

Annotated Case Law and Further Reading on Electronic Discovery

Kenneth J. Withers

Updated August 1, 2004

I. Annotated Case Law

A. *Data Preservation and Spoliation*

Anderson v. Crossroads Capital Partners, No. Civ. 01-2000 ADMISRN, 2004 WL 256512 (D. Minn. Feb. 10, 2004). In a sexual harassment and whistle-blower suit, the defendant requested and obtained access to the plaintiff's personal computer. The defendant's examining expert reported that the hard drive found in the plaintiff's computer had been manufactured more than two years after the alleged events and that the plaintiff had recently installed and used a file-wiping program called "CyberScrub." In response, the plaintiff claimed that she had been using the same computer throughout the litigation, despite changing the hard drive, and disclaimed any intent to use CyberScrub to destroy potential evidence. The judge found that although the plaintiff's "exceedingly tedious and disingenuous claim of naïveté . . . defies the bounds of reason," her behavior was not egregious enough to warrant dismissal of the case. The court instead would give the jury an adverse-inference instruction during trial.

Arista Records, Inc. v. Sakfield Holding Co. S.L., No. CIV.A.03-1474 (RCL), 2004 WL 881851 (D.D.C. April 22, 2004). In a copyright infringement suit brought by a record company against a Web site owner for maintaining a Web site from which subscribers could download copyrighted music, the central question was jurisdiction. The court ordered discovery limited to the jurisdictional issues, particularly discovery of the Internet servers that would presumably contain copies of the copyrighted works, Internet transaction histories, and subscriber information. When the plaintiffs' expert examined these servers, he found that the defendant had intentionally destroyed most of the data by running a "data wiping" program fifty times from a remote location after receiving notice of copyright claims. The court commented, "Defendant's argument that it destroyed crucial evidence to prevent further transfer of music files is without doubt one of the most ludicrous arguments ever visited upon this Court in written form. Defendant could have disconnected its website from the Internet in any number of ways without destroying one single file. [footnote omitted] The Court will not at this time impose any particular sanctions as a result of these actions but instead grants plaintiffs the right to file appropriate motions for sanctions or otherwise in the future." On the jurisdictional issue, the court accepted the plaintiffs' expert's extrapolation from the fragmentary data recovered that approximately 241 users in the District

of Columbia had downloaded approximately 20,000 copyrighted musical works, commenting that the “defendant is in a poor position to attack plaintiffs’ evidence. But for defendant’s destruction of crucial evidence on the servers, plaintiffs would not have had to resort to such methods of analysis. Destruction of evidence raises the presumption that disclosure of the materials would be damaging. . . . The Court finds the data plaintiffs extracted from the computer servers more than sufficient to establish that defendant maintained continuous and systematic contacts with the District of Columbia.”

Capricorn Power Co. v. Siemens Westinghouse Power Corp., 220 F.R.D. 429 (W.D. Pa. 2004). In a liability case stemming from the failure of electric generator equipment, both the plaintiff and the defendant filed motions for data preservation orders. The court noted that the case law on the standard for issuing such orders is “scant” and that attempts to borrow the four-part test for injunctive relief are inappropriate. The court announced a new three-part test for data preservation orders. The three parts are

1. the level of concern the court has for the continuing existence and maintenance of the integrity of the evidence in question in the absence of an order directing preservation of the evidence;
2. any irreparable harm likely to result to the party seeking the preservation of evidence absent an order directing preservation; and
3. the capability of an individual, entity, or party to maintain the evidence sought to be preserved, not only as to the evidence’s original form, condition, or contents, but also as to the physical, spatial and financial burdens created by ordering evidence preservation.

Applying this new test, the court concluded that the defendant’s motion for a data preservation order was not justified or necessary. In considering the plaintiff’s counter-motion, the court noted that it read more like a motion to compel the production of documents and appeared to be a “tactical, quid pro quo” response to the defendant’s motion. Therefore it was also denied.

Danis v. USN Communications, 53 Fed. R. Serv. 3d (West) 828 (N.D. Ill. 2000). The failure to take reasonable steps to preserve data at the outset of discovery resulted in a personal fine levied against the defendant’s CEO.

GTFM v. Wal-Mart Stores, 49 Fed. R. Serv. 3d (West) 219 (S.D.N.Y. 2000). The defendant’s counsel provided inaccurate information to the plaintiffs about computer records early in discovery, and discoverable computer records were later destroyed. The court ordered the defendant to pay attorneys’ fees and costs expended to litigate the sanction motion and recover the data.

Keir v. Unumprovident Corp., No. 02 Civ. 8781 (DLC), 2003 WL 21997747 (S.D.N.Y. Aug. 22, 2003). In an ERISA class action suit, the parties agreed to a data preservation order after several conferences. The order was very narrowly drawn and concentrated on preserving six days of e-mail records on the defen-

dant's backup media and hard drives. However, the defendant's upper management did not communicate the order to its information technology (IT) staff for nearly two weeks, and most of its data management functions had been outsourced to IBM, which failed to implement the required preservation. Although the court found that the defendant's failure to preserve the data was unintentional, it criticized the defendant's poor compliance with the preservation order. The court recommended that further action be taken to determine the feasibility of retrieving the lost data to which the plaintiffs were prejudiced, in order for the court to fashion an appropriate remedy.

Landmark Legal Found. v. EPA (Landmark II), 272 F. Supp. 2d 70 (D.D.C. 2003) (Memorandum Opinion and Order dated July 24, 2003). In a civil suit stemming from a Freedom of Information Act (FOIA) request, the court issued a preliminary injunction ordering that the EPA refrain from "transporting, removing, or in any way tampering with information responsive" to the plaintiff's FOIA request. Subsequently, the hard drives of several EPA officials were reformatted, backup tapes were erased and reused, and individual e-mails were deleted. The plaintiff filed a motion for contempt. The court held that under the strict standards of Federal Rule of Civil Procedure 65, the order was clear and the data destroyed went "to the heart" of the plaintiff's claims. The court found the EPA in contempt and ordered it to pay attorneys' fees and costs, but the court declined to hold several individuals and the U.S. Attorney's Office in contempt as well. *Cf. Landmark I*, under "Records Management" at C.

Lewy v. Remington Arms Co., 836 F.2d 1104 (8th Cir. 1988). In a product liability suit alleging defective design of rifles, documents concerning past consumer complaints relevant to the suit were destroyed. The trial court issued an instruction that the jury could infer that the destroyed documents would have provided evidence against Remington (a "spoliation instruction"). Remington appealed, claiming that the document destruction was routine, pursuant to the company's three-year records retention schedule. The appeals court remanded the case back to the trial court for a determination of whether a three-year records retention schedule was reasonable in the ordinary course of business, and whether suspension of the schedule when the lawsuit was filed should have been required, whether or not the schedule was reasonable.

Linnen v. A.H. Robins Co., 10 Mass. L. Rptr. 189 (Mass. Super. Ct. June 16, 1999). Defense counsel failed to adequately investigate their client's computer records and holdings, and thereby failed to preserve relevant computer records. In the face of repeated representations before the court that no relevant records existed, the court found that a spoliation instruction to the jury was a reasonable sanction.

MasterCard International v. First National Bank of Omaha, Nos. 02 Civ. 3691 (DLC), 03 Civ. 707 (DLC) (S.D.N.Y. Feb. 23, 2004). In a trademark infringement suit, the defendant moved *in limine* to exclude the testimony of the plaintiff's ex-

pert witness on the grounds that the expert destroyed e-mail correspondence with counsel and word-processed drafts of his report. The court found that since plaintiff's counsel denied that there was any e-mail correspondence with the expert, and the defendant produced no evidence that there ever was, the defendant had not met its burden on the first ground for exclusion. The court went on to find that the expert's draft reports had not actually been destroyed, but had been edited, overwritten, and updated over time. It also found that experts for both parties engaged in the same practice. Explicitly avoiding the question whether this practice is acceptable under Federal Rule of Civil Procedure 26(a)(2)(B), the court held that exclusion of one expert's testimony on this ground was not warranted.

MasterCard International, Inc. v. Moulton and KTM Media, Inc., No. 03 Civ. 3613, 2004 WL 1393992 (S.D.N.Y. June 22, 2004). In a trademark infringement suit against a Web site featuring a "fairly tasteless parody" of MasterCard's "Priceless" ad campaign, the defendants failed to take any measures to preserve e-mails until five months after the suit was filed, although the defendants were notified of their duty to preserve in a letter from the plaintiff's counsel and in a discovery request. In deposition testimony, defendant Moulton, owner of KTM Media, stated that he did not understand that he was required to preserve e-mail messages and that e-mail messages were automatically deleted from KTM Media's server after twenty-one days. MasterCard moved for spoliation sanctions. The court concluded that the missing e-mails were likely to have been relevant to MasterCard's claims and that the actions of the defendants constituted spoliation, but declined to find that Moulton and his employees acted in bad faith, "that is, for the express purpose of obstructing the litigation. They appear simply to have persevered in their normal document retention practices, in disregard of their discovery obligations. The absence of bad faith, however, does not protect the defendants from appropriate sanctions, since even simple negligence is a sufficiently culpable state of mind to justify a finding of spoliation." The court concluded that the appropriate sanction was an adverse-inference jury instruction, rather than default judgment for the plaintiff on key issues in the case.

McGuire v. Acufex Microsurgical, Inc., 175 F.R.D. 149 (D. Mass. 1997). In an employment case, the human resources director edited a word-processed report of an internal investigation after a state administrative complaint was filed but before suit was filed in federal court. While this action could be considered destruction or alteration of discoverable evidence, it was within the director's authority and not misconduct, and no harm occurred, given that an unedited version of the document was produced from another computer source. However, the facts surrounding the editing were admissible.

In re Merrill Lynch & Co. Research Reports Securities Litigation, Nos. 02-MDL 1484 (MP), 01 CV 6881 (MP); 2004 WL 305601 (S.D. N.Y. Feb. 18, 2004). In a suit under the Private Securities Litigation Reform Act (PSLRA), the plaintiffs moved for an order lifting the PSLRA's automatic stay of discovery, claiming that discovery was necessary to preserve and restore deleted e-mails. The court held

that part of the PSLRA's stay of discovery was a duty imposed on the parties to preserve all relevant evidence "as if they were the subject of a continuing request for production of documents," 15 U.S.C. § 8u-4(b)(3)(C), and therefore lifting the stay of discovery for the purpose of preserving such evidence, absent unusual circumstances, was unwarranted.

