1-1-2004

Paper Piles to Computer Files: A Federal Approach to Electronic Records Retention and Management

Marilee S. Chan

Follow this and additional works at: http://digitalcommons.law.scu.edu/lawreview

Part of the Law Commons

Recommended Citation
Available at: http://digitalcommons.law.scu.edu/lawreview/vol44/iss3/4

This Comment is brought to you for free and open access by the Journals at Santa Clara Law Digital Commons. It has been accepted for inclusion in Santa Clara Law Review by an authorized administrator of Santa Clara Law Digital Commons. For more information, please contact sculawlibrarian@gmail.com.
PAPER PILES TO COMPUTER FILES: A FEDERAL APPROACH TO ELECTRONIC RECORDS RETENTION AND MANAGEMENT

MARILEE S. CHAN*

I. INTRODUCTION

In today's technology-savvy world, companies are now creating enormous trails of electronic information instead of stacks of paper files. Businesses are able to save nearly every document because electronic information can be stored easily. Technological advancements not only have revolutionized the way in which businesses conduct transactions but also have affected the way companies resolve business disputes. "Litigation is increasingly becoming a digital battleground," as many causes of corporate liability have either indirectly or directly resulted from the electronic creation, storage, and transmission of information. However, because the main issues in most cases do not center on discovery of electronic documents, only a minority of published opinions discuss the subject extensively.

This comment discusses the responsibilities that publicly traded companies have to manage these bits and bytes and the increased corporate liability that is created with the

---

* Comments Editor, Santa Clara Law Review, Volume 44. J.D. Candidate, Santa Clara University School of Law; B.S. Business Administration, Haas School of Business, University of California, Berkeley.


4. Id.

5. See infra Part II.A.
transformation from paper records to corporate electronic records.\textsuperscript{6} The comment considers the various features of electronic documents and explores the myriad of current non-homogeneous retention and destruction policies governing these electronic documents.\textsuperscript{7} Next, it specifically addresses the problem of enhanced corporate liability due to both the mismanagement of electronic records and employee misuse of electronic communications.\textsuperscript{8} In conclusion, the comment proposes that the Securities Exchange Commission\textsuperscript{9} implement a federal electronic records retention policy, based upon the regulations\textsuperscript{10} adopted by the National Archives and Records Administration ("NARA"),\textsuperscript{11} in order to provide publicly traded companies uniform legal standards regarding management of electronic records.\textsuperscript{12}

II. BACKGROUND

A. Federal Regulation over Publicly Traded Companies

The Securities Act of 1933\textsuperscript{13} requires public companies to disclose pertinent financial data and other related information that will allow investors to judge whether a company's securities are a good investment.\textsuperscript{14} Congress passed the Securities Act of 1933 to achieve two primary objectives: (1) to ensure that investors receive financial and other significant in-

\textsuperscript{6} See generally infra Part II.
\textsuperscript{7} See infra Part III.
\textsuperscript{8} See infra Part IV.
\textsuperscript{9} See generally United States Securities & Exchange Commission web site, at http://www.sec.gov (last visited Feb. 12, 2004); see also infra Part II.A.
\textsuperscript{10} See infra Part II.F.
\textsuperscript{11} The United States National Archives and Records Administration (NARA) is an independent federal agency that preserves and oversees the management of all federal records that document the rights of American citizens and actions of federal officials. See http://www.archives.gov (last visited Jan. 4, 2004).
\textsuperscript{12} See infra Part V.
\textsuperscript{14} See, e.g., Cent. Bank, N.A. v. First Interstate Bank, N.A., 115 U.S. 164 (1994); A.C. Frost & Co. v. Coeur D'Alene Mines Corp., 312 U.S. 38 (1941); United States v. Custer Channel Wing Corp., 247 F. Supp. 481 (D.C. Md. 1965), aff'd by 376 F.2d 675 (4th Cir. Md. 1967). "Securit[ies]" is defined as "[a]n instrument that evidences the holder's ownership rights in a firm (e.g., a stock), the holder's creditor relationship with a firm or government (e.g., a bond), or the holder's other rights (e.g., an option)." BLACK'S LAW DICTIONARY 1358 (7th ed. 1999).
formation concerning securities being offered for public sale; and (2) to prohibit deceit, misrepresentations, and other fraud in the sale of securities. Most companies wishing to sell securities publicly in the United States must register with the United States Securities and Exchange Commission ("SEC"). In general, registration requires "a description of the company's properties and business; a description of the security to be offered for sale; information about the management of the company; and financial statements certified by independent accountants." Registration statements and prospectuses approved by the SEC become available to the public shortly after filing, and hence, the company is deemed publicly traded.

Not all offerings of securities must be registered. There are several exemptions from the registration requirement, including "private offerings to a limited number of persons or institutions; offerings of limited size; intrastate offerings; and securities of municipal, state, and federal governments." These exemptions from the registration process allow continuation of capital formation and economic growth by lowering the cost of offering securities to the public.

The SEC is the federal agency appointed to oversee all aspects of the securities industry. The Securities Act of 1934 empowers the SEC with broad authority to register, regulate, and oversee securities trade. Companies must register with

---


17. See id.; see also 15 U.S.C. §§ 77a, 77aa (listing specific requirements for registration).


19. See id.; see also 15 U.S.C. § 77d.


22. The SEC is an "agency" defined as "a governmental body with the authority to implement and administer particular legislation." BLACK'S LAW DICTIONARY, supra note 14, at 49.


