A Wreck on the Info-Bahn: Electronic Mail and the Destruction of Evidence

Matthew J. Bester

1. INTRODUCTION

At the National Building Museum in Washington, D.C., visitors often remark about a small metal bar lining the inside wall on the top floor. The building was completed in 1887 for the U.S. Pension Bureau (the present-day Veterans Administration). The metal bar was used to carry a basket which delivered messages from one office to another. Eighty years later, the U.S. Department of Defense developed an electronic network to exchange secret documents across the United States. The outgrowth of that system lead to today's electronic mail (“e-mail”) technology, available to millions of businesses and homes around the country.

E-mail affords its users a quick and simple way to communicate — whether between companies, within corporations, or among friends. With the right equipment users can send e-mail over phone lines and networks in less time than it takes to type the message. For example, at Microsoft Corp., several employment interviews are completed in a one-day multiple interview format. As the applicant passes through this process, interviewers pass along e-mail comments to the next interviewer about the applicant which may result in a different style of interview. The conversational tone often seen in e-mail has caused liability for companies in lawsuits for such claims as sexual harassment and fraud. One reason for this is that e-mail users often do not realize their messages may be saved.

In order to save space and storage costs, companies create guidelines for the regular and systematic destruction of old documents and correspondence. Generally, companies will avoid judicial sanctions when destroying stored documents pursuant to internal record retention policies. Ad

1 Based on the writer’s personal experience as a tour guide at the museum.
2 The network, called ArpaNET for Advanced Research Projects Agency, was created so that Defense Department officials, academics, and scientists could communicate confidentially around the United States. See Shawn McCarthy, Internet’s Evolution Becomes Computer-Era Revolution Series: Inside Internet, WASH. POST, June 1, 1992, at F24; Gordon D. Lee, Should Attorneys Use the Internet?, 44 R.I.B.J. at 27 (December 1995).
3 One recent article predicted that 40 million e-mail users will send 60 billion messages by 2000. See Susan J. Silvernail, Electronic Evidence: Discovery In the Computer Age, 58 ALA.LAW 176, 181 (1997). Americans spend 200 million hours per day using computers. See George Lardner, Jr., Panel Urges U.S. to Power Up Cyber Security, WASH. POST, Sept. 6, 1997. Time magazine estimated that 2.6 trillion e-mail messages passed through U.S.-based computer networks that same year. By 2000, it is estimated that number will be 6.6 trillion. See S.C. Gwynne and John F. Dickerson, Lost in the E-mail, TIME, Apr. 21, 1997, at 88.
4 E-mail addresses consist of a computer user’s name, a computer address, and a domain name. For instance, a hypothetical address for the writer would be Bester@cua.edu, where “Bester” is the user’s name, “cua” is the computer address at The Catholic University of America, and “edu” for educational institution is the domain name. Other common domain names include “.com” for a company or commercial institution, “.gov” for government addresses, and “.org” for addresses that do not fit in any other category. See G. BURGESS ALLISON, THE LAWYER’S GUIDE TO THE INTERNET 10, n.5 (1995); see also Brendan P. Kehoe, Zen and the Art of the Internet: A Beginner’s Guide to the Internet, (1993); <http://access.tuscon.org/zen/zen-1.0_toc.html#SEC96> (visited October 1, 1997). See Meloff v. New York Life Insurance Co., 51 F.3d. 372 (2d. Cir. 1995) (where an employee was fired over internal corporate e-mail system).
5 See Alex Markels, Management: Managers Aren’t Always Able to Get the Right Message Across with E-mail, WALL ST. J., Aug. 6, 1996, at B1.
7 See Martha Middleton, A Discovery: There May Be Gold In E-mail, 16 NAT’L L. J. JOURNAL, Sept. 20, 1993, at 1.
9 See GORELICK ET AL., supra note 8, § 10.3 at 311. See also
hoc paper document destruction, though, has caused problems for companies. Courts have also penalized litigants for destroying electronic records.11

This Comment will first examine the procedural steps necessary to use e-mail in a lawsuit. Next, this Comment will explore the use of e-mail as the “smoking gun.” This Comment will next focus on destruction of evidence, sanctions for that destruction and their application in the electronic age. Finally, it will conclude that judges should examine destruction of e-mail evidence in light of that technology’s unique characteristics.

II. E-MAIL AND LIABILITY: PERFECT TOGETHER

A. Electronic Mail: Technological and Legal Implications

To those who are not computer experts, e-mail is a simple concept: a computer user opens the appropriate e-mail program, types an e-mail address, then types a message, and hits a key to send the message. Seconds later, an icon on the screen of the recipient user flashes to alert the recipient she has a message. She opens the mail and reads it. The whole process, from conception to writing to sending and reading the message on the other end, can take less than five minutes.12

The Federal Rules of Civil Procedure govern discovery, the process of pre-trial information sharing of such a message, during a civil suit.13 According to Rule 26(b)(1) of the Federal Rules of Civil Procedure and case law,14 discovery may be made of any matter which is not privileged, that will likely lead to discoverable evidence. In 1970, Congress amended the Federal Rules of Civil Procedure to accommodate the computer age. Specifically, Rule 26(a) requires pre-trial disclosures to the opposing party.15 In addition, Rule 34(a)16 was re-written to require parties to produce electronic forms of evidence in “reasonably usable form,” when information is requested.17 Modern practice has proven that discovery of electronic information is “crucial” to complex litigation.18