Metropolitan Opera Ass'n, Inc. v. Local 100, Hotel Employees & Restaurant Employees Int'l Union, 212 F.R.D. 178 (S.D.N.Y. 2003). Contrary to counsel's representations, the defendant had failed to conduct a reasonable investigation in response to discovery requests, failed to prevent the destruction of documents, failed to adequately instruct the person in charge of document collection, and shortly before a scheduled on-site inspection had allowed computers subject to discovery to be replaced with new computers. The court found that the defendant's behavior constituted a "combination of outrages" and ordered judgment against the defendant as well as payment of attorneys' fees.

New York State Nat'l Org. for Women v. Cuomo, No. 93 Civ. 7146 (RLC)JCF, 1998 WL 395320 (S.D.N.Y. July 14, 1998). The court held that counsel have a duty to advise their clients to take reasonable steps to preserve records subject to discovery.

In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598 (D.N.J. 1997). In a major class action suit alleging deceptive sales practices by insurance agents, the defendant agreed to suspend its usual records retention schedule for sales literature nationwide in response to a document preservation order. Each field office had a detailed records management handbook, which was updated often in the usual course of business, but the order to suspend destruction of sales literature was communicated by bulk e-mail, which was routinely ignored by the field agents. This finding and the defendant's pattern of failure to prevent unauthorized document destruction warranted a \$1 million fine and court-ordered measures to enforce the document preservation order.

The Pueblo of Laguna v. United States, No. 02-24 L, 2004 WL 542622 (Fed. Cl. Mar. 19, 2004). In one of several cases against the United States for alleged mishandling of Indian land trusts, the plaintiffs filed a motion for a document preservation order that would affect computer data as well as paper documents. The Court of Federal Claims, although an Article I court, held that it had the same scope of inherent powers as an Article III court to issue either a document preservation order or a preliminary injunction against the destruction of documents, if appropriate. The court also held that a document preservation order does not constitute an injunction, and need not meet the strict requirements for injunctive relief. However, the court also held that it should exercise its inherent powers with restraint, and require that a party seeking a preservation order demonstrate that it is necessary and not unduly burdensome. The plaintiff relied on the many acts of document destruction reported in the related *Cobell v. Norton* class action pending in the U.S. District Court for the District of Columbia to establish the need for a

protective order in this case, which the court accepted. However, the court narrowed the plaintiff's proposed document inspection, identification, and indexing protocol, and adopted instead a protocol similar to the defendant's counterproposal.

Residential Funding Corp. v. DeGeorge Financial Corp., 306 F.3d 99 (2d Cir. 2002). Remanding the trial court's denial of a spoliation instruction, the Second Circuit held that the trial judge has the discretion to consider "purposeful sluggishness" resulting in denial of access to e-mail that may include discoverable data an equivalent to spoliation for the purposes of Federal Rule of Civil Procedure Rule 37. Conduct need not be willful and need not result in the physical destruction of the evidence to be sanctionable.

Sonnino v. University of Kansas Hospital Authority, 220 F.R.D. 633 (D. Kan. 2004). In a lengthy memorandum and order dealing with a number of discovery disputes in an employment discrimination suit, the court overruled the defendant hospital's objection to an interrogatory seeking information about its computer and e-mail systems. The court also ruled that the brief, general response proffered by the defendant in a supplemental answer was inadequate, and it gave the defendant twenty days to provide a complete and full answer.

Strasser v. Yalamanchi (Strasser II), 783 So. 2d 1087 (Fla. Dist. Ct. App. 2001). While delaying discovery to obtain a protective order the appellant claimed that its computer's hard drive was damaged and had to be disposed of, under circumstances that the court found suspicious enough to allow the issue of spoliation to go to the jury. *Cf. Strasser I*, under "Scope of Electronic Discovery" at B.

Thompson v. United States, 219 F.R.D. 93 (D. Md. 2003) (Memorandum and Order dated December 12, 2003). In a suit against the Department of Housing and Urban Development, the court entered an order under Federal Rule of Civil Procedure 37(b)(2) precluding the United States from calling certain witnesses until it either answered certain outstanding requests for the production of e-mail or demonstrated to the court's satisfaction that responsive e-mail did not exist. Later, after the deadline set by the court and on the eve of trial, the United States produced approximately 80,000 responsive e-mails. The court acknowledged that electronic discovery carries burdens that may trigger Federal Rule of Civil Procedure 26(b)(2) balancing when the burdens alleged are supported by facts, but when no such facts are presented, sanctions for failure to respond to discovery requests are appropriate. In determining an appropriate sanction, the court applied a five-part test:

1. surprise to the party against whom the evidence would be entered;
2. ability of that party to cure the surprise;
3. extent of possible disruption to the trial;
4. importance of the evidence; and

5. explanation for failure to produce the evidence in discovery.

Applying these factors, the court ordered that the United States be precluded from entering any of the e-mail into evidence and that U.S. attorneys be forbidden to use any of the e-mail in preparing witnesses. The plaintiffs were allowed to use the e-mails as evidence if they so chose, and were invited to move for costs and attorneys' fees necessitated by last-minute review of the e-mails for trial. In addition, if evidence from the trial regarding the nonproduction of these e-mails justified it, the plaintiffs could move for contempt of court against the United States.

Trigon Ins. Co. v. United States, 204 F.R.D. 277 (E.D. Va. 2001). In a corporate taxpayer suit against the United States, the United States hired a litigation support firm, which in turn hired experts to act as consultants and testifying experts. The litigation support firm had a policy under which all e-mail communications with experts and draft reports were destroyed. The court held that under the facts of this case, those communications and drafts would have been discoverable, and the United States was responsible for its litigation support firm's intentional spoliation. The court found that adverse-inference instructions regarding the content of the destroyed electronic documents were warranted.

U.S. v. Philip Morris USA, No. CIV.A.99-2496, 2004 WL 1627252 (D.D.C. July 21, 2004). A blanket data preservation order was entered early in this national tobacco products litigation. However, defendant Philip Morris USA continued for at least two years its routine practice of deleting e-mail messages more than sixty days old. After discovering this apparent violation of the order, counsel for the defendant delayed informing the court about it for an additional four months. The United States moved for sanctions against the defendant. The court found that eleven of the company's highest placed officers and supervisors violated not only the court order, but also the company's stated policy for electronic records retention. The court fined the defendant \$250,000 per employee, for a total of \$2,750,000, and precluded it from calling any of the eleven employees as witnesses at trial.

Wiginton v. Ellis, No. 02 C 6832, 2003 WL 22439865 (N.D. Ill. Oct. 27, 2003). In a putative class action alleging sexual harassment, the plaintiff's counsel sent a detailed, four-page letter to the defendant's general counsel, requesting that the defendant halt all destruction of potential paper and electronic evidence. Several months later the parties agreed to a joint data preservation order, which was endorsed by the court. However, prior to the entry of the order, the defendant followed its routine document management program, which resulted in the destruction of some e-mail backup tapes and employee computer hard drives, including the computer hard drive of the plaintiff's former supervisor. The plaintiff filed a motion for sanctions for spoliation and a blanket data preservation order going forward. The magistrate judge held that the plaintiff's initial letter did not, in itself, trigger any duty to preserve evidence or even a duty to respond, but served to inform the defendant of the possible scope of preservation necessary, which was beyond the action taken by the general counsel at the time. The judge heard evi-

dence on the nature and extent of the defendant's IT system and the cost of routine backups, and took note of the fact that backups were designed for disaster recovery purposes only. However, the judge held that simple assertions of burden and cost do not excuse "complete failure to perform any search" and constitute "willful blindness." Therefore, the judge found that the defendant "willfully and intentionally" violated the duty to preserve evidence. Turning to sanctions, the judge did not find the requisite degree of bad faith or fault to support a sanction of default. On the lesser possible sanction of a spoliation-inference instruction, the judge recommended that the motion be denied without prejudice, pending further investigation of the extent and nature of the data loss.

Wm. T. Thompson Co. v. General Nutrition Corp., 593 F. Supp. 1443 (C.D. Cal. 1984). The court entered default against the defendant for destroying computer records subject to discovery.

Zubulake v. UBS Warburg (Zubulake V), No. 02 Civ. 1243, 2004 U.S. Dist. LEXIS 13574 (S.D.N.Y. July 20, 2004). In this opinion, the fifth published in this employment discrimination lawsuit, the court considered the plaintiff's motion for sanctions against defendant UBS Warburg for deleting e-mails the plaintiff claimed would support her allegations of sex discrimination. The motion was based on information obtained through depositions of key UBS employees, which were ordered by the court in *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 92 Fair Empl. Prac. Cas. (BNA) 1539 (S.D.N.Y. 2003) (Opinion and Order dated October 22, 2003), to ascertain the nature of data the court ordered restored from backup media in *Zubulake v. UBS Warburg LLC (Zubulake III)*, 216 F.R.D. 280 (S.D.N.Y. 2003) (Opinion and Order dated July 24, 2003). The court found that contrary to instructions from both outside counsel and in-house lawyers, certain UBS employees deleted relevant e-mails. UBS counsel failed to conduct an adequate search for relevant electronic information from at least one key employee and failed to preserve backup tapes from which the deleted e-mails could have been recovered. Citing both a duty to preserve relevant evidence and a duty on the part of counsel to communicate discovery obligations effectively to clients and institute an appropriate "litigation hold," the court held that an adverse-inference jury instruction and an award of costs were appropriate, based on the apparent willful misconduct of certain UBS employees in destroying the e-mails. In a footnote, the court stressed that the sanctions were not based on the negligent failure to preserve the backup tapes, but if the backup tapes had been preserved and the missing e-mails recovered from them, the damage to the plaintiff would have been mitigated.

B. *Scope of Electronic Discovery*

Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV.2120 (LMM) (AJP), 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995). The court held that "[i]t is black letter law that computerized data is discoverable."

