Rhode Island Bar Journal

December, 1996

DISCOVERY AND THE USE OF COMPUTER-BASED INFORMATION IN LITIGATION

Peter v. Lacouture, Esq.

INTRODUCTION

Personal computers and electronic information have become ubiquitous in the information age. The most common form of electronic information--E-mail--is becoming widespread. [FN1] It has been estimated that 35% of corporate communications never reach paper. Electronic information is contained in many forms and formats including internal computer files, disks and diskettes, magnetic tapes and various transaction reports including those from fax machines and telephone systems. [FN2] It is routinely retained on diskette or tape as a backup for the inadvertent loss of data through computer malfunction or other casualty, for archive purposes, and in many instances because of laziness [FN3] or lack of understanding by the computer owner or operator. [FN4]

Computer based files are an often over-looked subject of discovery and source of helpful information in litigation. Knowledge about the methods of storing and using computer-based information can give a litigator a tactical advantage over opposing counsel. Similarly, counsel should advise clients of the potential dangers and burdens of uncontrolled retention of computer-based information.

An understanding of certain technical details is critical to the effective discovery of computer files. A computer file is not physically erased from a disk when it is deleted. Rather, the computer operating system changes the first character of the file name in the disk directory to indicate that the space occupied by the file is not in use and may be reused. Therefore, it is a relatively straightforward process to recover "deleted" files, as long as new information has not been written over them. Similarly, when a magnetic tape is reused, the information that is written over will be lost, but old files may exist and survive beyond the end of the new information.

Finally, an attorney seeking to discover electronic information from an opposing party should be aware of the chaos of disks and backup. The disks and tape cartridges used for backup are generally of a relatively small size, often are not cataloged and are rarely needed. In some organizations, backup materials are stored at an off-site location.

DISCOVERY TECHNIQUES

The basis for discovery of electronic information is Rule 34, [FN5] which permits a party to serve on the other party a request:

(1) to inspect and copy documents (including writings, drawings, graphs, charts, photographs, photo-records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form), or

(2) to inspect and copy, test or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) ... [emphasis supplied.]

Although the term "document" is defined in Rule 34, a request for production which seeks electronic information should be expressed so that there can be no misunderstanding. In particular, the requesting party should specify the form of storage (tapes, disks and memory), the condition (including back-up and deleted files) and location (on-site or off-site). It is also important to specify that drafts are to be considered additional documents. Unless one's client or computer expert has very good information about the other party's computer system, a request to inspect should be phrased broadly to avoid limiting the expert's search. One approach is to serve interrogatories on the other party to develop the information which counsel and the computer expert can use to determine whether to make a request to inspect. In particular, one would seek identification of computer systems and equipment in use, the persons responsible for operation and maintenance of the system, any written back-up policies and procedures, and any record retention and destruction policies. [FN6]

DUTY TO PRESERVE INFORMATION

An important issue in many of the reported discovery cases is the duty to preserve information during litigation. While it is generally accepted that a litigant is under no duty to keep or retain every document in its possession, one has a duty to preserve what he knows or reasonably should know (i) is relevant to the action, (ii) is reasonably calculated to lead to the discovery of admissible evidence, (iii) is reasonably likely to be requested during discovery, and/or (iv) is the subject of a pending discovery request.

However, there is disagreement as to when this duty arises. In Skeete v. McKinsey & Company, Inc., No. 9099 (S.D.N.Y.1993) (LEXIS), the court stated the duty arises "once a complaint is filed." In contrast, several courts have held that the duty arises when one is on notice that documents are relevant to either pending or potential litigation. Wm. T. Thompson Co. v. General Nutrition Corp., Inc., 593 F.Supp. 1443, 1455 (C.D.Cal.1984); Capellupo v. FMC Corp., 126 F.R.D. 545, 551 (D.Minn.1989). In any case, it is clear that a party ignores the obligation to

preserve information at his own peril:

The obligation to retain discoverable materials is an affirmative one; it requires that the agency or the corporate officers having notice of discovery obligations communicate those obligations to employees in possession of discoverable materials.

National Ass'n of Radiation Survivors v. Turnage, 115 F.R.D. 543, 557 (N.D.Cal.1987).

Given the duty to preserve information and the danger and ease of destroying electronic information, one should consider sending a letter to a prospective defendant or his counsel requesting preservation of computer-based files and records prior to the commencement of litigation.

SANCTIONS FOR DESTRUCTION OF EVIDENCE

Both state and federal courts have considerable authority to impose sanctions on parties who destroy requested documents under Rule 11, Rule 37, 28 U.S.C. 1927 and the "inherent power [of the court] to regulate litigation, preserve and protect the integrity of the proceedings before it, and sanction parties for abusive practices." Capellupo, supra, 126 F.R.D. at 551.