24. Id. § 77s.
the SEC to become publicly traded and are subject to the federal regulations and laws mandated by the SEC; however, these companies are not considered to be an agency or branch of the United States federal government.\(^2\)

**B. Defining the “Corporate Record”**

In general terms, a record is an account of information or facts set down in writing to preserve knowledge.\(^2\) From a legal standpoint, a record is more specifically defined as a documentary account of past events inscribed on a tangible medium or stored in an electronic form that is retrievable in a perceivable form.\(^2\)

Given the various definitions of a record, a company must know the requirements to establish an official corporate record. A corporate record can be defined broadly as any record created by an employee of a company.\(^2\) More specifically, corporate records can be classified into two distinct forms: 1) permanent records that are created and remain unchanged from the time of creation; and 2) transactional records that are typically updated to reflect obligations, communications, or regularly occurring expenditures.\(^2\)

In this comment, references to corporate records will include both permanent and transactional records. Additionally, the term “document” and “record” will be used interchangeably because the word “document” has been defined broadly in other legal contexts as “any physical embodiment of information or ideas.”\(^3\)

Corporate records are most always at the center of litigation\(^3\) and in turn, can be fatal to a company’s existence if the litigation is lost. Effective in November 1991, Chapter 8 of the Federal Sentencing Guidelines emphasizes the importance of maintaining corporate records.\(^3\) The Guidelines


27. BLACK'S LAW DICTIONARY, supra note 14, at 1279.


29. Id.


32. See id. § 1:25.
state that culpability for corporate crimes should generally be
determined "by the steps taken by the organization prior to
the offense to prevent and detect criminal conduct . . . and the
organization's actions after the offense has been committed." The
corporate records are key to showing both criminal and
civil culpability in litigation, as they reflect the extent of a
company's compliance program. Moreover, corporate rec-
cords represent a running log of the company's actions and
monitor the efforts the company has taken to deal with prob-
lems.

C. Overview of Corporate Records Retention Schedules

Nearly all companies engage in work that involves the
creation of records. In turn, the important question becomes
how long must records be kept. Companies currently face
significant challenges devising corporate document retention
programs that comply with the myriad of federal and state
statutes and regulations. To further complicate matters, the
obligation to meet these legal requirements merely provides
minimum standards for records retention guidelines. The
company's business or operational needs often require keep-
ing information longer than the law requires.

The corporate retention program is a balance between
the potential consequences of destroying corporate documents
that will be needed later and the savings that will be realized
by reducing the clutter around valuable documents. Moreover, the larger the number of records stored, the slower and
more rigorous the search for them will be.

D. History of Storage Mediums for Corporate Records

Companies historically regarded paper as the best vehicle
for the storage of records, as paper records were an excellent

33. See id. (citing the introductory comments of the FEDERAL SENTENCING
GUIDELINES MANUAL 347 (1992) and 18 U.S.C. app. ch. 8)).
34. See id.
35. See id.
36. See id. §1:1.
37. See Dietel, supra note 28, § 1:26.
38. Id.
39. See id.
40. See id.
41. See id. § 3:89.
long-term storage medium. Many companies developed systems to make filing, finding, and retrieving paper documents easy and efficient for business. However, paper records also proved to be bulky, heavy, susceptible to misfiling, environmentally threatening, expensive for business, and costly to store. Corporate records managers began to search for alternative mediums. Many managers opted to reduce the size of paper records through the attractive photographic process of microfilming. Despite the considerable space saved by microfilming, managers soon realized that microfilm offered no significant advantage over its paper counterpart. The task of physically retrieving and refiling the microfilm became labor exhaustive, required companies to invest in expensive equipment necessary for viewing and replication, and made indexing information more difficult.

As a result of the technology boom in the last quarter of the twentieth century, computers have become so commonplace that most corporate records are now stored electronically. A principle advantage of storing corporate records in an electronic form is that electronic records contain what is referred to as “metadata.” Metadata contains information such as the date the electronic document was created, the time that a recipient received the message, the status of the messages, and the name of the person, if any, to whom the recipient forwarded the message. Electronic records converted
to hard copies usually do not contain metadata information.51

E. Sources of Electronically Stored Information and the Corporate Document Disclosure Obligations

The prevalence of electronic discovery in many litigation matters should not be surprising since approximately seventy percent of business documents are now created electronically and are never printed.52 Therefore, it is imperative that corporate employees are technologically savvy about where and how electronic information may be stored.53

Desktop computers at employee workstations are the most common electronic medium to store corporate information, but there are a great number of other potential sources, including but not limited to laptops, personal digital assistants ("PDAs"), home computers, floppy disks, hard drives, CD-ROM devices, backup magnetic tapes, backup storage on the Internet, zip drives, e-mail servers, program files such as word processing documents or spreadsheets, voicemail, and digital cameras.54

Electronic mail ("e-mail") can be distributed easily to a large group of people and stored on both the sender and the recipient's computers.55 E-mail may also have multiple cloned copies on each system and can be forwarded to third party recipients with the click of a button.56 "In comparing this with copy proliferation that has multiplied exponentially through photocopiers and fax technology, [e]-mail will make that proliferation look minuscule in comparison."57

the document was created, the identity of the author; the identity of subsequent editors, the distribution route for the document, or the history of editorial changes") (alteration in original).

