A WRECK ON THE INFO-BAHN: ELECTRONIC MAIL AND THE DESTRUCTION OF EVIDENCE

Matthew J. Bester

I. 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.[1] 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.[2] The outgrowth of that system lead to today's electronic mail ("e-mail") technology, available to millions of businesses and homes around the country.[3]

E-mail affords its users a quick and simple way to communicate — whether between companies, within corporations, or among friends.[4] 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.[5] The conversational tone often seen in e-mail has caused liability for companies in lawsuits for such claims as sexual harassment and fraud.[6] One reason for this is that e-mail users often do not realize their messages may be saved.[7]

In order to save space and storage costs, companies create guidelines for the regular and systematic destruction of old documents and correspondence.[8] Generally, companies will avoid judicial sanctions when destroying stored documents pursuant to internal record retention policies.[9] 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 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://accesss.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.

[6] *See, e.g.*, Strauss v. Microsoft Corp., 814 F.Supp. 1186 (S.D.N.Y. 1993) (sexual discrimination liability for employer based on e-mail); Siemens Solar Industries v. Atlantic Richfield Co., 1994 WL 86368 (S.D.N.Y. 1994) (e-mail discovered which indicated that the defendant committed fraud); *see also* Matthew Goldstein, *Electronic Mail, Computer Messages Present Knotty Issues of Discovery*, N.Y.L.J., Feb. 8, 1994, at 1.

[7] *See* Martha Middleton, *A Discovery: There May Be Gold In E-mail.* 16 NAT'L L. J. JOURNAL, Sept. 20, 1993, at 1.

[8] *See* JAMIE S. GORELICK, ET. AL., DESTRUCTION OF EVIDENCE, App. A, B at 391 (1989).

[9] *See* GORELICK ET AL., *supra* note 8, § 10.3 at 311. *See also*

hoc paper document destruction, though, has caused problems for companies.[10] Courts have also penalized litigants for destroying electronic records.[11]

This Comment first will 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

---

GORELICK ET AL., *supra* note 8, §§ 10.4-10.8.

10 *See, e.g.*, Computer Associates Int'l v. American Fundware, Inc., 133 F.R.D. 166, 170 (D. Colo. 1990) (default judgment entered after defendant destroyed evidence); United States v. Fineman, 434 F.Supp. 197 (E.D. Pa. 1977), *aff'd by* 571 F.2d. 572 (3d Cir. 1978), *cert. den.* 436 U.S. 945 (1978) (prosecution for obstruction of justice under 18 U.S.C. § 1503 and 18 U.S.C. § 1962(c)). *See also* Michael Allen, *Cleaning House: U.S. Companies Increasing Attention to Destroying Files*, WALL ST. J. Sept. 2, 1987, at 1.

11 *See* American Fundware, 133 F.R.D. 166, 170 (D. Colo. 1990); Wm. T. Thompson Co. v. General Nutrition Centers, Inc., 593 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.

13 *See* FED. R. CIV. P. 26-37.

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 . . . ").

19 *See* Charles A. Lovell and Roger W. Holmes, *The Dangers of E-mail: The Need for Electronic Data Retention Policies*, 44 R.I. B.J., Dec., 1995, at 7.

20 *See generally* 54 F.R.D. 220 (W.D. Va. 1972).

21 *Id.* at 222.

22 Lovell and Holmes, *supra* note 19, at 9.

text and more than 80,000 e-mail messages.[23]

E-mail must also overcome evidentiary barriers before being admitted.[24] First, e-mail must be relevant.[25] Parties using e-mail must also overcome challenges to its admissibility on hearsay grounds.[26] Clearly e-mail is an out of court assertion.[27] However, it appears litigants could overcome the hearsay exclusion by arguing exceptions to the Federal Rule of Evidence.[28]

Such a tactical maneuver was used in *United States v. Ferber*.[29] A Massachusetts federal court held that e-mail was admissible against a defendant indicted on fraud and bribery charges.[30] An internal corporate e-mail message followed an incriminating conversation between the defendant and a co-worker.[31] An e-mail message was then sent by the co-worker to his supervisor, in what the writer termed an "upset" state of mind.[32] Although the trial court refused to admit the e-mail message under neither the business records exception[33] nor the excited utterance exception to the hearsay rule,[34] it did eventually admit the message as a present sense impression.[35] 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.[36]

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.[37] Computers delete data by moving it out of the way.[38] Data is "removed" when new saved data takes its place. Only then does it become inaccessible to the user.[39] One of the most notorious examples was Oliver North's attempt to cover up arms sales to support the Contras in Nicaragua.[40] The e-mail North thought were deleted were later retrieved from his computer and used against him.[41]

In addition, e-mail has caused civil and criminal liability,[42] and costly litigation.[43] *Siemens Solar In-*

---

23 *Id.*

24 *See* FED. R. EVID. 803(6); United States v. Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997).