The sanctions for bad faith include rulings that affect the proof or defense of a party's case, monetary sanctions and the imposition of special procedures to prevent future violations. The courts often preclude the introduction of evidence as to a contested issue if a party has destroyed relevant evidence. See Allstate Insurance Co. v. Creative Environment Corp., No. 13307 (D.R.I.1994) (LEXIS); Fashion House, Inc. v. K MART Corp. 892 F.2d 1076, 1080 (1st Cir.1989); but see Skeete, supra, where the court declined to impose sanctions because the plaintiff in a Title VII case who had lost tapes and documents was unsophisticated and did not act in bad faith. In particularly egregious cases, the courts may also terminate the litigation. Thompson was an antitrust suit in which the plaintiff alleged that the defendant had used bait-and-switch advertising practices. The plaintiff proved that the defendant had destroyed extensive records of inventory and sales. The court found that the records were irreplaceable and that the defendant "deliberately and purposefully undertook a program to impede and obstruct the litigation process." Thopmson, 593 F.Supp. at 1456. Finding the bad faith, it held that any sanction less severe than default would reward the defendant for its misconduct. Consequently, it entered default against the defendant. The Rhode Island Supreme Court has held that the remedy of termination under Rule 37(b)(2) is not available without the development of a record on the reasons for the unavailability of the evidence. Sampson v. Marshall Brass Co., 661 A.2d 971 (R.I.1995).

An extreme example of discovery abuse by defendants occurred in Turnage. In that case, veterans who had been exposed to ionizing radiation during military service were challenging the constitutionality of the claims procedure adopted by the Veterans Administration. The effect of the challenged claims procedure was to deny the claimants the right to counsel. Because of the obstruction of the discovery process by the VA, the court imposed additional discovery obligations on the VA. It ordered that all future responses to discovery requests be signed by an attorney designated by the VA and by general counsel of the VA. The court also required the VA to develop and present to the court a plan for compliance with future discovery. The VA was directed to circulate notices to all of its employees advising them of (i) the action and (ii) their obligation to preserve evidence and to cooperate in the proceedings. Finally, the court appointed a special master to oversee future discovery and impose monetary sanctions.

In Turnage, the court imposed a counsel fee of $105,000 against the defendant, while in Thompson, the court awarded a counsel fee of $457,000 for the plaintiff's efforts in discovery.

HOW TO PROTECT AGAINST DISCLOSURE

After litigation has been commenced or threatened, it is too late to consider measures to avoid disclosure of documents. However, a thoughtful record retention policy and control of the use of e-mail by corporate employees can reduce the discovery burden if one becomes a party to litigation.

There are several dangers associated with the adoption of a record retention policy. The first is uneven application or implementation of the policy. Thus, in Lewy v. Remington Arms Co., 836 F.2d 1104, 1112, (8th Cir.1988), the court held that the trial court should determine "whether the record retention policy is reasonable considering the facts and circumstances surrounding the relevant documents." There is also the risk of the inadvertent destruction of records after the commencement or receipt of notice of litigation--"[A] corporation cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy." Id.

A record retention policy must promote a business purpose (e.g., control of the volume of records and files that must be stored), and be adopted in good faith. The policy must provide for a reasonable retention period by category of documents and, as noted above, be implemented and enforced evenly. The policy itself should specify what files must be saved and provide a retention period for each class of files. It should specify storage location, storage media, and destruction processes. Finally, it should contain an explicit process to secure documents and files in case of litigation to avoid the inadvertent destruction of records.

E-MAIL

Corporate e-mail has been characterized as a "plaintiff's dream and a defendant's nightmare." Anyone who has used e-mail will likely recognize the following characteristics:

.E-mail is immediate--messages and replies are often stream of consciousness; unlike a letter or even voice mail, one often replies to e- mail immediately.

.E-mail is rarely thoughtful (most of us would not send a letter with the typos that we tolerate in e-mail).

.E-Mail messages proliferate with mailing lists, copies and replies.

The potential danger of e-mail to a corporate defendant was demonstrated in Strauss v. Microsoft Corp., No. 7433 (LEXIS), 68 Fair Employment Practice Cases 1576 (S.D.N.Y.1995), where the plaintiff, an assistant editor at the Microsoft Systems Journal, filed suit against Microsoft alleging sex discrimination in its failure to promote her to the position of technical editor. Microsoft sought to preclude the use of sexually explicit e-mail and comments, arguing that they were irrelevant, unfairly prejudicial, and would confuse and mislead the jury. Not surprisingly Microsoft's efforts were rebuffed. [FN7]

The risk of e-mail to a client can be reduced by adopting and enforcing a company e-mail policy or protocol. This should at a minimum include the following provisions:

The e-mail system is owned by the employer.

E-mail is to be used for business purposes only (no solicitation or distribution).

E-mail messages are to be kept confidential by the employee.

The employee acknowledges that e-mail may be monitored and disclosed by the employer. [FN8]

Humor and sarcasm are often misinterpreted and should not be used in e- mail.

Do not use the system for personal matters or comments about others.