Discovery requests for e-mail are becoming more popular.19 For example, in Adams v. Dan River Mills, Inc.,20 a federal district court held that because of the low cost and accuracy in producing computer printouts and computer tapes, their discovery should not be blocked.21 But the volume of electronic discovery can be massive. According to one report during the U.S. Justice Department’s investigation into the merger of Microsoft Corp. with Intuit Corp., Intuit was served with an electronic data request totaling 76 pages.22 Intuit met the request by searching 15,000,000 pages of

See generally supra note 8, §§ 10.4-10.8.
11 See American Fundware, 133 F.R.D. 166, 170 (D. Colo. 1990); Wm. T. Thompson Co. v. General Nutrition Centers, Inc., 595 F. Supp. 1443, 1450 (C.D. Cal.1984) [hereinafter “GNC”] (defendant had a duty to preserve records it should have foreseen would be relevant in lawsuit).
12 See Andrew Johnson Laird, Smoking Guns and Spinning Disks, 11 No. 8 COMPUTER LAW., Aug., 1994, at 1, 3.
14 See Hickman v. Taylor, 329 U.S. 495, 507 (1947). Hickman and subsequent cases hold that there are limits to discoverable information. Attorney-client privilege and work product doctrine are among the ways attorneys can prevent discovery of any information. See generally Jack H. Friedenthal et al., CIVIL PROCEDURE §§ 7.4-.7.5 at 385-86 (1993).
15 See Fed. R. Civ. P. 26(a). Rule 26(a) requires disclosure at the outset of litigation such information as the identities of those persons believed to have discoverable information. Rule 26(a)(1)(A), and copies of all documents relevant to the dispute. Rule 26(a)(1)(B).
16 See Fed. R. Civ. P. 34(a). Rule 34(a) reads: Scope: Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor’s behalf, to inspect and copy, any designated documents (including . . . other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form). See id.
17 See Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1383-84 (7th. Cir. 1993) (electronic information is discoverable and a party can be sanctioned for refusing to produce it).
18 See John T. Soma and Steven G. Austin, A Practical Guide to Discovering Computerized Files In Complex Litigation, 11 REV. LITIG. Summer, 1992, at 501, 502. See also Middleton, supra note 7 (“electronic media discovery is becoming increasingly critical in almost every kind of lawsuit . . . ”).
21 Id. at 222.
22 Lovell and Holmes, supra note 19, at 9.
E-mail must also overcome evidentiary barriers before being admitted. First, e-mail must be relevant. Parties using e-mail must also overcome challenges to its admissibility on hearsay grounds. Clearly e-mail is an out of court assertion. However, it appears litigants could overcome the hearsay exclusion by arguing exceptions to the Federal Rule of Evidence.

Such a tactical maneuver was used in United States v. Ferber. A Massachusetts federal court held that e-mail was admissible against a defendant indicted on fraud and bribery charges. An internal corporate e-mail message followed an incriminating conversation between the defendant and a co-worker. An e-mail message was then sent by the co-worker to his supervisor, in what the writer termed an "upset" state of mind. Although the trial court refused to admit the e-mail message under neither the business records exception nor the excited utterance exception to the hearsay rule, it did eventually admit the message as a present sense impression. On re-explanation of the trial judge's rulings, however, it reversed itself and found the message was admissible under the excited utterance exception because the it was written only a short time after the conversation.

B. E-mail as the Smoking Gun

One of the biggest myths in the electronic world is that once a recipient deletes a message from her screen it is gone forever. Computers delete data by moving it out of the way. Data is "removed" when new saved data takes its place. Only then does it become inaccessible to the user. One of the most notorious examples was Oliver North's attempt to cover up arms sales to support the Contras in Nicaragua. The e-mail North thought were deleted were later retrieved from his computer and used against him.

In addition, e-mail has caused civil and criminal liability, and costly litigation. Siemens Solar In-
dustries v. Atlantic Richfield Co.,44 began in 1989 when Siemens bought from defendant ARCO a company devoted to developing commercial solar energy technology.45 When Siemens made its decision to buy ARCO's company, it relied on reports made by the defendant that the new solar technology would be profitable.46 After the sale, however, it found that the technology was not commercially viable; Siemens sued for breach of contract, fraud and negligent misrepresentation.47 In its complaint, Siemens alleged that before the closing date, ARCO's officers knew that the new technology would not be profitable.48 Siemens based these allegations on e-mail it discovered between ARCO executives.49

In Strauss v. Microsoft Corp.,50 an assistant editor of a Microsoft publication filed a sex discrimination claim against the company.51 The plaintiff alleged Microsoft passed her over twice for promotions and instead hired less qualified male candidates.52 She pointed to an e-mail message sent by the publication's editor which stated that a hired male candidate was, "adequate—but not great."53 The plaintiff retrieved four additional e-mail messages with sexual references as evidence of gender discrimination.54 The court rejected the arguments made by Microsoft to exclude the e-mail on relevancy grounds and prejudice to the defendant.55 Microsoft argued that the messages unfairly could lead a jury to believe that the reason the plaintiff was not promoted was because of her gender.56 The trial court also denied a motion by the defendant for summary judgment, and held that the plaintiff showed a sufficient nexus between the e-mail and the decision not to promote her.57

Sending e-mail also lead to federal or state criminal liability.58 The Computer Abuse Act of 198459 prohibits unauthorized entry to federal interest computers,60 including "hacking" and spreading viruses.61 The Electronic Communication...
tions Privacy Act of 1986, prohibits unauthorized interception and access of electronically stored data. Also, traditional crimes such as fraud or threats can be adapted for prosecutions resulting from e-mail.