25 Strauss v. Microsoft Corp. held that e-mail was relevant to an employment discrimination case to show the company's underlying attitude towards promoting women. *See* 1995 WL 326492 *4 (S.D.N.Y. 1995).

26 FED. R. EVID. 801(c) defines hearsay as, "a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted."

27 *See* FED. R. EVID. 801(c). *See also* Anthony J. Dreyer, Note, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence*, 64 FORDHAM L. REV. 2285, 2287 (1996) (arguing that e-mail should be admissible under Federal Rule of Evidence 803(6), but it is often admitted under Evidence Rule 801(d)(1)(A), as a party's own statement). *See also* James H.A. Pooley and David M. Shaw, *Finding What's Out There: Technical and Legal Aspects of Discovery*, 4 Tex. INTELL. PROP. J. 57, 69 (Fall 1996).

28 *See* FED. R. EVID. 803 (1996) (which spells out 24 exceptions to the rule against admitting hearsay as evidence). *See also* Aviles v. McKenzie, 1992 WL 715248 n.2. (N.D. Cal. 1992) (where e-mail is admitted under FED. R. EVID. 801(d)(2)). Another avenue for litigants to pursue is exempting e-mail from the hearsay ban via FED. R. EVID. 803(6). However, this argument has not garnered court acceptance yet. *See* Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997); Dreyer, *supra* note 27, at 2322.

29 *See generally* 966 F. Supp. 90 (D. Mass. 1997).

30 *See* U.S. v. Ferber, 966 F. Supp. at 92, 99 (D. Mass. 1997).

31 *See id.* at 98.

32 *See id.*

33 *See* FED. R. EVID. 803(6).

34 *See generally* U.S. v. Ferber, 966 F. Supp. at 99; FED. R. EVID. 803(2).

35 *See id. See also* FED. R. EVID. 803(1).

36 *See id.*

37 In addition, the pathway taken by a particular e-mail can be traced. *See* Sharon Walsh, *Destroying Documents and Legal Defenses; Experts Say Texaco Case Points Up How Shredders Can Come Back to Haunt Companies*, WASH. POST, Jan. 26, 1997, at H01.

38 *See* Heidi L. McNeil and Robert M. Kort, *Discovery of E-mail and Other Computerized Information*, ARIZ. ATT'Y, Apr. 1995, at 18.

39 Even then, professionals and simple utility programs can bring back "lost" data. *Id.* One problem for law enforcement agencies is the lack of technical expertise to prosecute a crime such as trade secret theft. *See* People v. Eubanks, 47 Cal.App.4th 158, 165 (1997).

40 *See* Ronald J. Ostrow and Michael Wines, *North's Ex-Secretary Tells of Destroying Data*, L.A. TIMES, Feb. 23, 1987, at A1.

41 Pooley and Shaw, *supra* note 27, at 63. A staffer for the Tower Commission, which investigated the Iran-Contra scandal, found the messages that North and his colleagues believed were deleted. *See* Lawrence J. Magid, *As North Learned, Deleted Files Are Retrievable*, L.A. TIMES, Aug. 10, 1987, at Business 4.

42 *See, e.g.*, Harley v. McCoach, 928 F. Supp. 533 (E.D. Pa. 1996) (plaintiff claimed sexual harassment via e-mail); Knox v. Indiana, 93 F.3d. 1327, 1330 (7th Cir. 1996) (prison guard denied harassing subordinate until shown a copy of his e-mail); Aviles v. McKenzie, 1992 WL 715248 *10 (N.D. Cal. 1992) (plaintiff successfully rebutted defendant's motion for summary judgment using e-mail); United States v. Morris, 928 F.2d. 504 (2d. Cir. 1991), *cert. den.*, 502 U.S. 817 (1991) (upholding conviction for spreading a virus through the internet). *See also* Dreyer, *supra* note 27, at 2288 (noting that 90 percent of companies with 1,000 or more employees use e-mail).

43 The case regarded an e-mail message listing twenty

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 1984[59] prohibits unauthorized entry to federal interest computers,[60] including "hacking" and spreading viruses.[61] The Electronic Communica-

five reasons "why beer is better than women" and an anonymously sent pornographic image received by the plaintiff was part of a $2.2 million settlement in a sexual harassment case against Chevron Corp. *See* Marc Peyser and Steve Rhodes, *When E-mail is Oops Mail*, NEWSWEEK, Oct. 16, 1995, at 82. One of the more notable lawsuits includes a race discrimination suit by two Morgan Stanley & Co., Inc. employees after racist jokes were sent along the company's e-mail system. After the e-mail was sent, the employees complained about them and were subsequently denied promotions. The plaintiffs argued the denial was in retaliation for complaining about the e-mail. The two employees sued for $30 million each in damages and asked the court to certify their suit as a class action to include all black employees at the company. *See* Owens v. Morgan Stanley & Co., Inc., 1997 WL 403454 *1, 74, Fair Empl.Prac.Cas. (BNA) 876 (S.D.N.Y. 1997); Frances A. McMorris, *Morgan Stanley Employees File Suit, Charging Race Bias Over Email Jokes*, WALL ST. J., Jan. 13, 1997, at B8.