51. See Traynor & Ploeger, supra note 49, at 64.
54. See id. (providing a non-exclusive list of common electronic storage types). For specific definitions of each electronic storage medium listed, please refer to the DICTIONARY OF COMPUTER AND INTERNET TERMS (8th ed. 2003); see also DILLON & LEONARD, supra note 50.
55. See Traynor & Ploeger, supra note 49, at 57; see also DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 163-64.
56. See Traynor & Ploeger, supra note 49, at 57; see also DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 163-64.
57. See Dietel, supra note 28, § 3:88, at 1.
The Internet also employs a plethora of its own storage mediums, including but not limited to web sites, intranets and extranets, cache files,\textsuperscript{58} Internet browser history files, site log files, bookmarks,\textsuperscript{59} and cookies.\textsuperscript{60} Cookies, in particular, store important information such as usernames, passwords, and personal preferences.\textsuperscript{61} Additionally, the directory containing the “cookies” files on the user’s hard drive may reveal information regarding the user’s activities on the Internet.\textsuperscript{62}

To add to the hodgepodge of different ways to store digital information, electronically stored documents can also be categorized\textsuperscript{63} as active data,\textsuperscript{64} embedded or metadata,\textsuperscript{65} replicant data,\textsuperscript{66} residual data,\textsuperscript{67} back up data,\textsuperscript{68} or legacy data.\textsuperscript{69} Each of these six types of data could be considered a corporate

\textsuperscript{58} A “cache” is “a set of files kept by a [web browser] to avoid having to download the same material repeatedly.” DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 73.

\textsuperscript{59} A “bookmark” is “a remembered address on the [World Wide Web]. Web [browsers] normally let the user record the addresses of web pages in order to go directly to them in the future without having to type the address.” Id. at 59.

\textsuperscript{60} See Traynor & Ploeger, supra note 49, at 55-56 (providing a non-exclusive list of common electronic storage types). For specific definitions of each electronic storage medium listed, see generally DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54.

\textsuperscript{61} “[W]eb sites] use cookies to recognize users who have previously visited them . . . . The term cookie comes from a 1980s prank computer program called Cookie Monster that would interrupt users and demand that they type the word ‘cookie’ before continuing.” DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 115 (emphasis in original).

\textsuperscript{62} See Traynor & Ploeger, supra note 49, at 56 n.11.

\textsuperscript{63} See id. at 56.

\textsuperscript{64} See id. at 56 n.13 (“Active data consists of information readily available and accessible to computer users through file manager programs.”).

\textsuperscript{65} See DILLON & LEONARD, supra note 50.

\textsuperscript{66} See Traynor & Ploeger, supra note 49, at 56 n.15 (“Replicant data are copies automatically made and saved to the user's hard drive.”).

\textsuperscript{67} See id. at 56 n.16 (“Residual data are deleted files to which the reference has been removed from the directory listings and the file allocation table, but which have not been overwritten.”).

\textsuperscript{68} A “backup copy” is “a copy of working programs and related files that can be used to restore lost or damaged programs and files.” DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 41; see also Traynor & Ploeger, supra note 49, at 56 n.17 (“Back up data consist of information copied to removable media in the event of a system failure, usually only of data on a centralized storage medium or network, and frequently in compressed form.”).

\textsuperscript{69} “Legacy” data is data “left over from a previous version of the hardware or software.” DICTIONARY OF COMPUTER AND INTERNET TERMS, supra note 54, at 284; see also Traynor & Ploeger, supra note 49, at 56 n.18 (“Legacy data consist of information stored on media that can no longer be accepted or organized in a format that can be read using current software.”).
record subject to the disclosure and discovery obligations of materials under Federal Rules of Civil Procedure 26(a)(1)(B)\textsuperscript{70} and 34(a).\textsuperscript{71} Although the literal language of Rule 26(a)(1)(B) is silent on electronic documents, the 1993 advisory committee notes clarify that disclosure "include[s] computerized data and other electronically-recorded information . . . .\textsuperscript{72} Similarly, the 1970 advisory committee notes of Rule 34(a) make clear that electronic data is part of the definition of "document."\textsuperscript{73} Electronic discovery is also encompassed in the parties’ meet and confer obligations under Federal Rule of Civil Procedure 26(f), which states that a party responding to a request for production has the duty to search all available electronic systems for the information.\textsuperscript{74}

Even documents that have been “deleted” are subject to discovery. The district court in \textit{Simon Property Group L.P. v.}
mySimon, Inc. held that “[c]omputer records, including records that have been ‘deleted,’ are documents discoverable under [Federal Rule of Civil Procedure 34].” The court declared that there is no such thing as “deleting” computerized data because “[d]eleting a file does not actually erase that data from the computer’s storage devices.” Courts have clarified that:

[m]anual or automated deletion of... software may remove superficial indicia .... However, telltale traces of a previous installation remain, such as abandoned subdirectories, libraries, [and] information in system files .... [T]he operating system does not actually erase the files, but merely marks the space consumed by the files as free for use by other files.

Most corporate electronic systems have a scheduled “back-up” system that duplicates and transfers information by recording it to a tape. Often messages and information on a back-up system are filed by date, sender, and recipient and are not erased until the corporate schedule commands it to. Recovery may still be possible even in the case where no clone or back-up version is created.