Theft of trade secrets was at the center of a prosecution under section 499(c) of the California Penal Code in People v. Eubanks. California prosecuted co-defendant Eugene Wang after he became disenchanted with his employer and e-mailed messages containing his company's trade secrets to a competitor, Symantec. After Gordon Eubanks, president of Symantec, received the e-mails, Wang's company filed a criminal complaint.

III. DESTRUCTION OF EVIDENCE AND CORPORATE DOCUMENT DESTRUCTION POLICIES

The first impulse after a lawsuit is filed may be to rid storage of any evidence which may implicate oneself in the lawsuit. Besides criminal laws, which apply to the destruction of evidence in both criminal and civil suits, courts may invoke other sanctions to punish parties, such as allowing a jury to draw adverse inferences or ordering default judgments. In addition, ethics rules prohibit attorneys from destroying evidence. These punishments often turn on the intent of the "spoliating" or destroying party, as well as the overall damage done. Courts look at four key issues when confronted with destruction of evidence: (1) what evidence was destroyed, (2) when was the evidence in question destroyed, (3) who destroyed the evidence, and (4) how was the evidence destroyed.

Internal corporate document retention policies allow companies some leeway in destroying documents. Courts have recognized that organizations, due to high storage and organization costs, cannot be expected to keep documents forever. Most times, these records may be destroyed as long as they are not relevant to some ongoing or foreseeable litigation. This, however, begs the questions, "when is a document relevant," and, Supp. 1997).


See id. at 847.

See Eubanks, 44 Cal. Rptr. 2d at 846-47. Eubanks was charged with 11 counts of receiving stolen property and trade secret violations. See Carla Lazzareschi & Martha Groves, 2 Indicted On Trade-Secret Theft Charges Technology: Symantec's Chairman and an Employee Are Accused of Stealing Inside Information from Borland, L.A. TIMES, Mar. 5, 1993 at D1. The district attorney's office later was disqualified because Borland helped pay for technical assistance during the prosecution. See 927 P.2d. 310 (Cal. 1997).

"when is litigation foreseeable?"76

Lawrence Solum and Stephen Marzen (hereinafter "Solum and Marzen"), well known scholars in the field of destruction of evidence, argued destruction of evidence undermined two important goals of the judicial system—truth and fairness.77 Jamie Gorelick, another scholar in the field, added to these the fundamental integrity of the judicial system.78 The main reason to prohibit destruction of evidence, these scholars argued, is that destruction reduced the likelihood "that the judicial process will reach accurate results."79 Thus, prohibitions on the destruction of evidence punish, deter,80 compensate81 and restore accuracy82 to the fact finding process.

A. Methods Of Controlling Destruction of Evidence

1. Criminal Sanctions

It may surprise the reader that no Federal crim-

inal statutes deal specifically with destruction of evidence.83 However, Federal obstruction of justice statutes are available to prosecute parties who destroy evidence in both civil and criminal cases.84 The four elements necessary to prove an obstruction of justice charge are that (1) the defendant destroyed relevant documents;85 (2) the defendant knew the documents were relevant86 (3) to a pending judicial proceeding, with87 (4) the purpose of obstructing justice.88

Courts have differed on the level of mens rea necessary to prove an obstruction of justice

ied a $12.6 million penalty on defendants, in part because of defendants' failure to adhere to retention provisions. The applicable records retention statute mandated a three-year retention program. The defendants could produce only seven months of records. See United States v. Smithfield Foods, Inc., 972 F. Supp. 338 (E.D. Va. 1997).