44 *See generally* 1994 WL 86368 (S.D.N.Y. 1994).

45 *See id.* at *1.

46 *See id.* at *2.

47 *See id.*

48 *See id.*

49 *See id.* at *2. The message sent by an ARCO employee concerning the impending sale read, "as it appears that [the technology in question] is a pipe dream, let Siemens have the pipe." *See* Leslie Helm, *The Digital Smoking Gun: Mismanaged E-mail Poses Serious Risks, Experts Warn*, L.A. Times June 16, 1994 at D1. The federal court dismissed the case without prejudice for lack of diversity after it dismissed federal securities law claims with prejudice. *See id.* at *7.

50 *See generally* 814 F. Supp. 1186 (S.D.N.Y. 1993).

51 *See id.* at 1188.

52 *See id.* at 1188-89.

53 *Id.* at 1193. The message appeared to be written to Julian Birnbaum, another Microsoft employee. *See id.* The second person Microsoft promoted instead of the plaintiff needed much training, according to another e-mail message sent by the journal's editor, Jon Lazraus. *Id.*

54 The four e-mails at issue were: (1) an e-mail message received by plaintiff containing a satirical message entitled "Alice in UNIX Land"; (2) an e-mail advertisement sent by Lazarus to the Journal staff containing a product announcement for replacement "Mouse Balls"; (3) a message forwarded by Lazarus to a male Journal staff member containing a news report on Finland's proposal to institute a sex holiday; (4) a parody also forwarded by Lazarus, of a play entitled 'A Girl's Guide to Condoms' to a male staff member via e-mail, who later sent it to plaintiff. *See* Strauss, 1995 WL 326492, at *4. Lazarus also told the plaintiff that he was "president of the amateur gynecology club." Strauss, 814 F. Supp. at 1194.

55 *See* 1995 WL 326492 at *4, 5.

56 *See id.*

57 *See* Strauss, 814 F. Supp. at 1194, n.9. Microsoft renewed its motion for partial summary judgment after the Supreme Court's decision in *St. Mary's Honor Ctr. v. Hicks*, 509 U.S. 502 (1993), but the motion was denied again. *See* 856 F. Supp. 821, 823-26 (S.D.N.Y. 1994).

58 *See* Catherine Therese Clarke, *From Criminet to Cyber-Perp: Toward an Inclusive Approach to Policing the Evolving Criminal Mens Rea on the Internet*, 75 OR. L. REV. 191 (1996).

59 *See* 18 U.S.C. § 1030 (1994), *as amended.*

60 A federal interest computer is defined as:

(A) A computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such, used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such a computer; or (B) which is one of two or more computers used in committing the offense, not at all of which are located in the same State.

18 U.S.C. § 1030(e)(2)(A-B) (1994).

61 United States v. Petersen, 98 F.3d. 502, 504-510 (9th Cir. 1996) (affirming conviction for computer fraud under

tions Privacy Act of 1986,[62] 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.[63]

Theft of trade secrets was at the center of a prosecution under section 499(c) of the California Penal Code in *People v. Eubanks*.[64] 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.[65] After Gordon Eubanks, president of Symantec, received the e-mails, Wang's company filed a criminal complaint.[66]

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.[67] Besides criminal laws,[68] 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.[69] In addition, ethics rules prohibit attorneys from destroying evidence.[70] These punishments often turn on the intent of the "spoliating"[71] or destroying party, as well as the overall damage done.[72] 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.[73]

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.[74] Most times, these records may be destroyed as long as they are not relevant to some ongoing or foreseeable litigation.[75] This, however, begs the questions, "when is a document relevant," and,

---

18 U.S.C. § 1030 (a)(2)). In footnote one of the opinion, Judge Fletcher defines hacking as, "the ability to bypass computer security protocols and gain access to computer systems." *United States v. Morris*, 928 F.2d. 504, 511 (2d. Cir. 1991) *cert. denied* 502 U.S. 817 (1991) (affirming conviction under 18 U.S.C. § 1030(a)(5)(A) for spreading a virus through the Internet). *But see* U.S. v. Czubinski, 106 F.3d. 1069, 1079 (1st Cir. 1997) (overturning conviction under 18 U.S.C. § 1030).

62 *See* 18 U.S.C. §§ 2510-2521, 2701-2710 (1994).