Typically, when computers “write” data onto a storage device (such as a hard disk), they first check the storage device’s “directory” to locate unused bits of storage onto which the data may be written. After locating free “memory” sufficient to record the data, the computer then (1) writes the data onto the free bits of disk space, and (2) edits the directory to make sure that area of storage is marked “in use” – the computer will not use that space to store other data in the future.

In turn, erasing a file does not actually expunge the data from the computer’s storage devices but instead finds the data’s entry in the disk directory and changes it to a “not
used" status. The information is not erased entirely because computer systems are designed only to delete information if it is entirely written over with new information. Accordingly, many files are recoverable long after they have been deleted...

It is of utmost importance that a party in litigation take reasonable steps to ensure that it discloses any relevant “deleted” electronic corporate records. Courts have imposed heavy sanctions for both willfully and negligently destroying electronic records. In Crown Life Insurance Co. v. Craig, the appellant filed suit alleging that the appellees had wrongfully drawn checks on the appellant’s branch bank account. The court issued a sanction for the appellant’s failure to comply with discovery orders, finding that the appellant had willfully violated discovery orders for “written documents” by failing to make certain raw electronic data available. Similarly, in In re Prudential Insurance Co. Sales Practice Litigation, the plaintiff brought a class action suit against the defendant alleging deceptive sales practices. The court ordered all parties to preserve documents and other records potentially relevant to the litigation. The defendant did not take active steps to cease electronic records destruction in the normal course of business. Consequently, the court found the defendant grossly negligent for persistent and recurrent destruction of documents and imposed a $1 million sanction.

F. Federal Policies Mandating Electronic Records Retention

Most federal administrative and regulatory agencies that have proper jurisdiction over a specific industry have regulations and policies that apply to and govern the company’s records retention requirements. Unfortunately, there is little

82. See id.
83. Id.
84. See id.
85. See id. at 380-81 (noting that the broad language of FED. R. CIV. P. 26 includes disclosure of deleted electronic documents).
86. 995 F.2d 1376 (7th Cir. 1993).
87. Id. at 1383-84.
89. Id. at 612.
90. Id. at 601, 612-13.
91. Id. at 615-17.
92. See Dietel, supra note 28, § 1:56.
uniformity among these requirements, and often companies must comply with more than one federal agency.93 Furthermore, only a small number of policies include governance and management of electronic records and even fewer polices are designed specifically to address electronic document retention.

In 1992, the Internal Revenue Service passed Revenue Procedure 91-59 to create the first policy mandating specific requirements for electronic document retention of commercial enterprises.94 In 1995, the National Archives and Records Administration ("NARA")95 mandated regulations for all electronic records of the federal government with the General Record Schedule 20 ("GRS 20").96 GRS 20 outlines mandatory procedures for the destruction of records. Federal records may not be destroyed unless the records disposition schedule authorizes destruction.97 The Archivist of the United States must approve the records disposition schedule. "The records schedules indicate how long a document must be kept before it is transferred to a Federal Records Center, destroyed or transferred to NARA for permanent preservation."98

Currently, GRS 20 is one of the most evolved and complete set of guidelines created by any federal agency in the area of electronic documents, particularly in the area of e-mail regulations.99 These guidelines only apply to government agencies and do not apply to the private organizations they govern.100 For example, the SEC must follow the electronic guidelines of GRS 20 pertaining to any records that a publicly traded company files with the SEC. However, all other corporate records of the publicly traded company are managed privately within the corporation and are regulated

93. See id.
95. See supra note 11.
96. See Dietel, supra note 28, § 3:99.
98. Id.
99. See Dietel, supra note 28, § 3:99 (citing de Castro, NARA's Recent E-mail Regulations and Their Possible Private Sector Applications, 3 DATA L. REP. 24, 25-27 (1996)).
by other federal or state corporate governance laws.

Congress’s passage of the Sarbanes-Oxley Act of 2002 represents the latest federal regulation pertaining to electronic documents.101 The Sarbanes-Oxley Act requires corporate and accounting reform for public companies and the accounting firms who audit them.102 Of particular importance is section 802 of the Act, which is intended to address the “destruction or fabrication of evidence and the preservation of financial and audit records.”103 Section 802 requires the SEC to “promulgate rules related to the retention of records relevant to the audits and reviews of financial statements that issuers file with the Commission.”104

In response to the section 802 requirement, the SEC passed the Retention of Records Relevant to Audits and Reviews Rule (“the Rule”) effective March 3, 2003.105 The Rule requires that “the accountant shall retain . . . workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records). . . .”106 Critics of the Rule state that it does not define important terms, such as electronic records, nor does it clarify the procedures to be followed with respect to electronic records.107 Many companies are also concerned that the Rule requires exhaustive effort to develop new systems and procedures to identify communications that must be retained.108 Several commentators have suggested that the definition of “other

102. See Bastian, supra note 95, at 170 (“The [Sarbanes-Oxley Act] is structured to cover a broad range of companies . . . . [A]ny company that files or has filed a registration statement that has not yet become effective under the Securities Act of 1933 . . . and that it has not withdrawn, also will be covered.”).
103. See Retention of Records Relevant to Audits and Reviews, 17 C.F.R. § 210; see also Sarbanes-Oxley Act § 802.
104. See Sarbanes Oxley-Act § 802.
106. Id.
108. Id.
documents' be more clearly described”\textsuperscript{109} and that the Rule only apply to "reasonably . . . relevant records."\textsuperscript{110}

