DISCOVERY OF ELECTRONICALLY- STORED INFORMATION

DAVID C. PISHKO
WINSTON-SALEM, NORTH CAROLINA

For many businesses and individuals, computers have become the preferred means of communication and information storage. E-mail messages are replacing letters and memoranda; word processing programs retain "soft" copies of written communication; and data base software is used to preserve financial records, reports and other important information. Even material that was initially created in paper form is routinely being scanned into an electronic form for easier storage and retrieval.

As is often the case, the law has moved slowly in developing rules to deal with these changing circumstances. The Rules of Civil Procedure pertaining to discovery were drafted at a time when paper documents predominated, and many of us still think in terms of paper when developing our discovery plans and advising our clients what must be produced. Moreover, trial court decisions regarding the discovery of electronically stored information are rarely the subject of appellate review, so there are few published decisions to enable us to discern patterns and trends in dealing with these issues. This manuscript will set out the basic rules and then summarize the few cases which have considered three key questions: (1) what electronically- stored information is subject to discovery; (2) who should pay for the retrieval of this information; and (3) what happens if this information is destroyed prior to production.

I. DISCOVERY RULES APPLICABLE TO ELECTRONICALLY- STORED INFORMATION.

Rule 34(a) of the North Carolina Rules of Civil Procedure states, in pertinent part, that:

> Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on his behalf, to inspect and copy, any designated documents (*including . . . data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable*

form)...; or (2) to permit *entry upon* designated land or *other property* in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, . . . testing, or sampling the property or any designated object or operation thereon. . . .

The Advisory Committee Notes pertaining to the 1970 Amendment to Federal Rule 34 (which added "data compilations" to the definition of "documents") state that:

> The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data. The burden thus placed on respondent will vary from case to case and the courts have ample power under Rule 26(c) to protect respondent against undo burden or expense, either by restricting discovery or requiring that the discovering party pay costs. Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs.

II. WHAT ELECTRONICALLY-STORED INFORMATION IS SUBJECT TO DISCOVERY ?

Kleiner v. Burns, 2000 WL 1909470 (D.Kan.2000). The plaintiff filed a copyright infringement action against *Yahoo!* claiming that her copyrighted photographs were posted on a web site hosted by the defendant. She requested production of all voice mail, electronic mail, web sites, web pages and other electronic data relevant to the action. *Yahoo!* refused to produce this information, and the trial court granted the plaintiff's motion to compel discovery, stating that:

> Federal Rule of Civil Procedure 26(a)(1)(C) requires a party to provide other parties "a copy of, or

a description by category and location of, all documents, data compilations, and tangible things in the possession, custody, or control of the party that are relevant to disputed facts alleged with particularity in the pleadings.

> ****
>
> As used by the advisory committee, "computerized data and other electronically-recorded information"includes, but is not limited to: voice mail messages and files, back-up voice mail files, e-mail messages and files, backup e-mail files, deleted e-mails, data files, program files, backup and archival tapes, temporary files, system history files, web site information stored in textual, graphical or audio format, web site log files, cache files, cookies, and other electronically-recorded information. . . . The disclosing party shall take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any "deleted" electronic data.

Id. at 4.

The Court further cited the following discussion from a periodical concerning the retrieval of deleted electronic data:

> Back-up copies of files may be available as a result of formal or informal preservation of information. Formally, companies often make timed backed-ups of all of the information stored on a computer network at given points. These archival tapes may be preserved for short periods of time as a source of memory in the event of an emergency such as accidental deletion or loss of important data. Subsequently, such tapes may be recycled for further archiving or other use. Archival tapes may also be preserved for longer periods of time either because of government-mandated recordkeeping requirements or simply for purposes of historical preservation. Informally, employees may make their own random back-up copies of files to guard against accidental deletion or system failure. These back-ups may employ different file names. Indeed, different versions of evolving documents may be saved under different file names. Consequently, there are several sources for retrieving deleted documents or drafts of documents. Archival tapes may contain final versions and drafts of documents that were subsequently deleted from the hard disk on the computer

> terminal or network file server. Similarly, copies or drafts of deleted documents may still be found on the hard disk of a computer terminal or network file server under different file names than the file that was deleted." Mark D. Robins, *Computers and Discovery of Evidence-A New Dimension to Civil Procedure*, 17 J.Marshall J. Computer & Info.L.411, 416-17(1999).

Id. at 4-5 n.7.