79 Solum & Marzen, supra note 77, at 1138.
80 See GORELICK ET AL., supra note 8, § 1.21, at 27-28. A rule restoring accuracy to the factfinding process after destruction of evidence punishes the effects of the destruction rather than restores the actual destruction. See id. But see Nesson, infra note 81, at 801. Nesson calls the theory that the default sanction deters future spoliation "sophistry . . . [t]here is nothing punitive in imposing default or dismissal in a case the spoliator would have lost anyway." Id.
82 Restoring accuracy is not a solid basis on which to justify destruction of evidence sanctions because courts' reconstruction of evidence sometimes will be inaccurate, trumping the very goal of the doctrine. As a result, punishment is a much stronger justification for imposing penalties on spoliators of evidence than is accuracy.
83 See Fedders & Guttenplan, supra note 76, at 19. State criminal statutes on the destruction of evidence are beyond the scope of this paper. The federal statutes section here is meant only to give the reader an understanding of the criminal penalties and judicial inquiries on the doctrine. For an outline of state laws on destruction of evidence. See also GORELICK, ET AL., supra note 8, §§ 5.7-5.10.
84 See, e.g., 18 U.S.C. § 1503 (1994), (obstruction of justice); 18 U.S.C.A. § 1505 (West Supp. 1997) (prohibiting obstruction of justice in administrative or legislative proceeding). In civil cases, Solum & Marzen argue by comparison, "threat of criminal prosecution for evidence destruction . . . may be more theoretical than real," pointing out that no party has ever been convicted of destroying evidence in a civil case. Solum & Marzen, supra note 77, at 1106.
85 See United States v. Ryan, 455 F.2d. 728, 734 (9th Cir. 1972) (conviction under 18 U.S.C. § 1503 reversed where government could not show relevancy of destroyed evidence); GORELICK ET AL., supra note 8, § 5.3 n.17; Oesterle, supra note 70, at 1197 (where Oesterle argued that the relevancy requirement was "surprising" because nothing in the language of the statute required relevancy; he attributed the theory to a mistaken interpretation of the statute).
86 The test appears to be reasonable belief of the defendant. United States v. Vesich, 724 F.2d. 451, 457-458 (5th Cir. 1984), reh'g denied 726 F.2d. 168 (5th Cir. 1984); but see Oesterle, supra note 70, at 1199-1201 (which folds the knowledge test into the motive prong of the statute).
87 See United States v. Walasek, 527 F.2d. 676, 679 (3rd Cir. 1979); Fedders & Guttenplan, supra note 76, at 21 (stating that the pendency requirement ensures accused has notice that interfering with an ongoing proceeding carries criminal penalties).
88 Professor Oesterle argued that most times intent to obstruct justice may be inferred from the act itself. Oesterle, supra note 70, at 1199. What is in dispute is "whether an act violates this section if the defendant in fact does not specifically intend to obstruct justice . . . . but has knowledge or is on notice that an obstruction of justice is the likely result of his conduct." Id. at 1199. The statutory framework in 1503 is replicated in 1505 for obstruction of justice during agency or
charge. Some federal courts require knowledge that the probable outcome of the defendant's acts will be to obstruct justice. For example, in United States v. Jeter, the government prosecuted Jeter on obstruction of justice charges after he distributed grand jury transcripts to the targets of those grand jury proceedings. In affirming his conviction, the court held that the defendant must obstruct justice with a general intent of knowledge and a specific intent to obstruct justice. By contrast, the Fourth Circuit Court of Appeals in United States v. Neiswender held that while the defendant knew his conduct would not obstruct justice, he could still be found guilty. Chief Judge Haynsworth wrote "that the defendant's design [was] irrelevant," and as long as the "natural result" of his scheme was to obstruct justice his conviction would stand.

The pendency requirement of 18 U.S.C. § 1503 simply requires presentation of evidence before a grand jury. A federal district court maintained that a person who (1) knew about a Grand Jury investigation, (2) had reason to believe that a certain document may come to its attention, and (3) caused its destruction intentionally to prevent the Grand Jury from seeing it, was guilty of violating section 1503.

In addition to the obstruction of justice statutes, the Justice Department may prosecute destruction of evidence under the conspiracy section of Title Eighteen of the United States Code, alleging that defendants conspired to defraud the United States by destroying documents. Still another option is to charge criminal contempt under 18 U.S.C. § 401, which takes place when a court orders a party to produce documents and the party subsequently destroys them. Finally, although there has not been a prosecution for document destruction under it, 18 U.S.C. § 1001 generally prohibits false statements to a court.

2. Civil Sanctions

In civil suits, judges rely on the language of Federal Rule of Civil Procedure 37 to sanction parties who abuse the discovery process. For example, Rule 37(c) authorizes a court to "impose other appropriate sanctions" where a party does not disclose certain information, comply with a court order, attend a deposition, answer interrogatories, or fail to formulate a discovery plan.

Congressional proceedings and 1510 to provide sanctions for violations before legislative, judicial, or administrative proceedings begin. See 18 U.S.C. §§ 1505, 1510 (1994).

Obstruction of justice charges have both an actus reus, a physical action, as well as a mens rea, the commensurate mental state. See Joseph V. De Marco, Note, A Funny Thing Happened On the Way to the Courthouse: Mens Rea, Document Destruction, and the Federal Obstruction of Justice Statute. 67 N.Y.U. L.Rev. 570 (1992).

See Pettibone v. United States, 148 U.S. 197 (1893) (conviction under a predecessor to 18 U.S.C. § 1503); United States v. Ryan, 455 F.2d. 728 (9th Cir. 1972) (obstruction of justice conviction overturned). See also United States v. Sollow, 138 F.Supp. 812, 817 (S.D.N.Y. 1956) (holding that the statute, "condemns not only the corrupt obstruction of the administration of justice but also any endeavor to corrupt the due administration of justice").

See generally 775 F.2d. 670 (6th Cir. 1985).

See Jeter, 775 F.2d. at 673.

See Jeter, 775 F.2d. at 679.

See United States v. Neiswender, 590 F.2d. 1269 (4th Cir. 1979). In Neiswender, the defendant was convicted under 18 U.S.C. § 1503 when he approached an attorney during a criminal trial claiming he could influence the jury when he had no such ability. Id.

Neiswender, 590 F.2d. at 1274.

See United States v. Walasek, 527 F.2d. 676, 678 (3d Cir. 1978).