In conjunction with the Sarbanes-Oxley Act, the SEC's Rule may be a forewarning for future regulations to come, as one commentator notes that "[t]he financial industry is not the only business sector affected by the dangers of digital data . . . . All business organizations should bear in mind that retained and deleted electronic evidence could become intricate minefields of liability."\textsuperscript{111}

III. IDENTIFICATION OF THE PROBLEM

The ease of computer-generated information allows companies to create, process, and store information at unprecedented rates, resulting in an out-of-control "store everything" mentality.\textsuperscript{112} Supervisory review of data is often overlooked, and unreviewed information can grow to an unmanageable size.\textsuperscript{113}

The lack of a uniform corporate electronic record retention policy perpetuates the problem of unreviewed information. In turn, the mismanagement of such electronic records results in an increase in corporate losses and liability. "Even when electronic communications are not directly the source of corporate liability, they [are] the undoing of [companies] during litigation - as evidentiary smoking guns or as the source of sanctions or unfavorable inferences for spoliation\textsuperscript{114} of electronic documents."\textsuperscript{115} Outdated e-mails, ancient files, and archival information may be stored on backup electronic medi-


\textsuperscript{111.} See Lange, supra note 2.

\textsuperscript{112.} See Dietel, supra note 28, § 3:87.

\textsuperscript{113.} See id.

\textsuperscript{114.} "Spoliation" is the legal term for "[t]he intentional destruction, mutilation, alteration, or concealment of evidence, [usually] a document. If prove[n], spoliation may be used to establish that the evidence was unfavorable to the party responsible." BLACK'S LAW DICTIONARY, supra note 14, at 1409.

\textsuperscript{115.} Peter Brown, Policies for Corporate Internet and E-Mail Use, 564 PRACTISING L. INST. PAT., COPYRIGHTS, & LITERARY PROP. 637, 639 (1999).
ums such as tapes and disks which can be kept years past their useful life. There is also an assumption that electronic documents are less formal than paper documents and thus, are not shuffled into the files of permanent records which would be subject to discovery in litigation. Due to the misperception that electronic communication is informal, employees tend to use their corporate e-mail accounts or other electronic communication systems for personal use to e-mail jokes, conduct romances, criticize colleagues, or complain and gripe about work conditions. Countless employees are guilty of sending or downloading inappropriate content and posting corporate trade secrets, confidential information, or protected works. Corporate employees continue to engage in such conduct, believing that such evidence can be deleted.

However, all of the above-mentioned information may become an "unintentional" corporate record with great reprisal. This can come back to "haunt a [company] when litigation ensues," as the electronically stored information that could have been destroyed may still be used against a company to its own detriment during discovery. On the contrary, electronic information can also be the "source of sanctions," because permanently deleting or misplacing electronic documents may lead to allegations of concealment or destruction of evidence. It may seem obvious that if a corporation is contemplating a lawsuit, it will indeed preserve any pertinent information and records; however, keeping electronic documents from being inadvertently destroyed may not be as conspicuous as it seems. "If a [company] has a well-established document retention and destruction policy, it would be easy to overlook the fact that documents are being destroyed in the course of daily operations."

116. See Lange, supra note 2.
117. See Dietel, supra note 28, § 3:88.
118. See id.
119. See Brown, supra note 109, at 639-46.
120. See generally id.
121. See Nimsger & Lange, supra note 1, at 18.
122. See Dietel, supra note 28, § 3:87.
123. See Nimsger & Lange, supra note 1, at 17.
Recent court rulings emphasize the importance of managing electronic records for production of evidence. Although courts have not decided whether or under what circumstances a party is required to produce information in electronic form, courts have generally emphasized that a computer-generated printout presented as evidence is not equivalent to an electronically stored record itself.\textsuperscript{125} For example, in \textit{American Bankers Insurance Co. v. Caruth},\textsuperscript{126} the court entered a default judgment against a party for failing to produce the requested computer files despite having submitted 30,000 boxes of materials that contained the same information.\textsuperscript{127} Computer-stored information is often more comprehensive than paper print-out substitutes, and a hard copy of a document that is merely scanned by the opposing party does not contain all the information as in its native electronic form.\textsuperscript{128}

Accordingly, it is vital for companies to devote extraordinary attention to records that are stored in electronic form.\textsuperscript{129} However, no federal law solely addresses the management of electronic records retention and destruction.\textsuperscript{130} Companies are accountable for their own policies, yet are still responsible for incorporating a myriad of inconsistent state and federal laws. In light of this problem, it is critical to reassess the lack of uniformity in electronic records policies and the consequences that follow.

\textbf{IV. ANALYSIS}

“Mismanagement of e-mail and other electronic documents can complicate the defense or prosecution of lawsuits to which the [company] is a party and potentially expose a

\textsuperscript{125} See Anti-Monopoly v. Hasbro, Inc., No. 94CIV.2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1991) (holding that production of information in “hard copy” does not preclude a party from receiving the same information in electronic form); see also Dietel, supra note 28, § 3:87; cf. United States v. Davey, 543 F.2d 996, 1000 (2d Cir. 1976) (holding that the production of magnetic tapes was required even though identical information had been previously provided in printed-out form).