Bethea v. Comcast, 218 F.R.D. 328 (D.D.C. 2003). In an employment discrimination suit, the defendant stated that after making a diligent search, it had no documents responsive to one of the plaintiff's requests for production. Stating that it "[found] this assertion incredulous," the plaintiff moved to allow inspection of the defendant's computer system and copying of relevant documents. The court denied the plaintiff's motion, as it was not supported by any evidence, or even allegation, that the defendant had not produced all the responsive information in its custody, and was based instead on a vague assertion that a "qualified person" may have been able to retrieve additional responsive information from the computers.

Byers v. Ill. State Police, 53 Fed. R. Serv. 3d (West) 740 (N.D. Ill. June 3, 2002). The plaintiffs in a sex discrimination case requested discovery of e-mail backup tapes going back eight years. Citing *Rowe* and *McPeck*, among other cases, the court narrowed the request and ordered the plaintiffs to assume the cost of restoring the data, including obtaining the necessary software license.

Cumis Insurance Co. v. Diebold, Inc., No. Civ.A.02-7346, 2004 WL 1126173 (E.D. Pa. May 20, 2004). In an insurance recovery action against an armored car operator stemming from the misappropriation of funds intended to be used to replenish the cash of the insured credit union's ATM machines, the court ordered the defendant to produce requested computer data. The court briefly touched on the relative burdens of the parties in discovery—the requesting party's burden of demonstrating relevance, and the responding party's burden of demonstrating why the requested discovery should not be permitted. The requesting party in this case went beyond showing relevance and countered the defendant's argument that it had already produced all relevant computer data, by bringing into court relevant electronic documents and e-mails of the defendant, obtained from other sources, that the defendant had not produced.

Fennell v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996). The court held that discovery of a computer hard drive is not justified by mere supposition that relevant evidence might be found on it.

In re Ford Motor Co., 345 F.3d 1315 (11th Cir. 2003). In a design-defect suit against Ford Motor Co., the district court granted the plaintiff's motion to compel direct access to Ford's extensive dealer and customer contact databases without a hearing and before Ford had responded to the motion. Granting a writ of mandamus to vacate the district court's discovery order, the court of appeals held that Federal Rule of Civil Procedure 34(a) allows the requesting party to inspect and copy data "resulting from the respondent's translation of data into reasonably useable form." This rule allows the respondent to search its records to produce the requested information, but does not normally allow the requesting party to perform the search itself. Absent any finding by the district court that Ford had failed to comply with the original discovery request, or any discussion of Ford's objections to the requested discovery, or any protocols or limits on the scope of the search, the appeals court found that the district court had abused its discretion.

Marcin Eng'g, L.L.C. v. Founders at Grizzly Ranch, L.L.C., 219 F.R.D. 516 (D. Colo. 2003). In a construction-engineering suit, the defendant's motion for an extension of time for discovery of the plaintiff expert's computer drafts and preliminary work was denied, as the motion came five days before the deadline for expert disclosure and the defendants had delayed reviewing paper materials originally produced for them for five months. Delay and carelessness in requesting electronic discovery are not compatible with the showings of diligence and good cause necessary to extend discovery deadlines or delay summary judgment under Federal Rule of Civil Procedure 56(f). Furthermore, the defendant had been repeatedly advised by the court that its proposed discovery, "when considered in the light of the amounts claimed as damages, made no economic sense."

McPeek v. Ashcroft (McPeek I), 202 F.R.D. 31 (D.D.C. 2001). The court found that retrieval of specific records from computer backup tapes was not within the ordinary and foreseeable course of business, but ordered the restoration of a small sample of the backup tapes to determine whether the backup tapes contained relevant discoverable information not available from any other source.

McPeek v. Ashcroft (McPeek II), 212 F.R.D. 33 (D.D.C. 2003). Following up on a previous ruling in the same case, the court held that after ordering the "sampling" of a large collection of backup tapes, the resulting data supported further discovery of only one of the tapes. The opinion includes a detailed description of the sampling methods used to reach the conclusion.

Medical Billing Consultants, Inc. v. Intelligent Medical Objects, Inc., No. 01 C 9148, 2003 WL 1809465 (N.D. Ill. April 4, 2003) (Memorandum Opinion and Order dated April 4, 2003). In a copyright and trade secret appropriation case, the defendants moved to allow on-site inspection of the plaintiff's computers. The court held that absent any showing that the plaintiff's disclosures and responses to prior requests were inadequate or that more evidence was likely to be discovered, the request would be denied as unduly burdensome.

Stallings-Daniel v. Northern Trust Co., 52 Fed. R. Serv. 3d (West) 1406 (N.D. Ill. 2002). In line with *Fennell*, the court denied the plaintiff's motion for wide-ranging discovery of the defendant's e-mail system based solely on the allegation that the defendant had mishandled e-mail production in a previous, unrelated case.

Strasser v. Yalamanchi (Strasser I), 669 So. 2d 1142 (Fla. Dist. Ct. App. 1996). Access to a computer hard drive for the purposes of discovery was denied when the requesting party could not demonstrate the likelihood of retrieving purged information and could not show that access was the least intrusive way to acquire information. *Cf. Strasser II*, under "Data Preservation and Spoliation" at A.

Wright v. AmSouth Bancorporation, 320 F.3d 1198 (11th Cir. 2003). In a very brief opinion, the Eleventh Circuit held that the trial court did not abuse its discretion when it held that the plaintiff's request for discovery of "computer diskette

or tape copy of all word processing files created, modified and/or accessed by, or on behalf” of five employees of the defendant over a two-and-one-half-year period was not reasonably related to the plaintiff’s age discrimination claims, and was overly broad and unduly burdensome.

C. *Records Management*

In re Cheyenne Software, Inc., Securities Litig., No. CV-94-2771(NG), 1997 WL 714891 (E.D.N.Y. Aug. 18, 1977). The court held that routine recycling of computer storage media must be halted during discovery, when that is the most reasonable means of preserving available data.

Heveafil Sdn. Bhd. v. United States, Nos. 02-1085, 02-1086, 02-1087, 2003 WL 1466193 (Fed. Cir. March 19, 2003) (order not to be cited as precedent). The Federal Circuit affirmed the judgment of the U.S. Court of International Trade in refusing to admit into evidence computerized business records that, in the trial court’s view, were “at best, an unauthenticated duplicate of a database which may have been generated in the ordinary course of business.” The Federal Circuit explained that the manufacturer “did not produce evidence explaining how the copy was made, such as an affidavit by an employee with pertinent knowledge verifying the accuracy of the database,” and that key source documentation was not retained.

Kozlowski v. Sears, Roebuck & Co., 73 F.R.D. 73 (D. Mass. 1976). In the days before computers, Sears, Roebuck recorded all customer complaints about products on index cards, which were organized by the name of the complainant and with no cross-indexing, making it almost impossible to search the vast collection for complaints about the same or similar products. When Sears was sued for selling children’s pajamas made from highly flammable fabric, it argued that discovery of all complaints about flammable pajamas would be unduly burdensome and therefore should not be allowed. The court held that Sears was under an obligation to answer the discovery request, stating that “to allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules.” 73 F.R.D. at 76.

Landmark Legal Found. v. EPA (Landmark I), 272 F. Supp. 2d (D.D.C. 2003) (Memorandum Opinion dated July 24, 2003). After news articles appeared nationally claiming that the Environmental Protection Agency (EPA) was trying to push through regulations before the Bush administration took office, the plaintiffs filed a Freedom of Information Act (FOIA) request seeking records about the EPA’s rule-making activities in the months before January 20, 2001. Dissatisfied with the response to the FOIA request, the plaintiffs filed suit. In particular, the plaintiffs claimed that the EPA violated FOIA by not maintaining agency e-mail in a central file in “readily reproducible” form. The court disagreed, holding that the EPA practice of printing out e-mail and filing it in various files by subject

matter was a reasonable practice and did not violate FOIA. In addition, the court held that the EPA's search for responsive documents was reasonable and adequate, and that the plaintiff cannot require a particular search methodology in its FOIA request. Finally, the plaintiff complained that the EPA had destroyed documents subject to its FOIA request. The court held that although this was troubling, FOIA is not a records management statute, and the document destruction issue would have to be dealt with as a separate matter. *Cf. Landmark II*, under "Data Preservation and Spoliation" at A.

Public Citizen v. Carlin, 184 F.3d 900 (D.C. Cir. 1999). In promulgating the records management schedule known as GRS 20, the National Archivist determined that federal agency e-mail could be migrated to archival media, and once migrated, original messages left in native format on desktop computers and network servers need not be preserved. The Archivist's migration plan preserved the content of the records and all necessary information from which the provenance of the records could be determined, although the archival media selected (in this case, paper) did not allow for easy searching and sorting. The district court held that GRS 20 violated the Records Disposal Act, 44 U.S.C. § 3303a(d) (*see Public Citizen v. Carlin*, 2 F. Supp. 2d 18 (D.D.C. 1998)). On appeal, the circuit court reversed the decision, noting that the plaintiff had confused form with substance, and holding that the Archivist can reasonably "permit agencies to maintain their recordkeeping systems in the form most appropriate to the business of the agency."

Rambus, Inc. v. Infineon Technologies AG, 220 F.R.D. 264 (E.D. Va. 2004). In a complex patent infringement suit involving counterclaims of fraud, the defendant sought discovery of documents, including attorney-client communications, relating to the plaintiff's document retention program, on the theories that (1) the document retention program resulted in the intentional spoliation of relevant documents (as found by the court in a previous proceeding), and therefore the crime/fraud exception to the attorney-client privilege applied; and that (2) by disclosing details of the document retention program in discovery, the plaintiff had waived any privilege. The document retention program featured a "Shred Day," on which employees of the plaintiff were rewarded with pizza and beer after destroying an estimated 2 million pages of documents. While there were no Fourth Circuit precedents for the court to rely on, the court held that "the crime/fraud exception extends to materials or communication created for planning, or in furtherance of, spoliation." The court found that the plaintiff's document retention program was developed at approximately the same time as plans to file this lawsuit and that the plaintiff admitted that discoverability of the documents was a factor in the decision. But, the plaintiff claimed, it was motivated by the potential cost of discovery, not the desire to suppress evidence. The court held that even if the plaintiff "did not institute its policy in bad faith, if it reasonably anticipated litigation when it did so, it is guilty of spoliation." The court ordered an in camera review of the documents on the plaintiff's privilege log to determine the extent to which both the crime/fraud exception and the subject matter waiver applied.