Malone v. Ford Motor Company, 29 Va. Cir. 456 (1992). In response to the plaintiff's request for production of documents, defendant Ford Motor Company produced over 15,000 documents. The plaintiff filed a motion to compel, alleging that Ford had a computerized data base of all documents supplied and not supplied to the plaintiffs and seeking an order compelling Ford to produce a usable copy of the data base along with the coding needed to use the data base. The Trial Court denied this motion, finding that the data base contained codes, descriptions and analyses, including the mental impressions, opinions and conclusions of Ford's attorneys. The fact that data contained in the data base could be manipulated by the use of codes or commands to exclude such impressions and opinions from production did not render the remaining material discoverable. The Court acknowledged that the use of individual paper documents would be more time consuming than an electronic retrieval system, but stated that: " because trial preparation may be made more difficult does not equate to hardship . . . ."

The Court further rejected the plaintiff's argument that production of the data base and codes was necessary in order to gauge the sufficiency of the defendant's discovery response, citing, with approval, the statement by the Court in *Lawyers Title Insurance Corp. v. U.S. Fidelity and Guaranty Co.*, 122 F.R.D. 567, 570 (N.D. Cal.1988):

> The mere possibility that a party might not produce all relevant, unprotected documents, is not a sufficient basis for ordering such a party to disclose its entire computerized system of information management. Nor should the possibility that a lawyer could better frame his discovery requests serve as a sufficient predicate for ordering disclosure of proprietary information about a computer system.

Id. at 458.

Santiago v. Miles, 121 F.R.D. 636 (W.D.N.Y 1988). The plaintiffs

filed a discrimination action against a state correctional facility. In discovery, they sought computer generated documents showing the ethnicity of inmates at various facilities. The defendants resisted discovery of these documents, claiming that the printouts were produced from a computer program developed by counsel and another government employee in response to the filing of the lawsuit. The Court refused to order production, characterizing the printout as work product. The Court observed that the computer could be programmed to generate the raw data only and that a request for raw information in computer banks is proper, and the information is obtainable under the discovery rules.

Williams v. E.I. duPont DeNemours & Co., 119 F.R.D. 648 (W.D. Ky. 1987). The EEOC filed an action under Title VII of the Civil Rights of 1964 against the defendant corporation. During discovery, the EEOC discovered 30 years of the defendant's employment records and other related documents which were then converted into a computer readable database by the EEOC's expert. The expert analyzed the data and ran certain statistical tests pursuant to instructions from the EEOC's attorneys. The aggregate factual data and the expert's analysis and opinions were complied into a final report and furnished to the defendant corporation. The defendant then requested production of a copy of the computerized data base, the code book, all documents used in encoding the data base and documents relating to the program used to create the data base. The defendant contended that this discovery was necessary in order to cross- examine the EEOC's expert and to permit its own experts to analyze the data. Further, re-creation of the data base would constitute a time-consuming and expensive effort. The Court agreed that to encode manually the massive documentation originally afforded to the EEOC would constitute an undue hardship. The Court held that the defendant could not discover documents relating to the programs used to create the data base or the program itself, but could, at its own expense, discover copies of the computerized data base in the form of the computer storage disk, the code books, the user's manual and all documents used in encoding the data base. The Court also ordered the defendant to pay to the EEOC a fair portion of the fees and expenses incurred for the work of the expert in encoding the requested data and formulating the data base.

In re General Instrument Corporation Securities Litigation, 1999 WL 1072507 (N.D. Ill.1999). In this class action securities litigation, the plaintiffs sought to compel the production of e-mail documents and other computer-generated evidence. In response to the plaintiff's request, the defendant produced more than 110,000 pages of documents including thousands of pages of e-mail.

However, the defendant restricted its production to a one year time period and to e-mail generated by seven employees. The plaintiffs sought production of additional documents relating to a broader time period. The defendant argued that the production of more documents would be of little value to the plaintiffs given the enormous number of documents already in their possession. The plaintiff contended that retrieving the e-mail from back-up tapes is not unduly burdensome and produced an affidavit from their forensic computer expert that the e-mails could be retrieved from the back-up tapes with far less time and expense than what the defendants claimed would be necessary.

The Court held that discovery may be limited if the Court determines that the burden or expense of the proposed discovery outweighs its likely benefit. The Court found that the likely benefit of the requested discovery was minimal. Given the large number of documents already produced, it was unlikely that additional documents were necessary, and the plaintiffs had not identified any specific factual issues on which additional discovery would help them. The Court also found that, while the requested documents could be retrieved from the back-up tapes without undue expense, that would just be the start of the process. Defense counsel would then have to read each e-mail, assess whether the e-mail was responsive, and then determine whether the e-mail contained privileged information. The burden of reviewing the requested documents would be heavy and would distract counsel's energy from other parts of the on-going litigation. Therefore, the plaintiffs motion to compel discovery was denied.