63 *See, e.g.*, 18 U.S.C. §§ 1341, 1343 (1994) (mail and wire Fraud); 18 U.S.C. § 871(a) (1994); U.S. v. Patillo, 438 F.2d. 13,15 (4th Cir. 1971) (prosecution for verbally threatening the President); *U.S. v. Miller*, 115 F.3d. 361, 362 (6th Cir. 1997) (prosecution for threatening the President by letter).

64 *See generally* 44 Cal. Rptr. 2d 846 (Cal. Ct. App. 1995), *vacated* 927 P.2d 310 (Cal. 1997).

65 *See id.* at 847.

66 *See* Eubanks, 44 Cal. Rptr. 2d at 846-47. Eubanks was charged with 11 counts of receiving stolen property and conspiracy; and Wang was charged with 21 counts of conspiracy 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).

67 *See, e.g.*, GNC, 593 F. Supp. 1443 (C.D. Cal. 1984) (dismissal in civil case after defendant destroyed documents), *aff'd* 104 F.R.D. 119 (C.D. Calif. 1985) (sanction approved on appeal); United States v. Solow, 138 F. Supp. 812 (S.D.N.Y. 1956) (prosecution under 18 U.S.C. § 1503 for obstruction of justice by destroying documents); Smith v. Superior Ct., 151 Cal. App. 3d. 491 (Cal. Ct. App. 1984).

68 *See* 18 U.S.C. § 1503 (1994); 18 U.S.C.A. § 1505 (West Supp. 1997).

69 *See* Siemens Solar Indus. v. Atlantic Richfield Co., No. 93 Civ. 1126 (LAP), 1994 WL 86368, at *6 (S.D.N.Y. 1994).

70 *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 3.4 (1996); *see also* MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR7-102(7),(8); DR 7-109(A); DR 7-107(C)(7) (1979). Professor Oesterle said that the lack of charges brought and convictions obtained illustrates ethics rules do little to deter attorney conduct. *See* Dale A. Oesterle, *A Private Litigant's Remedies for an Opponent's Inappropriate Destruction of Relevant Documents*, 61 TEX. L. REV. 1185, 1219 (1983). The Model Code of Professional Responsibility deals with evidence destruction only under the auspices of refraining from participating or advising a client to participate in illegal activity. Texas attorneys Cedillo and Lopez call the codes "toothless" to prevent document destruction. *See* Ricardo G. Cedillo & David Lopez, *Document Destruction in Business Litigation From a Practitioner's Point of View: The Ethical Rules vs. Practical Reality*, 20 ST. MARY'S L. J. 637, 640 (1989).

71 The term "spoliation" originates from the doctrine of drawing an adverse inference against one who spoliates, or destroys evidence; it comes from the Latin phrase *omnia praesummuntur contra spoliatorem*. GORELICK, ET AL., *supra* note 8, § 1.3 at 56.

72 *See, e.g.*, Smith, 151 Cal. App. 3d. 491 (Cal. Ct. App. 1984); Bondu v. Gurvich, 473 So.2d. 1307 (Fla. Dist. Ct. App. 1984).

73 *See* GORELICK ET AL., *supra* note 8, § 1.7, at 11-12.

74 *See* Vick v. Texas Employment Comm'n, 514 F.2d. 734, 737 (5th Cir. 1975) (holding that documents destroyed pursuant to regular records destruction policy could not support adverse inference). *Cf.* Lewy v. Remington Arms Co., Inc., 836 F.2d. 1104 (8th Cir. 1987) (case remanded to determine reasonableness of corporate records retention policy).

75 In a prosecution under the Clean Water Act, the district court entered a default judgment for plaintiffs and lev-

"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] compensate[81] and restore accuracy[82] to the fact finding process.

A. Methods Of Controlling Destruction of Evidence

1. Criminal Sanctions

It may surprise the reader that no Federal criminal 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 relevant[86] (3) to a pending judicial proceeding, with[87] (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).

76 *See* John M. Fedders & Lauryn H. Guttenplan, *Document Retention and Destruction: Practical Legal and Ethical Considerations*, 56 NOTRE DAME LAWYER, 5, 18 (1980).

77 See Lawrence B. Solum & Stephen J. Marzen, *Truth and Uncertainty: Legal Control of the Destruction of Evidence*, 36 EMORY L.J. 1085, 1138 (1987).

78 *See* GORELICK, ET AL., *supra* note 8, § 1.13, at 16-18.

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.*

81 *See* Charles R. Nesson, *Incentives to Spoliate Evidence in Civil Litigation: The Need for Vigorous Judicial Action*, 13 CARDOZO L. REV. 793, 800 (1991) (compensation as rationale for discovery sanctions). *See also* GORELICK ET AL., *supra* note 8, § 1.21, at 27.