Renda Marine, Inc. v. United States, 58 Fed. Cl. 57 (Fed. Cl. 2003). In a contract dispute filed by a marine dredging contractor against the U.S. Army Corps of Engineers (the Corps), the plaintiff moved to compel production of backup tapes and for permission to make a bitstream image of the contracting officer's computer hard drive, based on admissions by the Corps that it did not search hard drives or backup tapes to answer previous discovery requests, and by the contracting officer that he routinely deleted e-mails before and after a suit was filed. The plaintiff also requested that, as a sanction for spoliation, the Corps be ordered to pay costs associated with recovery of deleted e-mails from the backup tapes and hard drive. The Corps countered that spoliation could not be found where the Corps followed its records management program, where it did not act in bad faith, and where there was no showing that evidence relevant and material to the defendant's case had been destroyed. The court found that the Corps' records management program was inconsistent with its obligations to preserve evidence when litigation is reasonably anticipated, which in this case was two years before suit was filed. The Corps was ordered to produce the backup tapes at its own expense and to allow creation of a bitstream image of the hard drive.

D. *Form of Production*

In re Bristol-Myers Squibb Securities Litig., 205 F.R.D. 437 (D.N.J. 2002). Early in the litigation, the parties had agreed to paper production and a per-page price for photocopying. However, the defendant did not disclose that the documents had been scanned, were being "blown back" to paper form at a cost below that of photocopying, and were available in electronic form for considerably less money. The court held the parties to the agreement to produce paper, but at the lower cost of the "blow backs," and ordered that the electronic versions also be produced, at the nominal cost of duplicating compact disks. The court rejected the defendant's argument that the plaintiff contribute to the cost of scanning the documents, as that action was taken unilaterally by the defendant, who didn't inform the plaintiff, for its own purposes. Finally, the court lamented that the parties did not take the "meet and confer" obligations of Federal Rule of Civil Procedure 26(f) seriously in light of electronic discovery.

In re Honeywell Int'l, Inc. Securities Litig., No. M8-85 WHP, 2003 WL 22722961 (S.D.N.Y. Nov. 18, 2003). In a putative securities class action, the plaintiffs served a subpoena on non-party PriceWaterhouseCoopers (PWC), the defendant's auditor. PWC produced 63,500 pages of financial work papers in hard-copy form. The plaintiff moved to compel the production in electronic form, claiming that the data as produced were neither in business record order nor labeled to correspond to the categories of the request, as required by Federal Rule of Civil Procedure 34. PWC opposed the motion to compel, stating that it had produced the requested data and provided an index to assist the plaintiffs in determining how the information was organized. In addition, production of the information in electronic form would require PWC either to provide the plaintiffs with its proprietary software for accessing the information or to spend more than

\$30,000 to convert the data into nonproprietary format, an amount which the plaintiffs should pay. The court acknowledged that PWC had produced paper versions of the documents requested, but had only provided “hieroglyphic indices that render the workpapers essentially incomprehensible.” The court required that PWC produce the data in electronic form and said that PWC could avoid the \$30,000 expense by also producing the proprietary software to access the data. The plaintiffs were not competitors and a confidentiality order was already in place, so PWC’s trade-secret interests were adequately protected.

In re Lorazepam & Clorazepate Antitrust Litig., 300 F. Supp. 2d 43 (D.D.C. 2004). After discovery generated a “mountain” of electronic documents, one of the parties complained that it was owed a “meaningful and detailed document index.” The judge said, “I only have two years left in my term, and discovery ends in approximately one month,” and he ordered the parties to consult with a litigation support firm to ascertain whether the entire collection of documents could be converted into an accessible database and searched using commercially available word-searching software.

McNally Tunneling Corp. v. City of Evanston, No. 00 C 6979, 2001 WL 1568879 (N.D. Ill. Dec. 10, 2001). The court held that the defendant’s request for computer files to supplement the plaintiff’s paper production was not supported by any demonstration of need. The court noted that case law is split on whether a party is entitled to discovery in electronic form as well as paper form, citing *Williams v. Owens-Illinois*, 665 F.2d 918 (9th Cir. 1982), which denied a request for computerized data to supplement paper production, and *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94CIV.2120 (LMM) (AJP), 1995 WL 649934 (S.D.N.Y. Nov. 3, 1995), which held that a party is entitled to both hard-copy and computerized data.

Northern Crossarm Corp. v. Chemical Specialties, Inc. No. 03-C-415-C, 2004 WL 635606 (W.D. Wis. Mar. 3, 2004). The plaintiff filed a motion to compel the production of 65,000 e-mail messages in electronic form, after the defendant had produced the requested e-mail in paper form. Lamenting the fact that counsel for both sides had not met and conferred on this question before discovery took place, the court held that the plaintiff was not entitled to its preferred form of production under Rule 34. Absent a specific request for the production to be in electronic form, and absent any showing that the form chosen by the producing party constituted a “sharp tactic” or “gamesmanship,” the court refused to grant the plaintiff’s motion based only on “an unfortunate failure to communicate adequately.”

Physicians Interactive v. Lathian Sys., Inc., No. CA 03-1193-A, 2003 WL 23018270 (E.D. Va. Dec. 5, 2003). In a civil suit against alleged hackers for theft of customer lists and trade secrets, the plaintiff moved for expedited discovery to enter the sites where the defendants’ computers were located and make “mirror” or bitstream images of the hard drives. Finding that the plaintiff met the four-part test for a preliminary injunction, as well as the more specific tests for expedited discovery, the court granted the motion, with the condition that the imaging be

done by a computer forensics expert and that discovery be limited to information related to the alleged attacks.

Super Film of America, Inc. v. UCB Films, Inc., 219 F.R.D. 649 (D. Kan. 2004). In a contract dispute over the sale of \$115,000 worth of transparent film, the defendant sought discovery of e-mail, documents, databases, and spreadsheets which the plaintiff claimed were beyond its “knowledge or expertise” to retrieve and produce. The plaintiff offered to make computers available to the defendant to retrieve the requested data itself. The defendant objected the offer as an unreasonable attempt to shift discovery costs to the requesting party. The court rejected the plaintiff’s unsupported and conclusory assertion of burden and ordered the plaintiff to produce the requested data.

Zakre v. Norddeutsche Landesbank Girozentrale, No. 03 Civ. 0257 (RWS), 2004 WL 764895 (S.D.N.Y. Apr. 9, 2004). The defendant had produced over 200,000 e-mail messages on two CDs in a word-searchable electronic format. The plaintiff filed a motion to compel the additional production of “a meaningful and detailed document index.” The court held that the defendant had produced the e-mail messages “in as close a form as possible as they are kept in the usual course of business,” and would not be required to produce an index or be “further obligated to organize and label them to correspond with Zakre’s requests.”

E. *Use of Experts*

Gates Rubber Co. v. Bando Chem. Indus., Ltd., 167 F.R.D. 90 (D. Colo. 1996). When allowed direct access to the plaintiff’s computer system for the purposes of discovery, the defendant’s unqualified computer discovery expert destroyed 7% to 8% of discoverable records and compromised the evidential integrity of the rest. The court sanctioned the defendant, holding that parties to judicial proceedings have “a duty to utilize the method which would yield the most complete and accurate results” (167 F.R.D. at 112).

Playboy Enters., Inc. v. Terri Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999). To protect privilege, confidentiality, and the integrity of the evidence, the court appointed a qualified neutral expert to conduct discovery of the defendant’s computer hard drive and approved a detailed protocol for the expert to follow.

Simon Prop. Group, L.P. v. mySimon Inc., 194 F.R.D. 639 (S.D. Ind. 2000). The court adapted the *Playboy Enterprises* approach to a trademark infringement case involving the computer hard drives of several employees of the defendant. The Supplemental Entry following the Order details the protocol for the expert to follow.

Northwest Airlines v. Local 2000 Teamsters, No. 00-CV-8, 2000 WL 20881 (D. Minn. Jan. 11, 2000), discussed in Michael J. McCarthy, *Data Raid: In Airline’s Suit, PC Becomes Legal Pawn, Raising Privacy Issues*, Wall Street J., May 24,

2000, at A1. In an unreported case, the court adopted the *Playboy Enterprises* approach, but discovered that the time, costs, and intrusiveness were all greater than originally assumed.

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 51 Fed. R. Serv. 3d (West) 1106; *aff'd*, 53 Fed. R. Serv. 3d (West) 296 (S.D.N.Y. 2002). In allowing the requesting party direct access to the respondent's computer files, the court adopted a protocol in which the requesting party's expert recovered files and the requesting party's attorney reviewed them for relevance *before* the responding party reviewed them for privilege. *See also Rowe*, under "Costs and Cost Allocation" at F.

Tempo Electric Heater Corp. v. Temperature Engineering Co., No. 02 C 3572, 2004 WL 1254134 (N.D. Ill. June 3, 2004). In a suit concerning theft of trade secrets, the defendant moved for summary judgment, stating that the plaintiff had failed to produce key evidence to support its claim. In particular, the plaintiff failed to show by direct evidence that any unauthorized files existed on the defendant's computers. The court held that to overcome summary judgment, the plaintiff must produce at least circumstantial evidence that would allow a reasonable jury to draw legal inferences in its favor, by a preponderance of the evidence considered in light of the direct evidence presented by the defendant. The circumstantial evidence offered by the plaintiff was that the defendant did not return several "access keys" and proprietary programs at the end of the parties' working relationship. The direct evidence offered in rebuttal was that the defendant hired an independent service bureau to inspect all of its computers for remnants of the plaintiff's proprietary software, and the service bureau reported that none were found. The court held that the plaintiff ultimately has the burden of proof, and that mere circumstantial evidence and failure to conduct its own investigation of the defendant's computers did not meet that burden.