See 18 U.S.C. § 371. A conspiracy exists when "there is (1) an agreement, (2) an overt act by one of the conspirators in furtherance of the conspiracy, and (3) an intent on the part of the conspirators to defraud the United States government." Fedders & Guttenplan supra note 76, at 31, citing United States v. United States Gypsum Co., 438 U.S. 422, 443 n.20 (1978); United States v. Shoup, 608 F.2d. 950 (3d. Cir. 1979); United States v. Bonanno, 177 F. Supp. 106 (S.D.N.Y. 1959) rev'd on other grounds sub nom. See also United States v. Buffalino, 205 F.2d. 408 (2d. Cir. 1960).

See Fed. R. Civ. P. 37(b)(2)(A-C) (which spells out a federal court's authority to impose sanctions).


See Fed. R. Civ. P. 26(a) or 26(e)(1). The 1993 Advisory Committee Notes state that sanctioning a party by precluding use of that evidence at trial is not an effective sanction; however, the notes go on to say that a court has many other sanctioning options, including declaring facts as established or allowing the jury to become aware of the nondisclosure. Fed. R. Civ. P. 37 Advisory Committee's Note.
The sanctions under Rule 37 are powerful, but are limited to cases where a court already has ordered a party to preserve evidence. One commentator suggested Congress cure this problem by codifying a ban on destruction of evidence and sanctioning power in the Federal Rules of Civil Procedure. In practice, though, this has been addressed already as courts have expanded their power to sanction parties for document destruction before an order is issued.

For instance, in Wm. T. Thompson Co. v. General Nutrition Corp., Inc., Wm. T. Thompson Co. ("Thompson") sued General Nutrition Center Corp., Inc. ("GNC") over "bait and switch" advertising practices. Thompson served GNC with requests for production of documents a few weeks after filing suit. In a set of findings of fact, the court concluded that GNC had kept and subsequently destroyed records, some in electronic form, pertaining to purchases, sales and inventory. The court ordered a default judgment against GNC because it had a duty to preserve these records. Notice was provided before the suit was filed that the documents were relevant to the dispute. The court announced that, even without a specific request for the documents, when a party knows or reasonably should know that a document will become important to a lawsuit, that party has a duty not to destroy that document.

By contrast, the Texas Supreme Court overturned the default sanction ordered by the trial court in Chrysler Corp. v. Blackmon after the trial court struck some of Chrysler's pleadings in the context of a wrongful death suit. The trial court's imposition of sanctions was overturned by state Supreme Court by: (1) examining the direct relationship between the offensive conduct and the sanction, and (2) the checking that the sanction was not excessive. By that standard, the trial court in Blackmon abused its discretion when it ordered the "death penalty" sanction. First, the sanction was not directed at the offensive conduct—there was no showing that the victim's family could not prepare for trial without the missing documents. Second, default judgment on lia-

---

107 See Solum & Marzen, supra note 77, at 1095; Oesterle, supra note 70, at 1222 (arguing that a destroying party may become sanctionable only after the court enters an order to preserve documents). Cf. Johnston, supra note 102, at 324-25 (asserting that pre-order sanctions are possible within the language of Rule 37, but that the court's "inherent power" justification is stronger for those sanctions). Professor Nesson said spoliation is a growing practice in civil litigation which threatens to undermine the integrity of the civil trial process, in part because of lax judicial enforcement of penalties. See Nesson, supra note 81, at 79495.

108 Professor Oesterle argued to reform the Federal Rules of Civil Procedure, adding new rules under Rule 26, Rule 34, and Rule 37 because the existing rules did not sufficiently deter spoliators of evidence. See Oesterle, supra note 70, at 1240-43. Oesterle's comments after his proposed rules indicate that the baseline doctrine is that a litigant may not destroy relevant evidence intentionally once he knows an action is pending. Oesterle would expand that standard to criminal prosecutions for destruction of evidence by removing the negligence defense. Under this regime, the only defense would be that the destruction was not only inadvertent, but also non-negligent. The comments to the proposed rules accord with the approach of the court in Levy v. Remington Arms Co.: one has a responsibility to preserve documents if she can foresee litigation concerning the documents. See 836 F.2d 1104, 1112 (8th Cir. 1988).


111 See id. at 1444. GNC also filed suit against Thompson, but its grounds are not relevant to this paper.

112 See id.
bility was more severe than necessary to satisfy the legitimate purposes of sanctions for discovery abuse. Another option for a judge is simply to allow a jury to infer certain facts when evidence destruction comes to light. This common law doctrine holds that the factfinder may draw an unfavorable inference against a party who has destroyed relevant documents because that party is assumed to have been motivated by a desire to cover up damaging evidence. The key to the spoliation inference is some form of intention to destroy the evidence. Some courts merely require an intent to destroy evidence, while others require a showing of bad faith. One lingering question when using the inference is how much weight to assign to it.

For instance, then-Circuit Judge Breyer upheld the district court's imposition of an adverse inference where a bankrupt company destroyed records which may have traced its financial obligations back to the plaintiff in Nationwide Check Corp., Inc. v. Forest Hills Distributors, Inc. Judge Breyer ruled that the adverse inference was warranted on two grounds: (1) the fact of destruction itself satisfies the relevance of the documents according to Fed.R.Evid. 401, and (2) a policy of punishing those who destroy relevant evidence. A trial court has wide discretion to impose sanctions once relevancy is established.