82 Restoring accuracy is not a solid basis on which to justify destruction of evidence sanctions because courts's 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 relevance; 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.[89] Some federal courts require knowledge that the probable outcome of the defendant's acts will be to obstruct justice.[90] For example, in *United States v. Jeter*,[91] the government prosecuted Jeter on obstruction of justice charges after he distributed grand jury transcripts to the targets of those grand jury proceedings.[92] 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.[93] 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.[94] Chief Judge Haynsworth wrote "[t]hat the defendant's design [was] irrelevant," and as long as the "natural result" of his scheme was to obstruct justice his conviction would stand.[95]

The pendency requirement of 18 U.S.C. § 1503 simply requires presentation of evidence before a grand jury.[96] 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.[97]

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.[98] 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.[99] 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.[100]

2. *Civil Sanctions*

In civil suits, judges rely on the language of Federal Rule of Civil Procedure 37[101] to sanction parties who abuse the discovery process.[102] For example, Rule 37(c) authorizes a court to "impose other appropriate sanctions" where a party does not disclose certain information,[103] comply with a court order,[104] attend a deposition, answer interrogatories, respond to a request for inspection,[105] or fails to formulate a discovery plan.[106]

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

89 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).

90 *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 F2d. 728 (9th Cir. 1972) (obstruction of justice conviction overturned). *See also* United States v. Solow, 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").

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

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

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

94 *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.*

95 Neiswender, 590 F.2d. at 1274.

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

97 *See* United States v. Fineman, 434 F.Supp. 197, 202 (E.D. Pa. 1977).

98 *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).

99 *See* Fedders and Guttenplan, *supra* note 76, at 31.

100 *See id.* at 34.

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

102 *See* Iain Johnston, *Federal Courts' Authority to Impose Sanctions for Pre-litigation or Pre-Order Spoliation of Evidence*, 156 F.R.D. 313, 315-16 (1994). *See* Wm. T. Thompson Co. v. General Nutrition Centers, Inc., 593 F. Supp. 1443 (N.D. Cal. 1984) (ordering dismissal); Nation-Wide Check Corp., Inc. v Forest Hills Distrib., Inc., 692 F.2d. 214, 218-19 (1st Cir. 1982) (affirming trial court's imposition of adverse inference).

103 *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.

104 *See* FED. R. CIV. P. 37(b).

105 *See* FED. R. CIV. P. 37(d).

106 *See* FED. R. CIV. P. 37(g).

The sanctions under Rule 37 are powerful, but are limited to cases where a court already has ordered a party to preserve evidence.[107] 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.[108] 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.[109]

For instance, in *Wm. T. Thompson Co. v. General Nutrition Corp., Inc.*,[110] Wm. T. Thompson Co. ("Thompson") sued General Nutrition Center Corp., Inc. ("GNC") over "bait and switch" advertising practices.[111] Thompson served GNC with requests for production of documents a few weeks after filing suit.[112] 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.[113] The court ordered a default judgment against GNC because it had a duty to preserve these records.[114] Notice was provided before the suit was filed that the documents were relevant to the dispute.[115] 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.[116]

By contrast, the Texas Supreme Court overturned the default sanction ordered by the trial court in *Chrysler Corp. v. Blackmon*[117] after the trial court struck some of Chrysler's pleadings in the context of a wrongful death suit.[118] 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 be excessive.[119] By that standard, the trial court in *Blackmon* abused its discretion when it ordered the "death penalty" sanction[120] 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.[121] Second, default judgment on lia-

107 *See* Solum & Marzen, *supra* note 77, at 1095; Oseterle, *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 794-95.

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. Osterle'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 Lewy 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).

109 Courts have relied on an "inherent power" not specifically vested in the Rules of Civil Procedure to punish spoliators before issuing a specific order not to do so. See Link v. Wabash Railroad Co., 370 U.S. 626 (1962). *Cf.* Cedillo & Lopez, *supra* note 70, at 647-48.

110 *See* generally 593 F. Supp. 1443 (C.D.Cal. 1984).

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

112 *See id.*

113 *See id.* at 1446.

114 *See id.* at 1456.

115 The records were "reasonably likely to be requested by Thompson during discovery in the litigation," and therefore GNC had a duty to preserve them. *Id.* at 1446.

116 *See id.* at 1455 *citing* Bowmar Instrument Corp. v. Texas Instruments, Inc., 25 FED. R. SERV. 423 (N.D.Ind. 1977) and In re Agent Orange Product Liability Litigation, 506 F.Supp. 750 (E.D.N.Y. 1980). *See also* Computer Associates Int'l, Inc., v. American Fundware, Inc., 133 F.R.D. 166 (Colo. 1990). In ordering sanctions, the Colorado court spelled out a three part test: "(1) that [American Fundware] acted willfully or in bad faith; (2) that [Computer Associates Int'l, Inc.] was seriously prejudiced by [American Fundware's] actions; and (3) that alternative sanctions would not adequately punish." *Id.* at 169.