YCA, LLC v. Berry, No. 03 C 3116, 2004 WL 1093385 (N.D. Ill. May 7, 2004). In a lawsuit for breach of an employee non-solicitation, non-disclosure, and non-recruitment agreement, the defendant Berry moved to strike the testimony of the plaintiff YCA's computer forensics expert on the grounds that YCA had failed to identify the expert and the nature of the evidence the expert would offer in a timely manner. The expert had recovered a "plethora" of documents apparently deleted by Berry from his company-issued computer. The court denied the motion on the grounds that Berry had deliberately misled YCA during discovery by denying that he had used his company-issued computer to further his plans to establish a competing business, and that YCA, relying on Berry's representations, made a rational cost-benefit decision to not hire an expert—at a cost of between \$5,000 and \$10,000—until the close of discovery, when Berry admitted that his statements were false. The court commented, "Berry's posture with respect to [the expert's] testimony brings to mind the tale of the criminal who murders his parents and then begs the Court's mercy because he is an orphan."

F. *Costs and Cost Allocation*

In re Air Crash Disaster at Detroit Metropolitan Airport, 130 F.R.D. 634 (E.D. Mich. 1989). The cost of producing data for the requesting party in a specific format for the purposes of litigation was borne by the requesting party.

In re Brand Name Prescription Drugs Antitrust Litig., Nos. 94 C 897, MDL 997, 1995 WL 360526 (N.D. Ill. June 15, 1995). When a defendant chooses a computer-based business system, the cost of retrieving information is an ordinary and foreseeable risk.

Federal Trade Commission v. U.S. Grant Resources, LLC, No. Civ.A.04-596, 2004 WL 1396315 (E.D. La. June 18, 2004). The defendant in this civil fraud action was also defending a related criminal fraud action brought by the State of Louisiana. The defendant in this case served a subpoena under Fed. R. Civ. P. 45 for hard-copy records the state seized from it in the criminal action. The state's attorney filed a motion to quash the subpoena on the basis that it was overbroad and duplicative, and that the defendant should pay the costs of copying the documents. The federal court denied the motion, stating that although the defendant already had computer files representing the alleged fraudulent transactions, it was entitled to hard copies of its own documents held by the state, and that under the three-part test established by *In re Exxon Valdez*, 142 F.R.D. 380 (D.D.C 1992), the cost of photocopying the documents was not an undue burden that entitled the state to reimbursement, even though it was not a party to this action.

Computer Associates Int'l, Inc. v. Quest Software, Inc., 56 Fed. R. Serv. 3d (West) 401 (N.D. Ill. 2003). Plaintiffs in a software copyright and trade secret infringement case requested that the defendant image the computer hard drives of six key employees. After the imaging, the defendant spent between \$28,000 and \$40,000 to remove privileged e-mails from the backups and create a privilege log. The defendant then filed a motion to require the plaintiffs to pay these preparation costs. The court reviewed the eight *Rowe* factors, and determined that none of them favored cost shifting, analogizing these preparation costs to costs for attorney review.

Medtronic Sofamor Danek, Inc. v. Michelson, 56 Fed. R. Serv. 3d 1159 (W.D. Tenn. 2003). In an intellectual property case involving spinal fusion medical technology, the defendant sought discovery of information from 996 computer backup tapes and 300 megabytes of data on the desktop computers of the plaintiff's employees. The plaintiff objected that the proposed discovery would be unduly costly and burdensome. The court agreed and applied the eight *Rowe* factors with painstaking factual detail to determine that the defendant should shoulder most of the costs of the proposed discovery. The court then ordered an equally detailed protocol for the parties to follow in conducting discovery of the backup tapes and hard drives. Finally, the court rejected as unwarranted the defendant's request that a special master be appointed under Federal Rule of Civil Procedure

53, and instead ordered the parties to agree on a neutral computer expert to supervise discovery under the protocol.

Murphy Oil USA, Inc. v. Fluor Daniel, Inc., 52 Fed. R. Serv. 3d (West) 168 (E.D. La. 2002). Following *Rowe*, the court offered the defendant two options for proceeding with discovery of e-mail from computer hard drives and allocating costs. Under one option, the defendant could forgo prior review of e-mail recovered at the plaintiff's expense. Under the second option, the defendant could review, at its own cost, all relevant documents recovered by the expert before production to the plaintiff.

OpenTV v. Liberate Technologies, 219 F.R.D. 474 (N.D. Cal. Nov. 18, 2003) (Order Re Discovery dated November 18, 2003). In an intellectual property infringement suit, the magistrate judge ruled that a portion of the costs of producing relevant computer source code should be shifted from the responding party to the requesting party. The plaintiff had requested production of some 100 additional versions of source code for software products being developed by the defendant. The defendant objected, stating that locating and duplicating the requested source code would be unduly burdensome and would yield only marginally relevant results. Instead, the defendant offered to make its complete source code database available at its facilities, along with a complete index to the database and a software engineer to provide technical assistance. The plaintiff rejected the offer, arguing that it essentially shifted production costs to the plaintiff, the requesting party. The court agreed that the offer effectively shifted costs, yet because extracting the source code would take the defendant 125 to 150 hours, the court found that the requested electronic data were inaccessible for purposes of discovery and that cost-shifting would be appropriate. Applying the *Zubulake* factors (see *Zubulake I* in this section), the court determined that the costs for extraction should be split evenly, although the cost of duplication should be borne solely by the defendant.

Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978). The Supreme Court held that the cost of creating eight new computer programs for identifying potential class members from a responding party's computer data can reasonably be shifted to the requesting party, when the need for access to the specific data requested is not foreseeable in the normal course of business.

Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002). In an action against talent agencies, alleging racial discrimination in bookings, the plaintiffs requested e-mail from the defendants' backup media. The four defendants objected, citing the high costs estimated by electronic discovery consultants to restore the backup media to accessible form and the legal costs associated with screening them for relevance and privilege. Balancing eight factors derived from the case law, the court required that the plaintiffs pay for the recovery and production of the defendants' extensive e-mail backups, except for the cost of screening for relevance and privilege. The eight "*Rowe* factors" are

1. the specificity of the discovery request;
2. the likelihood of discovering material data;
3. the availability of those data from other sources;
4. the purposes for which the responding party maintains those data;
5. the relative benefits to the parties of obtaining those data;
6. the total costs associated with production;
7. the relative ability and incentive for each party to control its own costs;
and
8. the resources available to each party.

Xpedior Creditor Trust v. Credit Suisse First Boston (USA), Inc., No. Civ. 9149(SAS), 2003 WL 22283835 (S.D.N.Y. Oct. 2, 2003). A corporation brought a putative class action against an investment banking house, alleging breach of contract in an Initial Public Offering (IPO), and sought discovery of electronic data from two decommissioned computer systems. The defendant moved for a protective order that would shift to the plaintiff the costs of restoring the computer systems to access the data. Applying the seven-part test enunciated in *Zubulake I* (below), the judge found that the plaintiff's request was narrowly tailored, the information was not available from any other source, and the cost of the proposed restoration (\$400,000), while high, was not extraordinary in light of the total monetary stake. She also noted that the plaintiff was a bankrupt corporation with no assets and the defendant was an international firm with assets of over \$5 billion. The final factors—ability to minimize costs, public interest in the issues at stake, and the usefulness of the information to both parties—were neutral. Therefore, although the information requested was inaccessible without incurring costs, there was no justification to shift those costs to the requesting party.

Zubulake v. UBS Warburg LLC (Zubulake I), 217 F.R.D. 309 (S.D.N.Y. 2003) (Opinion and Order dated May 13, 2003). In a sex discrimination suit against a financial services company, the plaintiff requested e-mail beyond the approximately 100 pages produced by the defendants. She presented substantial evidence that more responsive e-mail existed, most likely on backup tapes and optical storage media created and maintained to meet SEC records retention requirements. The defendants objected to producing e-mail from these sources, which they estimated would cost \$175,000 exclusive of attorney review time. The judge held that the plaintiff's request was clearly relevant to her claims, but both parties raised the question of who would pay for the discovery and urged the court to apply the *Rowe* factors. The court held that for data kept in an accessible format, the usual rules of discovery apply: The responding party should pay the costs of producing responsive data. A court should consider cost shifting only when electronic data are relatively inaccessible, such as on backup tapes. Furthermore, requiring the responding party to restore and produce responsive documents from a small sample of the requested backup tapes is a sensible approach in most cases. Finally, in conducting the cost-shifting analysis, the court rejected the *Rowe* factors and sub-

stituted a seven-factor test. The “*Zubulake* factors” are, in order of importance or weight:

1. the extent to which the request is tailored to discover relevant data;
2. the availability of those data from other sources;
3. the total cost of production, relative to the amount in controversy;
4. the total cost of production, relative to the resources available to each party;
5. the relative ability and incentive for each party to control its own costs;
6. the importance of the issues at stake in the litigation; and
7. the relative benefits to the parties in obtaining those data.

Zubulake v. UBS Warburg LLC (Zubulake III), 216 F.R.D. 280 (S.D.N.Y. 2003) Opinion and Order dated July 24, 2003). Following the May 13, 2003 Opinion and Order above, the defendants restored and reviewed five backup tapes selected by the plaintiff at a cost slightly over \$19,000. Six hundred e-mail messages were deemed to be responsive to the plaintiff’s discovery request. The defendants estimated that the cost for production of the entire seventy-seven-tape collection would be \$165,954.67 for restoration and \$107,694.72 for review. Analyzing each of the seven factors announced by the court in the previous decision, the court determined that the balance tipped slightly against cost shifting, and that requiring the defendants to bear 75% of the costs would be fair. However, the court determined that none of the costs for attorney review of the data, once they had been made accessible, should be borne by the requesting party.

G. *Privacy and Privilege*

In re Currency Conversion Fee Antitrust Litig., No. MDL 1409, M 21-95, 2003 WL 22389169 (S.D.N.Y. Oct. 21, 2003). Under the “functional equivalent” exception to the corporate attorney–client privilege, the privilege is maintained even though the communications are disclosed to a third party, if that third party is the functional equivalent of a corporate employee. The court held that the exception did not apply to otherwise privileged documents processed by an outsourced computer data processing firm.

Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003). In a wrongful discharge suit, the Third Circuit Court of Appeals upheld the district court’s ruling that an employer’s search for e-mails of an employee found on the workplace computer network did not violate the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 510, 2701. Title I of the ECPA prohibits “interceptions,” which are universally defined as searches of messages during transmission, not searches of messages that have reached their destination and are being stored. Title II of the ECPA prohibits “seizure” of stored e-mails, but exempts actions taken

by the “person or entity providing the wire or electronic communications service,” in this case, the employer.

Haynes v. Kline, 298 F. Supp. 2d 1154 (D. Kan. 2003). In a suit by a former employee of the Kansas State Attorney General, the plaintiff moved for a preliminary injunction, prohibiting the Attorney General’s Office from further accessing his private files on his former work computer. The court granted the injunction, holding that the employee demonstrated a Fourth Amendment right in the privacy of his personal computer files. The court found that although the employer stated, as part of the employee orientation, that there was “no expectation of privacy in using this [computer] system,” the orientation went on to distinguish between “public” and “private” files and to warn that access to any other employee’s files without permission was forbidden. Passwords were issued to each employee to prevent unauthorized access, and prior to this litigation, there had been no evidence that any other employee’s personal computer files had been monitored or viewed by supervisors. The defendant offered no evidence to justify its search of the employee’s personal computer files. The court held that given the totality of the circumstances, the plaintiff’s expectation of privacy was both subjectively and objectively reasonable.

Holland v. GMAC Mortgage Corp., No. 03-2666-CM, 2004 WL 1534179 (D. Kan. June 30, 2004). The parties in this civil suit stipulated to a broad protective order, which they offered to the court. The order provided that categories of documents, including “computer records or other confidential electronic information” be designated as “confidential,” and that any confidential material to be filed with the court would be filed under seal. The court refused to endorse the order, stating that “[t]he mere fact that a document is a computer record or an electronic document does not warrant protection from disclosure,” and that “the fact that the parties may agree to a protective order which provides for the filing of confidential materials under seal does not dispense with the requirement that the parties establish a harm sufficient to overcome the public’s right of access to judicial records.”

Jicarilla Apache Nation v. United States, 60 Fed. Cl. 413 (Fed. Cl. 2004). In one of the many Indian land trust fund mismanagement cases, the Court of Federal Claims found that good cause existed to issue a protective order to facilitate discovery while meeting the requirements of a number of federal confidentiality laws. The complete text of the order and a list of the applicable laws are published with this decision.

Navigant Consulting, Inc. v. Wilkinson, et al., No. 3-02-CV-2186-D, 2004 U.S. Dist. LEXIS 5439 (Mar. 29, 2004). In a suit by a corporation against a group of former employees for trade secret theft, the defendants moved to compel the production of e-mails and other documents related to the corporation’s internal investigation of the defendants and other employees. The corporation objected, claiming attorney-client privilege and work product protection. Among the docu-

ments withheld was a detailed forensic analysis of one employee's laptop computer, including a printout of data contained therein. Applying Texas law, the court held that the attorney-client privilege applies only to communications "made for the purposes of facilitating the rendition of professional legal services" and does not apply when the attorney is "functioning in some other capacity—such as an accountant, investigator, or business advisor." The mere fact that the corporation was contemplating litigation did not turn the attorneys' business assistance and advice into privileged attorney-client communications.

Portis v. City of Chicago, No. 02 C 3139, 2004 WL 1535854 (N.D. Ill. July 7, 2004). In a class action suit brought by citizens who claimed unlawful detention by city police for nonviolent ordinance violations that carry no jail time, attorneys for the plaintiff class obtained approximately 20,000 relevant arrest records from the city. They proceeded to create a computerized database from the arrest records at a cost of approximately \$90,000. The city then filed a motion to compel the plaintiffs to produce the database, stating that although the database is attorney work product, it is not "opinion" work product, and that the city has a "substantial need" for the database, which it cannot re-create itself from the available information without "undue hardship." The court found that the database was a hybrid of "fact" and "opinion" work product, but that disclosure to the city would not reveal the plaintiffs' legal strategy nor counsels' mental impressions. The court went on to find that the database, as distinct from the individual arrest records, was an essential piece of evidence. The crux of the lawsuit was the claim that there was a pattern of unlawful detention, and such a pattern can only be established through computer analysis that the database would allow. The court concluded that ordering the plaintiff to share the database would advance the interests of the litigation as a whole and would not violate the attorney work product doctrine, but that the parties must split the database development costs.

United States v. Rigas, 281 F. Supp. 2d 733 (S.D.N.Y. 2003). In a criminal case involving executives of the Adelphia Communication Corporation, the government issued grand jury subpoenas to Adelphia, pursuant to which Adelphia created twenty-six bitstream images of employee computer hard drives. The imaged hard drives were installed on a secure, limited-access computer in the offices of the assistant U.S. attorney (AUSA), where they were reviewed by a paralegal employed by the AUSA. Defense counsel was then allowed to access and copy the imaged hard drives. Three weeks later, during defense counsel's review of the imaged hard drives, it was discovered that a chronology and some other files created by the AUSA paralegal had been included on the imaged hard drive. Defense counsel immediately notified the AUSA, but declined a request to return the work product, and instead tendered the files to the court pending a resolution of their status. The court held that the "middle road" approach would be taken on the issue of whether this inadvertent production constituted waiver of the work product protection. The court concluded that given the reasonableness of the precautions and security measures taken by the AUSA, the tremendous volume of information on the twenty-six imaged hard drives, the small volume of work product material

inadvertently produced, and the prompt action taken by the AUSA upon discovery of the inadvertent production, a finding that work product protection had been waived would be unfair.

United States v. Stewart, 287 F. Supp. 2d 461 (S.D.N.Y. 2003). A year before her indictment on charges related to securities fraud, but after the investigation had been made public, Martha Stewart prepared a detailed e-mail relating her side of the facts and sent it to her attorney. The next day she accessed the e-mail and forwarded it to her daughter, without alteration. Later, attorneys for Martha Stewart Living Omnimedia (MSLO) produced documents and computer files in response to a grand jury subpoena. Both e-mails appeared on MSLO's privilege log; however, only the e-mail to the attorney was removed from the actual production. An AUSA attorney later found the copy sent to the daughter. Stewart objected to MSLO's production of the e-mail on the basis that it was privileged. The court held that the e-mail to the attorney would have been privileged as attorney-client communication, but that the privilege was waived by Stewart when she forwarded the e-mail to her daughter. However, the court found that the work product protections offered by Federal Rule of Civil Procedure 26(b)(3) and Federal Rule of Criminal Procedure 16(b) are broader than the attorney-client communication privilege, and that sharing factual work product with a family member did not waive those protections.

United States Fidelity & Guar. Co. v. Braspetro Oil Servs. Co., 53 Fed. R. Serv. 3d (West) 60, No. 97 CIV.6124JGKTHK, 98 CIV.3099JGKTHK, 2002 WL 15652 (S.D.N.Y. Jan. 7, 2002). In a surety action, the defendants provided their testifying experts with more than fifty CD-ROM disks containing 1.1 million documents, including many attorney-client communications and work product documents. The plaintiffs claimed that by providing the experts with unfettered access to the entire litigation support database, the defendants had waived any privileges and were required to produce the database under Federal Rule of Civil Procedure 26(a)(2), as material "considered" by the experts. The court acknowledged that while the scope of what is "considered" by an expert is unclear in the case law, the burden is on the party resisting discovery to clearly identify for the court the material that the expert did not "consider" out of the mass provided. Finding that the defendant provided no such guidance, the court held that the entire litigation support database was discoverable, as was the index and OCR-created text files the experts used in searching the database.

New York State Bar Association, Committee on Professional Ethics, Opinion 749 (December 14, 2001), Topic: Use of computer software to surreptitiously examine and trace e-mail and other electronic documents, found at http://www.nysba.org/Content/NavigationMenu/Attorney_Resources/Ethics_Opinions/Committee_on_Professional_Ethics_Opinion_749.htm. The receipt by an attorney of an electronic file does not constitute permission to open and read the metadata or imbedded data that file might contain. Opening and viewing such data is presumptively unauthorized and unethical. Similarly, placing a tracer "bug" in an e-mail to track

the distribution and modification of the message after it has left the attorney's computer system is unethical. For a short analysis of this ethics opinion and useful links to background technical information, see David Hricik, *The Transmission and Receipt of Invisible Confidential Information*, E-Ethics, vol. 2, no. 3, October 2003, found at <http://www.hricik.com/eethics/2.3.html>.

H. *Rule 37 Sanctions (see also "Data Preservation and Spoliation," above at A)*

Aero Products International, Inc. v. Intex Recreation Corp., No. 02 C 2590, 2004 WL 417193 (N.D. Ill. Jan. 30, 2004). In a patent infringement suit involving the manufacture and sale of air mattresses, the defendant was found to have been routinely deleting all its e-mail every thirty days during the first year of the litigation. The court entered an order requiring the defendant to recover as much destroyed electronic data as possible, and authorizing the plaintiff to petition the court for appointment of a computer forensics expert at the defendant's expense. The defendant engaged its own expert, who submitted a report and forty-five pages of recovered data. The plaintiff stated that the production was inadequate, but never petitioned the court for appointment of an expert or filed any other motion to compel further production. Instead, the plaintiff filed a motion under Fed. R. Civ. P. 37 for sanctions amounting to a default judgment against the defendant. The court denied the sanctions as inappropriate and unwarranted, given the plaintiff's failure to pursue the discovery opportunities offered to it.

Invision Media Communications, Inc. v. Federal Insurance Co., No. 02 Civ. 5461 (NRB)(KNF), 2004 WL 396037 (S.D.N.Y.). In an insurance suit stemming from business disruption caused by the 9/11 attacks, the plaintiff and the defendant filed cross-motions to compel discovery and for sanctions. Two of the many incidents alleged involved electronic discovery. In the first incident, plaintiff's general counsel testified that as the company's offices were closed and employees laid off, she directed that hard drives of those employees' computers be "wiped." The defendant requested sanctions for spoliation, which were denied by the court in the absence of any showing that the wiped hard drives would have rendered relevant evidence. In the second incident, the defendant requested e-mails from a three-month period around September 2001. The plaintiff initially responded that there were no responsive e-mails, as the policy had been to delete all e-mails after two weeks. However, the e-mails were eventually found and produced. The court found that a "reasonable inquiry by the plaintiff's counsel prior to responding to Federal's document request . . . would have alerted counsel that the plaintiff possessed electronic mail that fell within the scope of Federal's document request." The plaintiff was directed to pay costs and reasonable attorneys' fees resulting from the additional discovery required.