\textsuperscript{126} 786 S.W.2d 427 (Tex. App. 1990).

\textsuperscript{127} Id.

\textsuperscript{128} See Traynor & Ploeger, supra note 49, at 64.

\textsuperscript{129} See Dietel, supra note 28, § 3:87 (“It is easy to continue to save all information and materials created because the computer helps organize and retrieve specific information from mountains of stored information.”).

\textsuperscript{130} See Dietel, supra note 28, § 1:56.
The company has a duty to preserve any relevant or responsive records once it is on notice of a formal investigation or litigation. However, corporations have experienced increasing problems fulfilling this duty, given the nature of electronic documents and the relative ease of deleting or losing electronic documents. On the other hand, many electronic records are kept years beyond their useful life. Such unwieldy preservation can actually be the downfall of a company during the discovery process in litigation. This latter problem is addressed first.

A. Preventing Unnecessary Discovery Disputes

The preservation of all electronic data and e-mail created in the course of business can devastate a company when litigation proceeds, even when that company has adopted a formal document retention and destruction policy for electronic documents. In *Murphy Oil USA, Inc. v. Fluor Daniel, Inc.*, the court stated “[Defendant’s] e-mail retention policy provided that backup tapes were recycled after 45 days. If [defendant] had followed this policy, the e-mail issue would be moot.” As a result of the failure to adhere to its own document retention policy, the defendant spent a substantial amount of both time and money in contention over the discoverability of electronic documents that should have been destroyed. Clearly, corporate liability can be increased unnecessarily by retaining outdated electronic documents. Even if a company has established an electronic document retention policy, such policy serves no purpose unless it is strictly followed.

However, even if a company strictly adheres to its electronic document retention policy, there still remains the difficulty of completely deleting electronic documents unless a
company implements a conscious routine destruction schedule.\textsuperscript{139} Certain electronic documents may be outdated and legally may be deleted; however, even though “deleted,” they are nevertheless recoverable and thus, still subject to production during discovery.\textsuperscript{140} "Unlike the world of paper documents, where data destruction requires an overt act (i.e., putting a document in the shredder), electronic data is lost every day... merely by maintaining the status quo."\textsuperscript{141} Some courts have ruled that discovery of “deleted” electronic documents is only allowed to a “reasonable” extent;\textsuperscript{142} however, to avoid discovery of “deleted” electronic documents, a company must implement a routine destruction schedule that completely erases the information.

\textbf{B. Preventing Spoliation of Electronic Records}

The sanctions for failing to generate electronic records after receiving a request can be severe.\textsuperscript{143} The willful destruction of electronic records may clearly subject a company to sanctions, as in \textit{Crown Life Insurance Co. v. Craig},\textsuperscript{144} where failure to produce data in electronic form in response to a request for “written documents” resulted in severe sanctions for “willful misconduct.”\textsuperscript{145}

Even the negligent destruction of electronic records can result in a company sanction. The court in \textit{In re Prudential Insurance Co. Sales Practices Litigation}\textsuperscript{146} imposed a whopping $1 million sanction, as well as reimbursement of attorneys’ fees, even though it found no willful destruction of electronic records.\textsuperscript{147} In many spoliation matters such as \textit{Prudential}, courts have held consistently that litigants have a duty to interrupt regular “recycling” techniques.\textsuperscript{148} Informa-

\begin{itemize}
\item \textsuperscript{139} See supra Part II.E (explaining why electronic information is not completely deleted).
\item \textsuperscript{140} See supra Part II.E.
\item \textsuperscript{141} See Nimsger & Lange, supra note 1, at 17.
\item \textsuperscript{142} See id. at 18.
\item \textsuperscript{143} See generally \textit{FED. R. CIV. P. 26} (outlining discovery requirements and possible penalties for noncompliance); see also \textit{FED. R. CIV. P. 34(a)} (requiring respondents to produce documents and data that are in “the possession, custody or control of the party upon whom the [document] request is served”).
\item \textsuperscript{144} 995 F.2d 1376 (7th Cir. 1993).
\item \textsuperscript{145} Id. at 1383-84.
\item \textsuperscript{146} 169 F.R.D. 598 (D.N.J. 1997).
\item \textsuperscript{147} Id. at 615-17.
\item \textsuperscript{148} See Hanlon-Leh, supra note 3, at 2 (“Many companies use ‘recycling’
tion shall be destroyed according to schedule, but destruction of documents must cease immediately at the moment litigation is anticipated.\textsuperscript{149} This includes halting automated destruction software which may be programmed to destroy records on a scheduled basis.\textsuperscript{150} Courts have sanctioned companies for destroying communications related to litigation even when litigation had not yet commenced but the company had informal notice.\textsuperscript{151} In \textit{Linnen v. A.H. Robins Co.}, a discovery mêlée ended "when (despite numerous assurances from defendant's counsel that 'no mass storage devices or other backup tapes containing electronic messages' existed) the defendant was forced to reveal that many documents had in fact been destroyed in the ordinary course of backup tape recycling."\textsuperscript{152}

A company must be familiar with the technologies involved, and officers must have efficient communications with their technical department "regarding the creation, modification, storage and retrieval of electronic data in connection with or in anticipation of a lawsuit."\textsuperscript{153} Clearly, companies have the right to destroy both electronic documents and files, but this destruction should not occur unless it is codified in a formal electronic document retention policy.\textsuperscript{154} The policy must be reasonable and adopted in good faith, as "a [company] cannot blindly destroy documents and expect to be shielded by a seemingly innocuous document retention policy."\textsuperscript{155}