Public Citizen, Inc. v. Carlin, 2 F. Supp. 2d 1, 13-14 (D.D.C. 1997), *rev'd*, 184 F. 3d 900 (D.C. Cir., 1999). In response to an argument that electronic versions of records are merely copies of the paper records, the Court stated that: ". . .electronic communications are rarely identical to their paper counterparts; they are records unique and distinct from printed versions of the same records."

III. WHO SHOULD PAY THE COSTS OF THE DISCOVERY?

Bills v. Kennecott Corporation, 108 F.R.D. 459 (D.Utah 1985). In an age discrimination action, the plaintiff sought production of documents containing detailed information regarding numerous

employees of the defendant. The defendant offered to supply the plaintiffs with either a computer tape or a printout of the computer data, but only on the condition that the plaintiffs pay the cost to generate the information. When the plaintiffs refused to pay this cost, the defendant produced the data and then moved the court for an order requiring the plaintiffs to pay $5,000.00. The Court stated:

> It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil Procedure if it otherwise meets the relevancy standard prescribed by the rules, although there may be issues in particular cases as to the form of what must be produced . . . . Indeed, some courts have required the responding parties to develop programs to extract the requested information and to assist the requesting party in reading and interpreting information stored on computer tape. See, e.g. National Union Electric Co. v. Matsushita Electric Industrial Co., 494 F. Supp. 1257 (E.D. Pa. 1980). Depending on the type of case, a Court might even permit discovery of computer capabilities and capacities. See Dunn v. Midwestern Indemnity, 88 F.R.D. 191 (S.D. Ohio 1980). The Federal Judicial center has recognized the challenge presented to discovery processes in the computer age:
>
> > In many instances it will be essential for the discovering party to know the underlying theory and the procedures employed in preparing and storing the machine-readable records. When this is true, litigants should be allowed to discover any material relating to the record holders computer hardware, the programming techniques employed in connection with the relevant data, the principles governing the structure of the stored data, and the operation of the data processing system. . . . Manual for Complex Litigation ¶ 2.715, at 75 (1977).
>
> Additionally, a requesting party need not accept only data that exists in traditional forms, but may discover the same information when it is electronically stored in a computer. See, e.g., Adams v. Dan River Mills, Inc., 54 F.R.D. 220 (W.D. Va. 1972). Such information clearly falls within the scope of Rule 34, and is often more accurate and less expensive to produce than documents kept in manual record keeping systems.

****

> Although parties in the past have been able sometimes to shift the majority of the costs of document production to the requesting party merely by making records available for inspection, that cost-shifting tactic is less available and less necessary when the information is stored in computers. Parties are hesitant to open up their computer banks for inspection pursuant to discovery requests, and such a process currently is impracticable because of the myriad of types of computers and the lack of expertise on the part of parties and their lawyers in computer technology and data processing. As a result, the requested party most often has no reasonable choice other than to produce the documentation in a comprehensible form by the use of its own computer technicians.
>
> Improvements in technology which advantage almost everyone have become commonplace and widespread, and because we live in a society which emphasizes both computer technology and litigation, the mix of computers and lawsuits is ever increasing. Accordingly, parties requested to produce computer stored data will have to shoulder the burden of showing "undue" expense or burden before courts should shift the cost to the requesting party.

Id. at 461-62.

In determining whether the burden placed on the defendant was "undue," the Court considered the following factors: (1) whether the amount of money involved was excessive or inordinate; (2) whether the relative expense and burden in obtaining the data would be substantially greater to the requesting party as compared with the responding party; (3) whether the amount of money required to obtain the data as set forth by defendant would be a substantial burden to plaintiffs; (4) and whether the responding party is benefitted in its case to some degree by producing the data in question. *Id.* at 464. The Court concluded that, in this case, the cost of production should not be shifted to the plaintiffs.

Anti-Monopoly, Inc. v. Hasboro, Inc., 1995 WL 649934 (S.D.N.Y. 1995). The defendant sought sales and discount information from the defendant. The defendant produced "hard copy "reports generated

for use by its management, which provided the data in aggregate forms, broken down by item, customer, year or month. The electronic versions of these reports no longer existed. Nevertheless, the plaintiff asked the court to require the defendant to create electronic versions of each and every invoice and credit memo generated by the defendant over a four year period.