117 See generally 841 S.W.2d. 844 (Tex. 1992).

118 *See id.* at 845. The corporation argued that it had destroyed some records pursuant to its document destruction policy, and thus, were no longer available. *See id.* at 846 n. 6.

119 *See id.* at 844. *See also* Transamerican Natural Gas Corp. v. Powell, 811 S.W.2d. 913 (Tex. 1991). Transamerican involved a breach of contract dispute where a default judgment was entered against TransAmerica after its president did not attend his deposition. The sanctions imposed by the trial court were overturned on appeal on account of their severity. 811 S.W.2d. at 918-919. The appeals court focused on the range of sanctions available to a trial court, and held that the default judgment was not "just" as referred to in Texas Rule of Civil Procedure 215. Transamerican, 811 S.W.2d. at 916, 918.

120 "Death Penalty" discovery sanctions are "those that terminate the presentation of the merits of a party's claims." Blackmon, 841 S.W.2d at 845.

121 *Id.* at 849-50.

bility was more severe than necessary to satisfy the legitimate purposes of sanctions for discovery abuse.[122] Another option for a judge is simply to allow a jury to infer certain facts when evidence destruction comes to light.[123] 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.[124] The key to the spoliation inference is some form of intention to destroy the evidence. Some courts merely require an intent to destroy evidence,[125] while others require a showing of bad faith.[126] One lingering question when using the inference is how much weight to assign to it.[127]

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.*[128] 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.[129] A trial court has wide discretion to impose sanctions once relevancy is established.[130]

3. Suing in Tort to Remedy Destruction of Evidence

Nine states recognize that parties suffer a tortious injury when a party destroys evidence.[131] 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.[132] This new tort, first recognized in *Smith v. Superior*

---

122 *Id.* at 850.

123 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.

FED. JURY PRAC. & INSTR. § 12.05 (1997 supp.). *See also* Vodusek v. Bayliner Marine Corp., 71 F.3d. 148, 154 (4th Cir. 1995).

124 *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 his 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.

125 *See* Solum & Marzen *supra* note 77, at 1088.

126 *See id.* at 1089, n.10. Professor Oesterle argues that bad faith should not be a requirement for the inference because when the fact of destruction is made known to the factfinder, that in itself helps the factfinder determine how much weight to assign to the spoliator's other evidence. Oesterle, *supra* note 70, at 1235. There is also debate over how the adversely affected party can rebut the inference. Courts have accepted such arguments as: reliance on counsel; destruction was beyond the control of the spoliator (which itself lacks intent); other evidence which disproves that the evidence destroyed was what the court presumed it to be; or that the document was irrelevant. *See* Solum and Marzen, *supra* note 77, nn.12, 15, 17.

127 *See* Cedillo and Lopez, *supra* note 70, at 651. Courts have split on whether to allow the inference to justify a verdict against a 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 partrolman 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* Marrocco v. General Motors Corp.,

131 The states that recognize the tort are Alaska, California Florida, Michigan, Mississippi, New Jersey, North Carolina, Ohio, and Oklahoma. See Eric Marshall Wilson, Note, *The Alabama Supreme Court Sidesteps a Definitive Ruling in Christian v. Kenneth Chandler Construction Co. Should Alabama Adopt the Independent Tort of Spoliation?*, 47 ALA. L. REV. 971, 977-78 (Spring 1996).

132 *See* GORELICK ET AL., *supra* note 8, § 4.1 at 140.

Court,[133] was closely analogized to the tort of intentional interference with prospective business advantage.[134]

The *Smith* court spelled out five conditions necessary to prove spoliation of evidence, based on the test to prove intentional interference with prospective business advantage: (1) economic relationship between the moving party and some third person containing the probability of some future economic benefit to the moving party, (2) knowledge by the nonmoving party of the existence of the relationship, (3) intentional acts on the part of the nonmoving party designed to disrupt the relationship, (4) disruption of the relationship, and (5) damages caused by disruption.[135]

Smith stemmed from a personal injury suit in which the defendant car dealership agreed to maintain car parts for investigation.[136] The dealership then lost or transferred the parts, making it impossible to inspect the parts for trial.[137] On an interlocutory appeal, the *Smith* court ruled that "for every wrong there must be a remedy" and thus, a party could be held liable for spoliating evidence.[138] The court based its authority to create the tort in the "probable expectancy" of the impending suit and the harm the plaintiff suffered as a result of the defendant's acts.[139]

A more controversial practice is to sue under the tort of negligent spoliation of evidence.[140] Created in 1984 by a Florida appellate court in *Bondu v. Gurvich*,[141] the court held that a duty existed for a hospital to retain records concerning the victim of an operating room death. The hospital breached that duty when it failed to maintain medical records and treatment notes.[142] Relying on Professor Prosser's words that "new and nameless torts are being recognized constantly" and finding that the hospital owed the plaintiff a duty to preserve the records, the *Bondu* court remanded the case to litigate this new claim.[143] Solum and Marzen reasoned that this negligence tort is sound because it serves the goals of fairness and deterrence.[144]