Courts have also emphasized the need to manage electronic documents efficiently and effectively, due to the great

\textsuperscript{149} See Brown, supra note 109, at 663.
\textsuperscript{150} Nimsger & Lange, supra note 1, at 18 (citing Lauren Corp. v. Century Geophysical Corp., 952 P.2d 200 (Colo. Ct. App. 1998)).
\textsuperscript{151} See Brown, supra note 109, at 663 (citing Carlucci v. Piper Aircraft Corp., 102 F.R.D. 472, 485-86 (S.D. Fla. 1984)).
\textsuperscript{152} See Nimsger & Lange, supra note 1, at 17 (quoting Linnen v. A.H. Robins Co., No. 97-2307, 1999 WL 462015 (Mass. Super. June 16, 1999)) (Plaintiffs in a wrongful death action were granted a motion to compel the production of e-mail messages from the defendant even though the defendant had already produced a vast number of other electronic documents.).
\textsuperscript{153} Brown, supra note 109, at 661.
\textsuperscript{154} See id. at 662-63.
\textsuperscript{155} See id. at 663 (quoting Lewy v. Remington Arms Co., 863 F.2d 1104, 1112 (8th Cir. 1988)).
difference from paper documents. Although the primary issue in litigation was not electronic discovery, the court in *Armstrong v. Executive Office of the President*\(^{156}\) confirmed the difference between electronic records and print-outs of those records.\(^{157}\) The Executive Office of the President and government agencies claimed printing-out copies of e-mails satisfied their obligations to preserve presidential records under the Federal Record Act.\(^{158}\) They argued that the electronic versions of the printed-out e-mails were merely extra copies and therefore, were not official federal records.\(^{159}\) The court rejected this argument, confirming that the electronic versions of e-mails contain much more information than their paper counterparts. Specifically, the court pointed out that the "paper copies" do not include "non-screen" information such as acknowledgements of receipts or distribution lists.\(^{160}\) "[T]he mere existence of the paper printouts does not affect the record status of the electronic materials unless the paper versions include all significant material contained in the electronic records. Otherwise, the two documents cannot accurately be termed 'copies'—identical twins—but are, at most, 'kissing cousins.'\(^{161}\)

Without a doubt, hardcopies do not contain the same relevant information as their electronic counterparts. However, the challenge of identifying all the media where discoverable data may be found creates hardship with respect to tracking electronic documents and preserving them in their native form.\(^{162}\) With the wireless communications and portable devices of today, data can be stored in employees' homes or carried with them every day on a cellular telephone.\(^{163}\) "Increasingly, courts have required production of information that was stored on the home computers of employees"\(^{164}\) and have settled privacy complaints by using experts to search

---

156. 1 F.3d 1274 (D.C. Cir. 1993).
157. See generally id.
158. Id. at 1277. For more information on the Federal Records Act, see http://www.ed.gov/policy/gen/leg/fra.html?exp=0.
159. *Armstrong*, 1 F.3d at 1277.
160. Id. at 1280.
161. Id. at 1283.
163. Id.
164. Id.
electronic machines.\textsuperscript{165}

However, courts have emphasized that an employee who uses a computer for personal communication and also saves business documents on such computer assumes some risk that the computer could be accessed for discovery purposes and a privacy complaint will not have merit.\textsuperscript{166} In \textit{Simon Property Group L.P. v. mySimon, Inc.}, the court granted the plaintiff permission to recover deleted computer files from the defendant's employees, whether those computers were located at home or at work.\textsuperscript{167} Moreover, discovery is not limited to an employee's computer at home. Employees carry a wide variety of portable devices and "[t]hese... devices increasingly hold valuable contact information as well as email, other wireless messages, and call logs."\textsuperscript{168} If an employee stores business information on a PDA or cell phone that he or she personally owns, courts have ruled that such person is obligated to turn over the device for inspection.\textsuperscript{169} The reasoning behind this obligation is that Federal Rule of Civil Procedure 34 applies to items in the possession of corporate officers.\textsuperscript{170} Corporate officers who have control over their employees are in turn responsible for producing information stored on their employees' electronic devices.\textsuperscript{171} However, courts have held that producing such information is only required if the information was used by employees in the regular course of business.\textsuperscript{172}

\begin{footnotesize}
\textsuperscript{165} Id.
\textsuperscript{166} Id.
\textsuperscript{167} Simon Property Group v. mySimon, Inc., 194 F.R.D. 639, 641 (S.D. Ind. 2000) (granting the plaintiff's motion to compel with respect to electronic documents in order to prove defendant's intent in adopting trade identifiers and trademark infringement).
\textsuperscript{168} See Hanlon-Leh, \textit{ supra} note 3, at 3.
\textsuperscript{171} See \textit{id}.
\end{footnotesize}
V. PROPOSAL

Corporate management needs to evaluate the quality of information being retained as corporate records and organize information in an electronic medium to protect against the inadvertent sharing of otherwise privileged documents. However, publicly traded companies currently have wide discretion in creating and implementing policies concerning corporate governance of electronic records. Such wide discretion has led to mismanagement of electronic documents, which in turn has resulted in increased corporate liability and losses, and ultimately, has been detrimental to investors and the United States economy. To remedy this problem, the SEC must implement a federal electronic records retention policy that will provide publicly traded companies uniform legal standards regarding the management of electronic records. The policy should be based upon the regulation adopted by NARA.

