sending notification letters to unnamed parties even before litigation has actually begun, so that preservation may begin at the earliest possible time, before any potentially relevant information has been innocently destroyed.⁸

This initial notice should carefully outline the types of information to be preserved. This should include e-mail and all attachments to those messages, data files created, and data that may be under the control of both employees (current and past) and other third parties (such as outside directors).⁹ The location of these materials should also be specified—for example, laptop computers, home computers and other remote office locations, network activity logs, server activity and maintenance logs, and data within electronic organization programs such as Microsoft Outlook. You also want to make very clear that all data should be preserved, both active and archived (or “backed-up”). Users should be directed not to install or remove any applications on their computers and not to run any disk-altering utilities such as a disk defragmenter. This notification letter should emphasize that special efforts must be taken to suspend usual processes for deletion of data.

B. Ask the Court to Shape Certain Parameters of the Discovery Process

Electronic data is discoverable under Federal Rule of Civil Procedure 34, because such data falls under the definition of “documents.”¹⁰ This in-

8. As explained in Chapter 2, Spoliation, *infra*, the duty to preserve arises when it becomes apparent that evidence possessed by a company may be relevant to an existing dispute.

9. *In re Triton Energy Ltd. Sec. Litig.*, No. 5:98CV256, 2002 WL 32114464, at *4 (E.D. Tex. Mar. 7, 2002) (after notification letter, company never sent instructions to preserve to outside directors on the theory that they were not within company’s control).

10. FED. R. CIV. P. 34(a)(1) (“Any party may serve on any other party a request . . . to produce . . . documents (including . . . data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form); *see also* FED. R. CIV. P. 34, Advisory Committee’s Note (noting that data considered to be a discoverable document under Rule 34 “applies to electronic data compilations from which information can be obtained only with the use of detection devices”); *Crown Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (ruling that Fed. R. Civ. P. 34 makes computer data discoverable); *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645 (D. Minn. 2002) (analyzing the data at issue and finding that “the deleted information, on the Defendants’ computer equipment, may well be both relevant and

cludes not only current data being utilized by a party, but also backups of data and even deleted data that can be recovered.¹¹ In *Antioch Co. v. Scrap-*

discoverable”); *MHC Investment Comp. v. Racom Corp.*, 209 F.R.D. 431 (S.D. Iowa 2002) (mentioning, without comment, the general discoverability of e-mail); *Collette v. St. Luke’s Roosevelt Hospital*, 2002 WL 31159103 (S.D.N.Y. 2002) (passing without comment on the general discoverability of e-mail); *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 427 (S.D.N.Y. 2002) (finding that “[e]lectronic documents are no less subject to disclosure than paper records” and that “Rules 26(b) and 34 of the [FRCP] instruct that computer-stored information is discoverable under the same rules that pertain to tangible, written materials.”); *McPeck v. Ashcroft*, 202 F.R.D. 31, 32 (D. D.C. 2001) (ordering that during discovery “the producing party has an obligation to search available electronic systems for information demanded”); *Simon Property Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) (holding that “computer records, including records that have been ‘deleted,’ are documents discoverable under Fed. R. Civ. P. 34”); *Santiago v. Miles*, 121 F.R.D. 636 (W.D.N.Y. 1998) (commenting that a “request for raw information in computer banks is proper and the information is obtainable under the discovery rules”); *Storch v. IPCO Safety Prods. Co.*, 1997 WL 401589 (E.D. Pa. 1997) (ruling that “in this age of high-technology . . . it is not unreasonable for the defendant to produce the information on computer disk for the plaintiff.”); *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 WL 649934 (S.D.N.Y. 1995) (stating as black letter law that computerized data, if relevant, is discoverable, even where hard copies of the same information have already been produced); *Unnamed Physician v. Bd. of Trustees of St. Agnes Medical Ctr.*, 113 Cal. Rptr. 2d 309 (Cal. Ct. App. 2001) (ordering, for purposes of a physician review hearing, that the hospital allow the physician access to all documents relating to the hospital’s computer system, excepting those of a proprietary nature); *Linnen v. A.H. Robins Co.*, 1999 WL 462015 (Mass. Sup. Ct. 1999) (commenting that a discovery request for electronic documents is no different “in principal, from a request for documents contained in any office file cabinet”). See also D. WYO. L. R. 26.1 (requiring counsel to investigate their client’s information management systems so as to be familiar with them and to provide initial discovery disclosures as to electronic evidence, including archived and legacy data prior to pretrial conference); ILL. SUP. CT. R. 201, 214 (the word “document” includes “all retrievable information in computer storage”; also, counsel is required to review their own and their client’s computer system for discoverable data and to attach an affidavit to this effect; also, production of data is to be done in printed form); TEX. CT. R. CIV. PRO. 196.4 (requiring responsive parties to produce “electronic and magnetic data” responsive to discovery requests; when this data cannot be recovered through “reasonable efforts,” the responding party may object and the court may then, at its discretion, enforce the request for discovery, but must, in doing so, shift the cost of discovery to the requesting party).