C. Document Retention Policies: Eliminating Smoking Guns and Nuclear Warheads[145]

The reasons for implementing a document destruction policy are plain.[146] 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.[147] After years of operation, storage costs are staggering for a company such as IBM.[148]

Perhaps the most important reason is that a properly managed records retention policy reduces legal exposure.[149] A document manage-

---

133 *See* Smith v. Superior Court, 151 Cal. App. 3d. 491 (Cal. Dist. Ct. App. 1984).

134 *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. Hale & Norcross Silver Mining Co.*. 41 P. 308 (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 365 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.

135 *See* Smith v. Superior Court, 198 Cal. Rptr. 829, 835 (Cal. App. 2 Dist. 1984). *See infra* note 180 and accompanying text for the test in its exact terms.

136 *See id.* at 494.

137 *See id.*

138 *Id.* at 496.

139 *Id.* at 502. Alaska established the tort in *Hazen v. Anchorage. See generally* 718 P.2d. 456 (Alaska 1986).

140 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, Mississippi, and Oklahoma have recognized the tort of negligent spoliation of evidence. *See* Wilson *supra* note 131, 978-79.

141 *See* 473 So. 2d. 1307 (Dist. Ct. App. 1984). California established the tort in *Velasco v. Commercial Building Maintenance Co.*, by borrowing from the tort of negligent interference with prospective economic advantage. *See generally* 169 Cal. App. 3d. 874 (1985). The court applied a six-part test: (1) the extent to which the transaction was intended to affect the plaintiff, (2) foreseeability of harm to the plaintiff, (3) degree of certainty of the plaintiff's separate inquiry, (4) the closeness of the connection between defendant's conduct and the injury suffered, (5) the moral blame attached to the defendant's conduct, and (6) policy of preventing future harm. *See id. at* 877-79 (1985). Because the claim in *Velasco* failed the second prong, the case was dismissed. *See id.*

142 *See id.* at 1312.

143 *Id.* at 1312-13, *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.

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

145 *See* Allen, *supra* note 10.

146 *See* Betty Ann Olmstead, *Electronic Media: Management Litigation Issue When "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 532 (1996).

147 *See* Fedders and Guttenplan *supra* note 76, at 11.

148 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).

149 Fedders and Guttenplan outlined the advantages and

ment program performed routinely is much less likely to raise eyebrows than one done informally or on an as-needed basis.[150] A retention program must make sure that (1) companies preserve documents to comply with laws and regulations for as long as necessary, (2) companies file documents necessary for the conduct of business in a systematic way to ease access, (3) they keep documents that the they know will be relevant in a judicial, investigative or congressional investigation, (4) that permanent documents are stored on microfilm to aid storage and retrieval, and (5) everything else is destroyed.[151]

For example, in *Lewy v. Remington Arms Co.*,[152] the Eighth Circuit Court of Appeals created a test for the reasonableness of such a records retention policy. The plaintiff brought a products liability action when she was injured accidentally by her son's gun.[153] After an adverse jury verdict, Remington argued that the inference imposed by the trial court was unwarranted because the documents were destroyed pursuant to its routine document destruction procedures.[154]

The appellate court remanded the case to the trial level to determine (1) if Remington's record retention policy was reasonable considering the circumstances surrounding the relevant documents;[155] (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]

---

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.

150 Welsh and Marquardt, *supra* note 124, at 36, contending that any ad hoc document destruction done without a record management plan will be "viewed with . . . . suspicion." Gorelick et al. wrote that "cavalier" document destruction invites "grave risks." *Supra* note 8, § 8.1 at 276. *See generally* GNC, 593 F. Supp. 1443 (C.D. Cal. 1984) at 1446-50; King v. National Security Fire and Casualty Co., 656 So.2d. 1335, 1336-37 (Fla. Dist. Ct. App. 1995); Willard v. Caterpillar Inc., 40 Cal.App.4th 892, 905-06 (Cal. Ct. App. 1995).

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

152 *See generally* 836 F.2d. 1104 (1988).

153 *See id.* at 1105.

154 *See id.* at 1111. The documents in this case were records of complaints and gun examination reports. *See id.* If no action was taken concerning these documents, Remington destroyed them after three years. *See id. See also* Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472 (S.D.Fla. 1984) (where court entered default judgment against Piper because it failed to show it complied with its own document retention policy).

155 *See* Lewy, 836 F.2d. at 1112. The court asked, "For example, the court should determine whether a three year retention policy is reasonable given the particular document." *Id.* The remanded case was not reported nor available on Westlaw. *See id.*

156 *See id.*

157 *See id.*

158 *See id.*

159 *See* 169 F.R.D. 598 (D. N.J. 1997).