Do not send an e-mail message if you are angry.

All messages will be deleted 30 days after they are sent unless archived by the recipient.

Employees should archive only important or critical messages.

Employees should organize archived messages by subject and delete groups when they are no longer needed.

Archived messages will be subject to review and production in litigation (**see** the "Providence Journal rule, above.)

CONCLUSION

The proliferation of e-mail and other computer-based files presents fertile opportunity for discovery by creative counsel in litigation. It also presents a danger to counsel who does not understand the measures one must take to preserve electronic evidence. Finally, it offers a challenge for corporate counsel in developing policies to control and minimize the risk and burden of responding to discovery.

APPENDIX

Sample definition for request for production (RCP 34)

"Document means any writing, drawing, graphic material or data compilations, including, without limiting the generality of the foregoing, agreements, contracts, notes, work papers, memoranda, ... [insert additional descriptive phrases as preferred], whether stored in tangible, electronic, mechanical or electric form or representation of any kind (including (i) materials on or in computer tapes, disks and memory and (ii) backup copies and "deleted" files on a computer or computer storage device or media) whether located on-site or off-site. All drafts, copies or preliminary material which are different in any way from the executed or final document shall be considered to be additional documents as that term is used herein."

Sample interrogatories

1. Describe the computer system(s) used by [plaintiff/defendant] currently and at any time within the past [5] years, including, but not limited to, for each such system, the brand and model of the computer, the amount of memory and size of the hard disk, the version of the operating system, the type and version of network software, if any, the brand and model of all peripheral devices including tape drives, external disk drives, other storage devices and modems; the brand and version of major software in use on the system(s) during such period, and the name of all on-line (electronic) services that have been accessed with the system(s) during such period.

2. Provide the name, employer, title, business and home addresses and telephone numbers for each person with operational or maintenance responsibility for the computer system(s) described above [during time period], including, but not limited to, the person(s) who maintain the

hardware described in (1) above, the person(s) responsible for installing new and upgraded software on the system(s), the person(s) responsible for the day-to- day operation of the system(s), and the person(s) responsible for making back- ups or archiving files and data on the system(s).

3. Describe policies and procedures followed by [plaintiff/defendant] for backing-up files and data on the computer system(s) described in (1) above, including, but not limited to, the frequency of backups, the type of backup (full, differential or incremental), the software used during [period], the number of sets of tapes or other media and the rotation of such media, and whether such policies are in writing.

4. Describe all record retention and destruction policies and procedures followed by [plaintiff/defendant] during [period] including, but not limited to, the date the policy was adopted, the types of documents covered and the respective retention periods, the frequency of document destruction, whether any record is kept of what documents are destroyed, the manner the policy is communicated to [plaintiff's/defendant's] employees, and the identity of all employees with responsibility for implementing and executing the policy.

Sample request to inspect (RCP 34)

Plaintiff requests that defendant permit plaintiff to enter defendant's premises at [address] and to inspect, test, sample and copy the data, records and files (including e-mail sent or received by defendant and files located on remote computer systems that may be accessed by defendant's computer system(s)) on the hard drive(s), other storage devices, backup tapes and in memory of the following computer system(s) and any other computer systems located on said premises.

[List computer systems.]

Note 1. Peter V. Lacouture, Esq. is a partner at Peabody & Brown and is the chairperson of the Rhode Island Bar Association's Law Office Management/Computer Committee. This article is adapted from a presentation at the Rhode Island Bar Association Annual Meeting in June, 1996 by Mr. Lacouture and Thomas R. Galligan of Electronic Evidence Recovery, Inc.

[FN1]. It has been reported that Kodak employees send 2 million e-mail messages per day over their systems.

[FN2]. A typical 3 1/2 inch diskette which is used in a personal computer can hold 1,000 pages of double-spaced, type-written material; a CD can hold up to a half million pages; and there are tape cartridges on the market which can hold 2 1/2 million pages of information.

[FN3]. It is easier and probably cheaper to buy more hardware to store more data than to review an old index of documents to delete outdated, obsolete documents.

[FN4]. Many on-line services retain copies of e-mail messages that are sent or received by a subscriber on the service's central computer system. Therefore, deleting the message from the user's own computer will not delete the message stored on the service's computer.

[FN5]. The Federal and Rhode Island Rules are identical except for the time periods for responses provided in Rule 34(b).

[FN6]. A definition of "document," sample request for production, request to inspect and interrogatories are contained in the appendix to this article.

[FN7]. [T]he court quoted other courts as follows: "the Federal Rules favor placing even the nastier side of human nature before the jury if to do so would aid its search for the truth" and "what is prejudicial to the defendant is beneficial to the plaintiff." It failed to note the irony of Microsoft's attempt to exclude e-mail from the record.

[FN8]. The first four items can be summarized in the "Providence Journal" rule--do not write anything in e-mail that you do not want to see on the front page of the Providence Journal.

END OF DOCUMENT