Kucala Enters., Ltd. v. Auto Wax Co., No. 02 C 1403, 2003 WL 21230605 (N.D. Ill. May 27, 2003). In a patent infringement case, the defendant repeatedly requested documents from the plaintiff, including business records and correspondence from the plaintiff's computer system. After three motions to compel pro-

duction, the defendant was allowed access to the plaintiff's computer to conduct an inspection. The computer forensics expert conducting the inspection discovered that the plaintiff had used a commercially available disk-wiping software, "Evidence Eliminator," to "clean" approximately 3,000 files three days before the inspection, and another 12,000 on the night before the inspection between the hours of midnight and 4:00 a.m. The magistrate judge found that, based on the totality of the circumstances, the spoliation was intentional and recommended to the trial judge that the plaintiff's case be dismissed with prejudice, and that the plaintiff pay the defendant's attorneys' fees and costs from the time the Evidence Eliminator was first used. On de novo review, the district court judge rejected the recommendation to dismiss the plaintiff's case with prejudice, favoring adjudication of the claims and counterclaims, but upheld the recommendation that the plaintiff bear attorneys' fees and costs. *Kucala Enters., Ltd. v. Auto Wax Co.*, No. 02 C 1403, 2003 WL 22433095 (N.D. Ill. Oct. 27, 2003) (Rulings on Objections dated October 27, 2003).

Procter & Gamble Co. v. Haugen, 2003 WL 22080734 (D. Utah Aug. 19, 2003) (Order dated Aug. 19, 2003). *Procter & Gamble (P&G)* sued several independent distributors of rival Amway products, claiming unfair trade practices for allegedly distributing e-mail associating P&G with Satanism. P&G immediately informed the defendants of their duty to preserve computer evidence crucial to the case, but neglected to impose a similar duty upon itself, resulting in the destruction of e-mail records of five key P&G employees. Without citing Federal Rule of Civil Procedure 37, the court granted the defendant's motion to dismiss the case on three grounds, each of which the court stated were sufficient alone to grant dismissal. The three grounds were (1) the plaintiff failed to preserve evidence it knew was "critical" to the case, (2) the plaintiff's actions rendered an effective defense "basically impossible," and (3) the plaintiff destroyed the very evidence it would need to support its proposed expert testimony on damages, rendering the testimony inadmissible on *Daubert* grounds. In a previous decision, the trial court sanctioned the plaintiff \$10,000–\$2,000 for each of the five key employees whose files had been destroyed. *Procter & Gamble Co. v. Haugen*, 179 F.R.D. 622 (D. Utah 1998), *rev'd on other grounds*, 222 F.3d 1262 (10th Cir. 2000).

Sheppard v. River Valley Fitness One, 2003 F.R.D. 56 (D.N.H. 2001). The defendant attorney's failure to produce requested computer records, attributed to lack of diligence as opposed to intentional obstruction of discovery, warranted a fine of \$500 and a testimonial preclusion order.

Stevenson v. Union Pacific R. Co., 354 F.3d 739 (8th Cir. 2004). In a negligence action arising out of a railroad crossing collision, the trial court granted the plaintiffs partial summary judgment and imposed an adverse-inference instruction on the defendant as a sanction for the destruction of recorded voice communications between the train crew and dispatchers, and destruction of track maintenance records both before and after commencement of litigation. On appeal, the circuit court looked at the circumstances of each allegation of spoliation and applied the

test of *Lewy v. Remington Arms*. It held that the trial court did not abuse its discretion in imposing the adverse-inference instruction sanction for destruction of the tape recordings, as the tape recordings were clearly relevant to reasonably anticipated litigation, there were no alternative records, and there was evidence that such recordings had been preserved in other litigation. Likewise, the destruction of track maintenance records after litigation commenced warranted the sanction. However, the routine destruction of track maintenance records pursuant to a records management policy prior to litigation did not give rise to a presumption of bad faith to justify the adverse-inference instruction. And on remand, the trial court was instructed to allow the defendant to present evidence challenging the rebuttable presumption that an adverse-inference instruction creates.

Theofel v. Farey-Jones, 341 F.3d 978 (9th Cir. 2003). In a commercial lawsuit, the defendant issued a subpoena to the plaintiff's Internet Service Provider (ISP) requesting "all copies of e-mail sent or received by anyone" employed by the plaintiff, with no limitations of time or scope. The ISP, which was unrepresented by counsel, complied, producing many privileged and irrelevant messages. The plaintiff moved to have the subpoena quashed and for sanctions for discovery abuse, which the magistrate judge granted. Individual employees of the plaintiff also filed civil suits against the defendant under the Stored Communications Act, Wiretap Act, and Computer Fraud and Abuse Act, which the district court dismissed. The appellate court reversed the dismissal of the claims under the Stored Communications Act and Computer Fraud and Abuse Act, stating that although the subpoena was purported to be a valid request under Federal Rule of Civil Procedure 45, it "transparently and egregiously" violated the standards of Rule 45 and the "defendants acted in bad faith and with gross negligence in drafting and deploying it." In so ruling, the appellate court negated any argument that the ISP knowingly consented to the request. By remanding the statutory claims to the district court, the appellate court left open the possibility of civil penalties against the defendant.

Tulip Computers Int'l B.V. v. Dell Computer Corp., 52 Fed. R. Serv. 3d (West) 1420 (D. Del 2002). In a patent infringement case, defendant Dell failed several times to answer discovery requests, provide any reasonable explanations for its failures, or provide any witnesses who could answer questions about its records management systems, paper or computerized. In apparent frustration, the court granted the plaintiff's request for direct access to the respondent's records warehouse and computer data.

Zubulake v. UBS Warburg LLC (Zubulake IV), 92 Fair Empl. Prac. Cas. (BNA) 1539 (S.D.N.Y. 2003) (Opinion and Order dated October 22, 2003). [For factual background, see *Zubulake I* and *Zubulake III* under "Costs and Cost Allocation" above at F.] After restoring backup tapes to locate missing e-mails, the defendant found that certain relevant tapes were missing. The plaintiff moved for sanctions, including a spoliation-inference instruction. The court found that (a) a duty to preserve the missing tapes existed, (b) the defendant was negligent and possibly

reckless in failing to preserve the tapes, but (c) the plaintiff failed to demonstrate a reasonable likelihood that the missing tapes contained evidence that would have been relevant to the lawsuit. Had the plaintiff shown either that the defendant had acted with malicious intent or that the missing tapes actually held evidence that would have been damaging, a spoliation-inference instruction would have been appropriate. In the absence of either of those elements, the appropriate sanction was limited to awarding the costs of additional depositions taken pursuant to this discovery.

II. Further Reading

A. Web Sites

<http://www.kenwithers.com>

This Web site is maintained by Ken Withers of the Federal Judicial Center, but is unofficial. It contains articles on electronic discovery, sets of PowerPoint slides and text from judicial education and bar association seminars on electronic discovery, and additional resources.

<http://CaliforniaDiscovery.findlaw.com>

This Web site is maintained by retired California State Court Commissioner Richard Best of San Francisco, but is unofficial. It contains an exhaustive outline of electronic discovery issues.

<http://arkfeld.blogs.com/ede>

This blog is updated every few days with current case law and news developments in the field of electronic discovery and evidence. It is maintained by Arizona attorney Michael R. Arkfeld, author of *Electronic Discovery and Evidence* (Law Partner Publishing 2003).

Digital Discovery and E-Evidence

This is a monthly publication of Pike & Fischer, a division of the Bureau of National Affairs (BNA). It reports on recent cases and contains analyses by experts. Subscription information and sample articles can be found at <http://www.pf.com/digitaldisc.asp>.

Electronic discovery and computer forensics vendor sites

Of the scores of electronic discovery and computer forensics firms currently doing business in North America, a handful have developed useful educational Web sites to keep their current and prospective clients up to date on the law. These sites feature state and federal case law dealing with electronic discovery, computer forensics, and electronic evidence; “white papers” and links to leading law review articles; and sample forms for practitioners. Some good examples are the following:

- Applied Discovery
<http://www.applieddiscovery.com/lawLibrary/default.asp>
- Computer Forensics, Inc.
http://www.forensics.com/html/resource_center.html
- Cricket Technologies, Inc. (free registration required)
http://igdev.crickettechnologies.com/case_studies/search/
- Kroll Ontrack
<http://www.krollontrack.com/LawLibrary/>

B. *Handbooks and Treatises*

Michael R. Arkfeld, *Electronic Discovery and Evidence* (Law Partner Publishing 2003)

“Th[is 454-page loose-leaf] book addresses every aspect of [electronic discovery,] including electronic information storage, outside expert assistance, the inherent benefits of electronic formats, as well as the laws and procedures for admitting evidence in your case.” The book is updated annually in print and daily on a Web site, one-year access to which is included in the price of the book. For more information, see http://www.arkfeld.com/elec_summary2.htm.

Adam I. Cohen & David J. Lender, *Electronic Discovery: Law and Practice* (Aspen Publishers 2004).

A complete, well-researched guide to electronic discovery in civil litigation, both theoretical and practical, with plenty of references to relevant statutes, rules, case law, and secondary authority.

Joan E. Feldman, *Essentials of Electronic Discovery: Finding and Using Cyber Evidence* (Glasser LegalWorks 2003).

A well-organized and easy-to-read compilation of Feldman’s many contributions to the electronic discovery Continuing Legal Education circuit, with a large appendix of useful forms, checklists, and sample documents. The printed book is accompanied by a CD-ROM for copying and pasting forms into litigation documents.

Michele C.S. Lange & Kristin M. Nimsger, *Electronic Evidence and Discovery: What Every Lawyer Should Know* (American Bar Association 2004).