160 *See id.* at 612.

161 *See id.* at 607-10, 611-12.

162 *See id.* at 616-17.

163 *See id.* at 616. In October 1997, The Wall Street Journal reported that the plaintiffs' attorneys discovered that 1,200 documents, including some key documents in the litigation, were thrown into a trash bin at Prudential's offices. See Leslie Scism, *Prudential Tried to Destroy Papers, Lawyer Alleges*, WALL ST. J. Oct. 7, 1997 at B10.

164 *See generally* 1 F.3d. 1274 (D.C. Cir. 1993), *rev'd on other grounds*, 90 F.3d. 553 (1996).

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.[165] At issue, *inter alia*,[166] were the duties of federal agencies to preserve electronic documents — e-mail messages.[167] The district court found that agencies' practice of printing out e-mails which employees thought fell under the Federal Records Act[168] was insufficient because the information on-screen contained data which the printed copy did not.[169] 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.[170] The D.C. Circuit Court of Appeals ultimately reversed itself on other grounds.[171]

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.[172] 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.[173] Yet many computer users mistakenly believe when the message leaves their "inbox" it is gone forever.[174] Courts have little trouble overruling employees' privacy claims when superiors monitor their transmissions.[175] 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.[176]

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.[177] 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

165 At the same time, plaintiffs filed Freedom of Information Act requests for material stored electronically on systems in the Executive Office of the President and the National Security Council. *See id.* at 1280.

166 *See* 44 U.S.C. § 3105; *see also* Armstrong v. Bush, 924 F.2d. 282, 293 (D.C. Cir. 1991). A long procedural history preceded this opinion, and defendants initially agreed to preserve the computer tapes, but also filed a motion for dismissal, or alternatively, for summary judgment. *See* Armstrong, 1 F.3d. at 1280. That motion was denied in *Armstrong v. Bush*, 721 F.Supp. 343 (D.D.C. 1989). Next, the D.C. Circuit court held on an interlocutory appeal, first, that the plaintiffs had standing, and that only the agencies' destruction programs could be reviewed. *See* Armstrong, 1 F.3d. at 1280, *citing Armstrong v. Bush*, 924 F.2d. 282, 287-288. Then, the case was remanded to determine what instructions the agencies gave their employees, and on remand, the district court determined electronic communications were included within the meaning of the FRA, and determined that the agencies' methods for preserving the communications was insufficient under the FRA. *See* Armstrong, 1 F.3d. at 1281, *citing* 924 F.2d. at 340-341.

167 *See* Armstrong, 1 F.3d. at 1274.

168 *See* 44 U.S.C. §§ 2101 et seq., 2901 et seq., 3101 et seq.

169 The district court also found that the record keeping method was "arbitrary and capricious" because individual employees, instead of designated records managers, made decisions to dispose of records. *Armstrong*, 1 F.3d at 1281, *citing* 924 F.2d. at 347.

170 *See id.* at 1287-88.

171 *See generally* 90 F.3d. 553 (1996).

172 *See* John Montaña, *Record Retention Schedules in Court: The Pitfalls* 10/96 REC. MGMT. Q. 32.

173 *See* Betty Ann Olmstead, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523 (1996).

174 *Id.* at 523; *see also* Kim S. Nash, *Computer Detectives Uncover Smoking Guns: Cybersleuths Glean Evidence From Backup Tapes*, COMPUTER WORLD, June 9, 1997 at 1.

175 *See* Jonathan Rosenoer, CYBERLAW 168 (1997).

176 *See* Strauss, 814 F. Supp. 1186 (S.D.N.Y. 1993); Markels, *supra* note 5.

177 *See* FED. R. CIV. P. 37(b)(2).

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.

181 *See* Willard v. Caterpillar, Inc., 40 Cal. App. 4th 892, 910-11 (Cal. Ct. App. 1995).

182 *See* Welsh and Marquardt, *supra* note 124.

183 *See* John Montaña, *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 § 240.17a3(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.

> "Archivists 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.[186] With improved technology, electronic storage adds another layer of complexity to companies' storage needs.[187] The three criteria spelled out in *Remington*, along with the analysis provided by *Armstrong*, should give companies a clearer understanding of courts' concerns when electronic messages are destroyed.

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.

---

nently e-mail as quickly as 90 days or as late as one year to avoid liability. See Barb Cole-Gomolski, *Lethal Sting of Forgotten Mail: IS Examines Policy as Costly Suits Pile Up*, COMPUTER WORLD, Sept. 8, 1997 at 117.

186 *See* Markels, *supra* note 184.

187 *See* Cox, *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, *supra* note 183. *See also* Lovell and Holmes, *supra* note 19.