11. *In re Amsted Indus.*, 2002 WL 31844956 (N.D. Ill. Dec. 17, 2002) (court ordered defendant to search its backup tapes a second time using a broader subject

Sample Preservation Letter

Please be advised by this communication that [*counsel's name*] requires your assistance in preserving all electronically stored information relevant to the matter of [*describing in detail the time frame, parties, transactions, and issues to which evidence may be relevant*]. This is a case in which electronic data, such as e-mail, will be critical to the discovery process and various evidentiary matters.

This upcoming lawsuit and the discovery to take place require the immediate and future preservation of all of [*corporation's name*]'s computer systems, removable media, any existing backup data, and any other relevant electronic data existing in any format. This includes, but is not limited to, electronic mail, any electronic communications, any word processing documents (e.g., Word, Word Perfect, etc.), any database spreadsheets (e.g., Excel, etc.), any databases (e.g., Access, SQL, Exchange, etc.), electronic calendars, electronic planners, telephone logs, network logs, and network maintenance logs.

Employees and directors (both inside and outside, present and past) of [*corporation's name*] must take all reasonable and logical steps to preserve the above-listed information.

If any portion of this letter or any term used herein is unclear, vague, or might be clarified in any way, please contact [*identify contact person with contact information*] for further direction.¹²

matter and time period; court required the same search of any relevant individual's e-mail). As to backups of data, considering the sometimes high cost involved in their re-creation, a court may require a showing of necessity and will often consider shifting costs. *See* Section VII, Allocation of Costs, *infra*.

12. *See* *Wiginton v. Ellis*, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003) for another illustration of the type of notice that has been given in an action involving electronic communication and for a discussion of the other lengths to which the lawyer had to go to ensure notice was given and disseminated.

*book Borders, Inc.*¹³ the court found that the parties could be relied upon to make appropriate disclosures of current data requested by opposing counsel, but established the following specific guidelines for the discovery of deleted information on the defendants' computer equipment:

- First, the plaintiff had to select a computer forensics expert and notify the defendant of its choice.¹⁴
- The defendant then had to make its computer systems available to that expert so that a "mirror image" of the data could be made.¹⁵
- Only the computer forensics expert was allowed to review this data, and was required to keep the data confidential.
- Within ten days of completing its analysis, the expert was to supply both parties with a full report of what was produced by the defendant for examination and what actions were taken by the expert.
- Finally, the court ordered the expert to compile the collected and filtered data and to make two copies, one for the court and one for the defendant. Thereafter, the defendant would have the responsibility of sifting through the data and responding appropriately to the plaintiff's document requests.

The court in *Antioch* relied upon the precedent of two similar cases in structuring the discovery order. In *Playboy Enterprises v. Welles*,¹⁶ the court first required plaintiffs seeking discovery to submit to the court an affidavit from a computer forensics expert as to the feasibility of recovering certain deleted data.¹⁷ Assuming that this affidavit stated that there was at least a 50 percent chance of a successful data recovery and that the process would not damage the defendant's computer system, the court would then appoint its own computer forensics expert, based upon an agreement between or suggestions of the parties, to create a mirror image of the defendant's systems. The mirror image then would be turned over to the defendant for purposes of filtering out privileged information

13. 210 F.R.D. 645 (D. Minn. 2002).

14. *Id.* at 653.

15. A "mirror image" is a very exact, byte-by-byte duplication of a data compilation, usually of a hard drive.

16. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).

17. *Playboy Enterprises*, 60 F. Supp. 2d at 1055.

and responding to plaintiff's document requests. In *Triton Energy Limited Securities Litigation*,¹⁸ the court appointed a forensic expert and required the offending party to give the expert unfettered access to its computer equipment. After the expert retrieved what was retrievable, the materials were to be reviewed by a special master appointed by the court to make any necessary relevance and privilege determinations.

In *Simon Property Group L.P. v. mySimon, Inc.*,¹⁹ the court ordered discovery to proceed much the same as in *Playboy Enterprises*, with a few key differences. The expert in *Simon* was ordered to make a full report not only to the defendant, but also to the court.²⁰ In addition, the expert was to inform the defendant of specifics as to "deleted" files, both recoverable and unrecoverable, was ordered not to communicate with plaintiff's counsel *ex parte*, and was to retain the collected data until the conclusion of litigation.

III. INTERROGATORIES AND REQUESTS FOR ELECTRONIC DOCUMENTS

An initial series of interrogatories should be used in order to gain an overall view of the computer system and data that are in play. In lieu of this formal procedure, the discovery of information about the existence and location of electronic documents can also be handled through the pretrial conference required by Fed. R. Civ. P. 16(c). Rule 16 permits the judge to issue appropriate orders to manage and control the pretrial process and ensure the just and speedy disposition of the action.

If interrogatories are employed, they should seek all available information on the types and locations of every current and past data creation and retention mechanism. An exhaustive list of inquiries directed to that end is provided in the following sample interrogatory.

18. No. 5:98CV256, 2002 WL 32114464, at *6 (E.D. Tex. Mar. 7, 2003).

19. 194 F.R.D. 639 (S.D. Ind. 2000).

20. *Id.* at 641.