This American Bar Association publication is designed to provide lawyers with practical guidance in conducting electronic discovery, both as requesting parties and as responding parties. It includes analysis of emerging case law, rules and statutes; sample forms; advice on the effective selection and use of experts; and a complete bibliography of references.

The Sedona Conference, *The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (2004).

The Sedona Principles is the work product of a top-level think tank of litigators, corporate general counsel, academics, and jurists. It is designed to establish a set of working ground rules or assumptions for the conduct of electronic discovery, particularly for complex civil litigation. The book was updated in January 2004 and is available as a free download from The Sedona Conference at http://www.thesedonaconference.org/publications_html.

U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004).

Although this handbook is designed for use in criminal investigations, it is a valuable reference source for computer forensics terms and procedures that may be presented in civil litigation, where the expert recovery and analysis of otherwise inaccessible data from computer hard drives and storage media are relevant in discovery. The eighty-five-page book is available as a free download from the Department of Justice's Web site at <http://www.ojp.usdoj.gov/nij/pubs-sum/199408.htm>.

C. Recent Articles

Annual Survey of Electronic Discovery Law, 10 Rich. J. L. & Tech. 49 (Spring 2004).

This is the first instance of an academic law review devoting an entire issue to electronic discovery. It leads off with an article by Hon. David Waxse of the U.S. District Court for the District of Kansas on the relationship between mandatory disclosure under the Federal Rules of Civil Procedure and electronic discovery. The journal then presents an article by Virginia Llewellyn of Applied Discovery, Inc. on the practical aspects of electronic discovery for businesses and lawyers. Stephen Williger and Robin Wilson of the Cleveland firm of Thompson Hine LLP contribute an article on cost shifting and marginal utility analysis under the *Rowe* and *Zubulake* decisions, and Robert Brownstone of the Palo Alto firm of Fenwick and West LLP writes on the need for collaboration between opposing counsel to make electronic discovery work for all parties. The full text of the special issue is available as a free download from the journal's Web site at <http://law.richmond.edu/jolt/index.asp>.

Lisa Arent, Robert D. Brownstone & William A. Fenwick, *E-Discovery: Preserving, Requesting & Producing Electronic Information*, 19 Santa Clara Computer and High Tech. L.J. 131 (2002).

A thorough review of current case law dealing with data preservation and the scope of electronic discovery, with valuable practice tips for lawyers and advice for clients.

Mary Kay Brown & Paul D. Weiner, *Digital Dangers: A Primer on Electronic Evidence in the Wake of Enron*, 74 Pa. B.A.Q. 1 (2003).

An introduction to the fundamental technical issues, relevant rules, and case law governing electronic discovery, presented in an easy-to-follow question-and-answer format. Perfect for the novice practitioner or nervous in-house counsel. A condensed version was published by the American Bar Association Section of Litigation in 30 Litigation (Fall 2003), at 24.

Robert F. Carangelo & Gina M. Graham, *Passing the Buck: Cost-Shifting in Electronic Discovery*, 50 Fed. Law. (November/December 2003), at 35.

A discussion of the *Rowe* and *Zubulake* cases and their position in electronic discovery litigation, and in upcoming discussions of amendments to the Federal Rules of Civil Procedure.

Barbara A. Caulfield & Zuzana Svihra, *Electronic Discovery Issues for 2002: Requiring the Losing Party to Pay for the Costs of Digital Discovery*, <http://www.kenwithers.com/articles/sedona/index2001.html> (2001).

In this paper from the 2001 Sedona Conference on Complex Litigation, the authors argue that an English-style cost-shifting rule, under which the prevailing party in litigation recovers discovery costs, may curb the perceived abuses and “economic waste” associated with electronic discovery.

Geoff Howard & Hadi Razzaq, *Electronic Discovery Cost Allocation: Why Requesting Parties May Increasingly Find Themselves Rowe-ing Upstream to Fund Electronic Fishing Expeditions*, A.B.A. Computer & Internet Litig. J. (May 24, 2002).

This paper explores the differences between conventional and electronic discovery, focusing on costs, and dissects the *Rowe* case to support an argument that federal courts will increasingly shift electronic discovery costs to requesting parties.

Richard L. Marcus, *Confronting the Future: Coping With Discovery of Electronic Material*, 64 Law & Contemp. Probs. 253 (Spring/Summer 2001).

Marcus, the reporter for the Discovery Subcommittee of the Civil Rules Advisory Committee, summarizes the problem of electronic discovery as it has been presented to the subcommittee and presents a list of the various amendment ideas that have surfaced in the literature and from the discussions.

Michael Marron, *Discoverability of “Deleted” E-Mail: Time for a Closer Examination*, 25 Seattle U. L. Rev. 895 (2002).

“[T]his Comment [argues] that the discovery rules presently require disclosure of an unacceptable amount of information. In particular, public policy concerns such as communication efficiency, individual privacy, and free speech should outweigh the rights of a litigant to access deleted e-mail correspondence without some showing of particular relevance or need.”

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

An introductory-level, somewhat superficial review of electronic discovery. While this article contains no deep analysis or new revelations, it may serve as background material to instruct clients, especially in-house counsel, who are not aware of their electronic discovery obligations.

Point/Counterpoint: Should the Federal Rules of Civil Procedure Be Amended to Accommodate Electronic Discovery?

<http://www.kenwithers.com/articles/> (2001).

Computer-based discovery presents new and unique challenges for judges, lawyers, and parties in civil litigation. But does it demand amendments to the Federal Rules of Civil Procedure? Two very different points of view are presented: “Yes,” says Tom Allman, general counsel of BASF Corporation. “No,” says the New York State Bar Association’s Commercial and Federal Litigation Section, Committee on Federal Procedure.

Marnie H. Pulver, *Electronic Media Discovery: The Economic Benefit of Pay-Per-View*, 21 Cardozo L. Rev. 1379 (2000).

“An economic analysis of relevant case law illustrates the inefficiency of modern discovery rules as applied to EMD [electronic media discovery]. Modern discovery practice often leads to misallocated funds and wasted human capita. The misallocated resources stem from an externalized discovery practice. Efficient allocation can be achieved only when the costs and benefits of EMD are internalized.” In other words, the author proposes that all electronic discovery costs be borne by the requesting party.

Jonathan M. Redgrave & Erica J. Bachman, *Ripples on the Shores of Zubulake: Practice Considerations from Recent Electronic Discovery Decisions*, 50 Fed. Law. (November/December 2003), at 31.

The authors present ten reasons why practitioners should read the Zubulake and Rowe decisions closely and plan their electronic discovery accordingly.

Jonathan M. Redgrave & Ted S. Hiser, *Fishing in the Ocean: A Critical Examination of Discovery in the Electronic Age*,

<http://www.kenwithers.com/articles/sedona/> (2001).

In this paper from the 2001 Sedona Conference on Complex Litigation, the authors explore the explosive growth of the “paperless” business environment, review the history of judicial concern about “fishing expeditions,” apply these historic concerns to electronic discovery, and argue for a flexible judicial approach to the question of scope.

Martin H. Redish, *Electronic Discovery and the Litigation Matrix*, 51 Duke L.J. 561 (2001).

Redish argues that electronic discovery is unique and demands a different set of rules and procedures than conventional, paper-based discovery does to prevent undue costs, burden, and intrusion.

Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-Mail at Trial in Commercial Litigation*, 29 Rutgers Computer & Tech. L.J. 219 (2003).

The unstated but obvious point to this exhaustive review of the evidential issues involving e-mail is that if you don't pay attention to the evidential foundations during discovery, the e-mail may either fail to get into evidence when it should be admitted, or fail to be excluded when it shouldn't be admitted. The article provides many words to the wise.

Hon. James M. Rosenbaum, *In Defense of the DELETE Key*, 3 Green Bag 393 (2000); *In Defense of the Hard Drive*, 4 Green Bag 2d 169 (2001).

In a pair of short, provocative articles, a federal district court judge and member of the Judicial Conference of the United States expresses his concern that far-reaching computer-based discovery may violate privacy and stifle creative thought. In the first article, he proposes a "statute of limitations" on the recovery of stale, deleted files. In the second, he proposes a "cyber time-out," a notice period for employees during which their computer files are sequestered, before employers may investigate them. This would allow the employer and employee to negotiate the scope and conditions of the investigation, preventing de facto general searches.

Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327 (2000).

A federal district court judge takes a close look at the technology, current rules, and case law surrounding computer-based discovery, and proposes two amendments to Rule 34. One change would clarify the scope of document discovery, replacing the 1970 language ("other data compilations from which information can be obtained") with more modern language ("electronically stored information"). A new paragraph added to Rule 34 would establish a presumption that discovery of computer data would be subject to a protective order and establish a presumption that costs for producing data in print form, as opposed to electronic media, would be borne by the requesting party.

Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Retaining, Destroying and Producing E-Data* (pts. 1 & 2), New York L.J., May 8, 2002, at 1; New York L.J., May 9, 2002, at 1.

Scheindlin returns to the topic of electronic discovery in this two-part article, this time focusing on obligations related to the retention and destruction of electronically stored information and business records, as well as the production of such data in civil litigation. She reviews several important recent cases in which poor electronic records management practices and failures during the discovery process

resulted in sanctions against defendants, including Linnen, GTFM, and Danis. She concludes that a written electronic records management policy, a thorough understanding of a client's actual compliance with that policy, and early disclosure are key elements to successful discovery for both sides.

The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production,

http://www.thesedonaconference.org/publications_html (Jan. 2004).

This is the product of a think tank representing the best and brightest of the private defense bar, in-house corporate counsel, and defense-oriented technical consultants. It is a working document, and the authors invite observations, comments, and criticism.

Samuel A. Thumma & Darrel S. Jackson, *The History of Electronic Mail in Litigation*, 16 Santa Clara Computer & High Tech. L.J. 1 (1999).

An interesting and entertaining survey of the evolving role of e-mail as either evidence or subject matter in both civil and criminal cases from the early 1980s through June 1999. Of particular interest is extensive use of e-mail to establish elements of various commercial actions, such as jurisdiction, statute of limitations, and notice.