The Court stated that:

> The law is clear that data in computerized form is discoverable even if paper “hard copies” of the information have been produced, and that the producing party can be required to design a computer program to extract the data from its computerized business records, subject to the Court’s discretion as to the allocation of the cost of designing such a computer program.

Id at 1.

In this case, however, the Court concluded that it did not have sufficient information as to the plaintiff’s need for electronic invoices in light of other available discovery data or of the real cost to defendants to create a program to collect that data. The Court therefore ask the parties to continue discussions.

IV. WHAT IF ELECTRONICALLY-STORED INFORMATION IS DESTROYED BEFORE PRODUCTION?

Proctor & Gamble Company v. Haugen, 179 F.R.D. 622 (D.Utah 1998), *aff’d in part, rev’d in part*, 222 F.3d 1262 (10th Cir. 2000) The plaintiff corporation failed to save all of its e-mail communications during the pendency of the litigation and failed to search or save the e-mail communications of five key employees. The defendant therefore sought discovery sanctions against the plaintiff. The Court stated that it had the power to impose sanctions against a litigant who is on notice that documents and information in its possession are relevant to litigation or potential litigation, and destroys such documents and information. However, the Court could not determine that the plaintiff acted in bad fath because no discovery order was in effect at the time of destruction of the e-mail communication. The Court therefore refused to apply the evidentiary document of spoliation, which provides that the bad faith destruction of a document relevant to proof of an issue at trial gives rise to an inference that production of the document would have been unfavorable to the party

responsible for its destruction.

The Court held, however, that the plaintiff's failure to search or preserve the e-mail communications of five individuals that it had identified as having relevant information constituted a sanctionable breach of its discovery duties. The company's own identification of these individuals in its pre-trial disclosures belied any claim that it was not on notice that their e-mail communications would be relevant. The Court imposed a monetary sanction of $10,000.00 for this conduct.

William T. Thompson Company v. General Nutrition Corporation, 593 F.Supp. 1443 (C.D. Cal.1984). The plaintiff filed an anti-trust action against the defendant and served a request for production of documents within a few weeks after the filing. Sometime after the case was filed the defendant destroyed electronically-recorded computer records pertaining to its inventory and sales. The defendant did not instruct its employees to preserve these records, nor did it take any steps to insure the preservation of the records. The Court held that the erasure of computer tapes and disks which could have been utilized to store information reflected bad faith on the part of the defendant and entered default against the defendant.

Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999). Playboy sued a former Playmate of the Year for trademark infringement and unfair competition, alleging that the defendant used the Playboy trademark on her own web site. Playboy requested production of the defendant's e-mail communications. The defendant responded that it was her custom and practice to delete electronic e-mail soon after it was sent or received. Playboy requested access to the defendant's personal computer hard drive to make a mirror image of the hard drive and then have the defense counsel review the recovered e-mails to produce relevant and responsive documents.

The Court confirmed that the description of "document" in Rule 34 included electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can, as a practical matter, be made useable by the discovering party only through the respondent's devices, the respondent may be required to use his devices to translate the data into useable form. The Court found that by requesting "documents," the plaintiff also effectively requested production of information stored in electronic form. Had the defendant printed any of the relevant e-mails, these would have been produced as a "document." Playboy need to access the hard drive of the defendant's computer only because her actions in deleting those e-mails made it

impossible to produce the information as a paper document.

The Court found that the e-mails could reflect knowledge that she knew her contract with Playboy required her to obtain written approval before she could use the “Playmate of the Year” designation and could also negate her emotional distress claim because they could indicate her state of mind regarding issues addressed in the lawsuit. The Court acknowledged the defendant’s contention that her business would suffer financial losses due to the 4 to 8 hour shut down required to recover information from the hard drive and that the hard drive could contain e-mail messages between her and her attorneys that were protected by the attorney-client privilege. The Court determined that the need for the requested information outweighed the burden on the defendant. The Court ordered that an outside expert retained to produce the mirror image of the hard drive would be required to sign a protective order and would be acting as an officer of the court. Further, the Court ordered Playboy to pay the cost associated with the information recovery. However, the Court found that the down time for the defendant’s computer would result in a minimal business interruption.

The Court appointed a computer specialist, and specifically provided that his access to information protected by the attorney-client privilege would not result in a waiver of the privilege. The computer expert would make a mirror image of the defendant’s hard drive and give it to the defendant’s counsel. The defendant’s counsel was then ordered to print and review any recovered documents and produce to the plaintiff those communications that were responsive to any request for production. All documents withheld on a claim of privilege were to be recorded in a privileged log.