3. Suing in Tort to Remedy Destruction of Evidence

Nine states recognize that parties suffer a tortious injury when a party destroys evidence. The tort allows a litigant to recover money damages against a party who spoliates evidence and can be tried before a judge or jury along with the underlying claim (personal injury, wrongful death, etc.) which gave rise to the spoliation. This new tort, first recognized in Smith v. Superior

---

122 Id. at 850.
123 See Solum & Marzen supra note 77, at 1088.
124 Consider the following jury instruction:
If you find in this case the plaintiff's counsel and agents, including (their expert witnesses) failed to fulfill this duty [not to take actions that will cause the destruction or loss of relevant evidence that will hinder the other side from making its own examination and investigation of all potentially relevant evidence], then you may take this into account when considering the credibility of (the expert witness) in his opinions and also you are permitted to, if you feel justified in doing so, assume that evidence made unavailable to the defendants by acts of the plaintiff's counsel or agents, including (the expert witness), would have been unfavorable to the plaintiff's theory in the case.


125 See W. Russell Welsh and Andrew C. Marquardt, Spoliation of Evidence, 23 The Brief, Winter 1994, at 9. One of the earliest cases to recognize such an inference was Armory v. Delamirie, 93 Eng.Rep. 664 (K.B. 1722). In Armory, the plaintiff sued the defendant jeweler after the plaintiff claimed the jeweler stole his stone when appraising it. Finding for the plaintiff, the judge ordered the jury to estimate damages using the value of the highest quality stones, not the supposed value of the actual stone. Id. Compare Scout v. City of Gordon, where the spoliation inference was not drawn where plaintiff could not show any intentional destruction or fraudulent misplacement of records by defendant. Scout based its spoliation inference argument only on the mere unavailability of hospital records. See 849 F. Supp. 687, 691 (D. Neb. 1994). That was not enough, and the Scout court used three tests to determine whether a spoliation inference was warranted: was the destruction of evidence "[1] intentional, [2] fraudulent or [3] done with a desire to conceal and, thus, frustrate the search for truth." See also Vick, 514 F.2d. 734, 737 (5th Cir. 1975) There, the trial court factored the lack of bad faith in the destruction of the documents, as well as the fact that destruction was performed well before interrogatories were served.

126 See Solum & Marzen supra note 77, at 1088.
127 See Cedillo and Lopez, supra note 70, at 651. Courts have split on whether to allow the inference to justify a verdict against the spoliator. See Welsh and Marquardt, supra note 124, at 10 (contending that most courts do not hold that the inference is sufficient to justify a verdict against the spoliator).

128 See 692 F.2d. 214 (1st. Cir. 1982).
129 See id. at 218. But see Williams v. California, where California Supreme Court refused to find the state liable for evidence destruction. 664 P.2d. 137 (1983). A state highway patrolman negligently inspected evidence relevant to a negligence action after a car accident, but he had assumed no duty to do so. See id. at 142-43.

130 See id. at 219. See also Martocco v. General Motors Corp.


132 See Gorelick et al., supra note 8, § 4.1 at 140.
Established the tort in Mississippi, and Oklahoma have recognized the tort of negligent Anchorage. See generally

document for the text in its exact terms.

The Pirocchi court held that one who assumes control of evidence was a "tortious act". Further, Pirocchi v. Liberty Mutual Ins. Co., was the first case to impose tort liability for pending suit and the harm the plaintiff suffered the tort in the "probable expectancy" of the im-

Thus, a party could be held liable for spoliating ev-

"for every wrong there must be a remedy" and

"for every wrong there must be a remedy" and thus, a party could be held liable for spoliating evidence. The court based its authority to create the tort in the "probable expectancy" of the im-

The reasons for implementing a document de-

Cost is a significant factor. With paper piling up in warehouses and file cabinets, a systematic purge of files helps keep storage more manageable and cheaper. After years of operation, storage costs are staggering for a company such as IBM. Perhaps the most important reason is that a properly managed records retention policy reduces legal exposure. A document manage-

C. Document Retention Policies: Eliminating Smoking Guns and Nuclear Warheads

The reasons for implementing a document de-

The reasons for implementing a document de-

Cost is a significant factor. With paper piling up in warehouses and file cabinets, a systematic purge of files helps keep storage more manageable and cheaper. After years of operation, storage costs are staggering for a company such as IBM. Perhaps the most important reason is that a properly managed records retention policy reduces legal exposure. A document manage-


See Welsh and Marquardt supra note 124, at 11.

Although the Smith court was the first to name the tort, its origins go back over 100 years, to another California case, Fox v. Hule & Norcross Silver Mining Co., 41 P. 508 (1895). The California Supreme Court there held that the destruction of evidence was a "tortious act". Further, Pirocchi v. Liberty Mutual Ins. Co., was the first case to impose tort liability for destruction of evidence. See 965 F.Supp. 277 (E.D.Pa. 1973). The Pirocchi court held that one who assumes control of evidence also assumes a duty to take reasonable care of that evidence. See Gorelick ET AL. supra note 8, § 4.2 at 144-45.


See id. at 494.

See id.

Id. at 496.


Florida was the first to recognize the tort in Bondu v. Gurvich, 473 So.2d. 1307 (Dist. Ct. App. 1984). According to a recent law review note, only California, Florida, Idaho, Missis-


Florida was the first to recognize the tort in Bondu v. Gurvich, 473 So.2d. 1307 (Dist. Ct. App. 1984). According to a recent law review note, only California, Florida, Idaho, Missis-

See Wilson supra note 131, 978-79.

See 473 So. 2d. 1307 (Dist. Ct. App. 1984). California established the tort in Velasco v. Commercial Building Mainte-

See generally id. at 1312.

Id. at 1312-15, citing W. PROSSER, TORTS § 1 pp. 3-4 (4th ed. 1971). The dissent argued that under the majority's reasoning, "every case would be subject to constant retrials in the guise of independent actions." Bondu, 473 So.2d. at 1314.

See Solum and Marzen, supra note 77 at 1105-06.

See Allen, supra note 10.

See Betty Ann Olmstead, Electronic Media: Management Litigation Issue When "Delete" Doesn't Mean Delete, 65 Der.


See Fedders and Guttenplan supra note 76 at 11.

In one long standing antitrust suit, IBM spent $2 million in document storage costs alone in an eight-month period. See In re International Business Machines Corp., 687 F.2d. 591, 603 (2d. Cir. 1984).

Fedders and Guttenplan outlined the advantages and
Disadvantages of a document retention plan.

Advantages [include]: (1) elimination of storage of unnecessary documents, (2) reduction in the retrieval cost of documents when requested in a lawsuit, investigation or business relation, (3) reduction in the legal risks from documents, especially ones which were "hastily drafted, erroneous or misleading," and (4) the avoidance of an adverse inference from the non-production of those documents.

Fedders and Guttenplan supra note 76, at 13.

Disadvantages [include]: (1) the expense of establishing the program, both in time and money, (2) inability to prove a fact conclusively later on, (3) less flexibility to respond to requests for documents, (4) adverse inferences stemming from incomplete compliance with the program, (5) adverse inferences from the "selective destruction" of documents not subject to the program, and (6) other adverse effects, including discovery of how the program works.

Id.


151 See Fedders and Guttenplan, supra note 76, at 12.

circumstances surrounding the relevant documents; 153 (2) whether lawsuits concerning the complaint or related complaints were filed, how many were filed, and the magnitude of each complaint; 156 and (3) whether the retention policy was begun in good faith. 157 Even if the policy was instituted in good faith, the circumstances surrounding the document destruction in a particular case may suffice for an adverse inference. 158

In early 1997, Prudential Insurance Company ("Prudential") came under fire for its document retention policy and recurring destruction of documents by its employees. 159 After a class action suit was filed by policyholders in 1995, the district court ordered Prudential to preserve all relevant documents. 160 Prudential sent orders to its employees to preserve documents in accordance with the court's order, but destruction of relevant documents continued. 161 In response, the court levied a $1 million fine, directed a mailing to all employees describing the litigation, and ordered the company to promulgate a document retention policy. 162 Significantly, the court found, however, that there was no willful misconduct on Prudential's part. 163

In Armstrong v. Executive Office of the President, 164
archivists and federal officials litigated a point crucial to this Comment. On the last day of President Reagan's second term, journalists filed suit against the Executive Office of the President to prevent destruction of electronic records contained in White House computers. At issue, inter alia, were the duties of federal agencies to preserve electronic documents — e-mail messages. The district court found that agencies' practice of printing out e-mails which employees thought fell under the Federal Records Act was insufficient because the information on-screen contained data which the printed copy did not. The court ordered the agencies to retain the electronic copies under the Federal Records Act, and also held that agencies must periodically review their electronic record keeping policies. The D.C. Circuit Court of Appeals ultimately reversed itself on other grounds.

These cases illustrate that organizations' document retention policies may become a part of the lawsuit in which they are involved. In fact, one writer predicted that courts may be less willing to excuse the lack of relevant documents due to a records retention policy. If this trend continues, organizations will need to reevaluate their policies to ensure that they not only follow them, but that the policies themselves pass judicial scrutiny.

IV. SYNTHESIS: COMPANIES MUST RETHINK DOCUMENT RETENTION POLICIES IN LIGHT OF THE PREVALENCE OF E-MAIL

A. Destruction of Electronic Mail Evidence

As stated, simply hitting delete most likely will not rid the computer of the e-mail. Yet many computer users mistakenly believe when the message leaves their "inbox" it is gone forever. Courts have little trouble overruling employees' privacy claims when superiors monitor their communications. Employers have a well-defined interest in making sure employees are performing towards company goals; as the case law indicates, employers need to monitor their employees' electronic messages.

Courts should not hesitate to impose Rule 37 default sanctions for destruction of e-mail evidence. It is clear from the rule's language that courts need not exclude certain types of evidence from their purview. The Rules of Civil Procedure empower courts to administer discovery in the most efficient way possible. Thus, other popular sanctions for evidence destruction should be applied to e-mail. Judges should instruct juries to find a fact as true if they determine that a party destroyed evidence. In the alternative, the judges...
should tell juries that the fact should be accepted as established without giving them any discretion to find otherwise.