Samuels v. Mitchell, 1995 WL 936327 (N.D.Cal. 1995). In this securities fraud litigation, the plaintiff sought discovery of e-mail messages in the defendant’s system for a two year period of time. The defendant explained that e-mail system was set up to notify users that messages that were over 90 days old would be moved to a computer storage unit called a “ waste basket.” Unless the user acted to preserve certain e-mails stored in the “waste basket”, they would be destroyed. The purpose of this deletion from the system or destruction was to create more storage space. The Court found that the system was used properly and not to willfully destroy evidence. The Court therefore denied the plaintiff’s motion for sanctions. The defendant stated that some of the deleted e-mails could be located on quarterly back- up tapes. The Court stated that if these messages were on these tapes, they should be produced.

Lauren Corp. v. Century Geophysical Corp., 953 P. 2d 200 (Colo. Ct. App. 1998). The plaintiff sought to inspect the defendant's computers for evidence to support its claim that the defendant had unlawfully used the plaintiff's licensed software. The Court compelled inspection of the computers, but the defendant disclosed that it had disposed of some of this hardware in the interim. The Court sanctioned the defendant for this destruction by creating a presumption at trial that the defendant had used the software in violation of the plaintiff's license.

Fennell v. First Step Designs, Ltd., 83 F. 3d 526 (1st Cir. 1996). A discharged employee brought an action against her former employer alleging that she was fired in retaliation for making a sexual harassment claim. The plaintiff sought discovery of information in the defendant's computer files pertaining to the timing of a particular memorandum. The plaintiff claimed that the memorandum was fabricated after she reported the harassment, though dated prior to her report. The employer produced a diskette containing a copy of the word processing file of the memo. The plaintiff's computer expert stated that this file showed that the document was "autodated" and therefore the creation date could not be determined. He proposed that the original date of creation could be determined by review if the file as it resided on the employer's hard drive. The employer's computer consultant stated, however, that the system could not reveal the creation. The First Circuit affirmed the Trial Court's refusal to permit the plaintiff to inspect the hard drive, holding that the plaintiff had not sufficiently set forth a plausible basis for believing that specified facts, susceptible of collection within a reasonable time frame, probably exist. The most that the plaintiff's expert could say was that "there may be a way" to determine the date. Whether the "autodating" indicated an intentional conspiracy to cover up the document's fabrication by obliterating the actual creation date was mere speculation.

Strasser v. Yalamanchi, 669 So. 2d 1142 (Fla. Dist. Ct. App. 1996). The plaintiff requested an inspection of the defendant's computer system to search for financial information that the defendant claimed was purged. The Court acknowledged that the information was within the scope of the discovery rules, but that the request was overly broad. On the basis of expert testimony, the Court found that it was unlikely that the purged information could be retrieved. The Court further stated that the plaintiff would have unfettered access to the defendant's entire computer system, including confidential information pertaining to the defendant's patients, and that such broad access could cause irreparable harm.

In re Brand Name Prescription Drugs Antitrust Litigation, 1998 WL 474146 (N.D. Ill. 1998). In a complex price-fixing case, the Court required the defendant to produce electronically stored information, even thought it meant turning over approximately thirty million pages of electronic mail at a cost of $70,000.00. The Court balanced the burden on the defendant against the plaintiffs' entitlement to the production of such documents, and concluded that the plaintiffs need not bear the costs caused by the defendant's choice of electronic storage. If a party chooses to store information electronically, it should recognize the need for a retrieval program.

COMPUTER FORENSIC EXPERTS

Derek Pierce
Innovative Techs
721 Edinbrugh Court
Burlington, NC 27215
Phone: (336) 684-0090
E-Mail: Derek@innovativetechs.com

Center for Computer Forensics
7512 East Independence Blvd., Suite 100
Charlotte, NC 28227
Phone: (888) 458-3222
Website: www.computer-forensics.net

Computer Forensics, Inc.
1749 Dexter Avenue North
Seattle, WA 98109
Phone: (206) 324-6232
E-Mail: cfi@forensics.com
Website: www.forensics.com

Computer Forensics Specialists
P.O. Box 177081
Irving, TX 75017-7081
Phone: (972) 785-2000

Website: www.contactcfs.com

New Technologies, Inc.
2075 NE Division Street
Gresham, OR 97030
Phone: (503) 661-6912
Website: www.forensics-intl.com