But courts should not leap to conclusions based on traditional document destruction. When deleting e-mail, intent is more difficult to measure for two reasons: (1) acts on a computer can be quick and permanent and (2) such wide levels of computer proficiency exist.\(^{178}\) Intent is more difficult to measure when a user hits the enter button by mistake and destroys the last copy of an e-mail message. For instance, nearly every computer user has inadvertently hit the wrong key and supplied the computer with an unintended command. These mistakes often can be corrected, but sometimes a message cannot be restored.

Obstruction of justice statutes’ application to destruction of e-mail evidence is unclear.\(^{179}\) Errant keystrokes may delete an e-mail, and under the Neiswender approach it appears that courts may impute intent.\(^{180}\) If carried to its conclusion, one who deletes an e-mail by mistake may subject himself to criminal liability. In addition, there appears to be much room for debate on what level of intent would be necessary to find a destroyer of e-mail liable under intentional spoliation of evidence. As the reader will recall, there are six prongs necessary to prove the tort: (1) pending or probable civil litigation, (2) defendant’s knowledge that litigation is pending, (3) willful destruction of evidence, (4) intent to interfere with plaintiff’s prospective civil suit, (5) a causal relationship between the evidence destroyed and the inability to prove the allegations in the lawsuit and (6) damages caused by destruction.\(^{181}\) It is the third and fourth prongs which in the context of e-mail destruction may cause judges to pause and think.

Because of the greater physical contact with the piece of paper to be shredded, it is harder to argue that one accidentally shredded a document. It is not disputed that accidental shredding of paper occurs regularly, but the overwhelmingly widespread use of computers and varying levels of understanding of that technology appear to make mistakes like these much more common than with paper shredding.

The intent question becomes even more difficult when suing under negligent spoliation of evidence tort because, as in all negligence actions, courts impute a duty to defendants. The duty revolves around a standard of care which is especially hard to define in this scenario because of varying levels of computer competence. Courts must decide how does a “reasonable person” operate her e-mail program? Estimation of damages, in addition, presents a problem in either the intentional or negligent tort.\(^{182}\) The same is true for destruction of e-mail evidence.

V. CONCLUSION

The computer revolution has changed how companies store documents.\(^{183}\) Corporate America, however, has been slow to react.\(^{184}\) Many companies have records managers and systems to preserve company records, but few have electronic records managers.\(^{185}\) It is obvious that

---

\(^{178}\) See Clarke, supra note 58, at 223 (arguing that proving mens rea for computer-related crimes is the most difficult aspect of the prosecution).

\(^{179}\) See Gorelick, et al., supra note 8, § 2.22H at 61 (Supp. 1997)

\(^{180}\) See supra notes 94-95 and accompanying text.


\(^{182}\) See Welsh and Marquardt, supra note 124.

\(^{183}\) See John Montafia, Legal Issues in EDI (Electronic Data Interchange), 7/96 Rec. MGMT. Q. 39 (arguing that record retention policies are more complicated because electronic data systems are programmed to automatically backup information, rather than discard it, making it more difficult to know whether all copies of a document have been destroyed). See 17 C.F.R. § 240.17a-4 (mandating preservation of all communications which fall within § 240.17a-3(4), (6-10)).

\(^{184}\) In response, The New York Times has installed a program which automatically deletes e-mail after 30 days, and Amgen, Applied Materials Corporation, and 76 Products Company created document retention policies to deal with e-mail. See Alex Markels, Workplace: The Messy Business of Culling Computer Files, WALL ST. J., May 22, 1997 at B1. In addition, software is being developed that looks for “hotwords” in an e-mail that might trigger a lawsuit. See id.

\(^{185}\) See Richard J. Cox, Re-Defining Electronic Records Management, 10/96 Rec. MGMT. Q. 12.

"Archivist and records managers need to develop a coherent approach to electronic records management because we need to assume that the majority of record keeping systems will be electronic and because institutional managers and technical professionals are beginning to understand better the challenges of managing information in electronic form. The declining costs, the greater array of software, the increasingly hospitable legal environment, and other such factors are providing means by which record keeping systems will be transferred to electronic systems and used in electronic means."

Id. The author of a recent piece on e-mail destruction and lawsuits wrote that many companies want to delete perma-
companies need such managers when they store thousands of e-mails going back three years or more.\textsuperscript{186} With improved technology, electronic storage adds another layer of complexity to companies' storage needs.\textsuperscript{187} The three criteria spelled out in \textit{Remington}, along with the analysis provided by \textit{Armstrong}, should give companies a clearer understanding of courts' concerns when electronic messages are destroyed.

\footnotesize{\textsuperscript{186} See Markels, \textit{supra} note 184.}

\footnotesize{\textsuperscript{187} See Cox, \textit{supra} note 185. A few of the benefits of records storage in the electronic age are (1) reduced costs, (2) faster more complete data interchange, and (3) quicker access to information. Montaña, \textit{supra} note 183. See also Lovell and Holmes, \textit{supra} note 19.}

For many reasons, the legal consequences of e-mail transmission will continue to confront courts. As e-mail technology becomes more and more global, standardized solutions will ease courts' burdens in confronting cutting edge legal issues. We are only at the beginning.