Currently, NARA’s GRS 20 is one of the most evolved and complete set of guidelines in the area of electronic documents. However, because different types of businesses will need to maintain different records for their specific business purposes and GRS 20 is geared specifically towards federal government electronic documents and systems, the SEC cannot mimic GRS 20 in its entirety. The SEC can implement a policy similar to GRS 20 with the addition of outstanding policy suggestions found in many of the continuing legal education practicing guides and corporate treatises. This comment suggests the codification of the following three guidelines: (1) instructions pertaining to files and records re-

---

173. See supra Part II.F.
175. See supra Part II.A.
176. See supra Part V.
177. See supra Part II.F (discussing current federal policies and NARA’s GRS 20).
179. For example, Corporate Policy Statements is a continuing legal education guide published by the Law Journal Seminar Press and contains various corporate suggestions and rules for electronic records management.
lating to the creation, use, and maintenance of computer systems, applications, or electronic records;\(^{180}\) (2) instructions regarding the disposal schedule for electronic versions of records\(^{181}\) and information on back-up files;\(^{182}\) and (3) instructions on record classifications.\(^{183}\)

A. Files and Records Relating to the Creation, Use, and Maintenance of Computer Systems, Applications, or Electronic Records

Provision 1 of GRS 20 provides instructions regarding record-keeping methods and requirements relating to the creation, use, and maintenance of computer systems, applications, or electronic records.\(^{184}\) The SEC should implement similar guidelines, as such information will provide greater efficiency and reduce confusion in managing electronic records. Such instructions should specify that electronic records must preserve transmission data pertaining to the identity of the sender, addressees, and the date the message was sent.\(^{185}\) Instructions on how to retain names on directories or distribution lists should also be provided.\(^{186}\)

Companies should provide a list of all electronic devices owned by the company and used by company employees. In addition, every company should provide a business policy on employee e-mail and Internet use, including a description of the company's monitoring activities to the extent necessary to further legitimate business objectives.\(^{187}\)

B. Disposal Schedule for Electronic Versions of Records and Back-up Information

GRS 20, Provision 3 mandates that when all hard-copy records are retained to meet record-keeping requirements and

---

181. See id. at Provision 3.
182. See id. at Provision 8.
183. See Dietel, supra note 28, § 3:99.
186. See id.
187. See Brown, supra note 109, at 666-67.
the electronic copies are no longer needed for operational purposes, such as for legal audit, then the electronic copies shall be deleted permanently. The SEC should also establish a similar procedure for companies to follow regarding recopying, reformatting, and other necessary maintenance to ensure retention and usability of electronic records throughout their authorized life cycle. The goal of all corporate electronic records retention programs is to retain records only as long as they benefit the company. Providing a fundamental framework based on Provision 3 will assist corporations in achieving this goal.

The disposal schedule shall include a description of the e-mail deletion process, accompanied by a confirmation that when messages are deleted, all copies including the one on the back-up tape or disk are destroyed. Because there may be some preventive and protective value in saving some messages, a standard process should be in place that halts automatic or periodic message destruction if relevant litigation is filed.

C. Classification Requirements

Additionally, the SEC may also consider adopting rules that require every company to classify types of business records and files specifically. This will permit easy retrieval of records in a prompt manner, facilitate distinction between record and non-record material, and allow records to be retained in a usable format until their authorized disposal. An electronic inventory and an outline of the company's electronic structure should be at the core of these classifications. Although the retention polices will vary according to the type of business, the bulk of the policies should include methods used for "classifying documents, determining retention periods, setting the retention schedule and procedures and selecting a records custodian."

189. See Dietel, supra note 28, § 3:99.
190. See id. § 1:26.
191. See id. § 3:88.
192. See id. § 3:99.
193. See Nimsger & Lange, supra note 1, at 17-18.
194. See Lange, supra note 2.
VI. CONCLUSION

Today, people no longer need to leave their computer terminals or other electronic devices to conduct many of their daily tasks and to communicate globally. However, with each keystroke, corporate employees create trails of electronic information and records. The shift from paper documents to electronic documents has increased corporate liability and loss due to mismanagement of such records and employee misuse of electronic communications. Publicly traded companies have been left the discretion to develop their own governance polices over electronic documents; however, the lack of an adequate, focused electronic records retention and destruction policy has added to the problem of electronic file mismanagement.

In turn, it is critical that the Securities Exchange Commission implement a federal electronic corporate retention program that would help public companies to balance the potential consequences of spoliation of electronic documents with the savings that may be realized by reducing unnecessary discovery. The proposal suggests that the SEC adopt a regulation similar to the electronic retention schedule of the National Archives and Records Administration, with additional rules stemming from individual corporate policies. Corporate liability and losses can be minimized with a uniform federal policy. The proposed electronic document policy allows flexibility so that each company may create a policy appropriate to its respective business needs and at the same time, sets general legal guidelines necessary for effective implementation.

Although the proposal would only apply to publicly traded companies, some commentators suggest a need for a uniform federal minimum standard of corporate law. This comment urges private organizations outside the governance of the Securities and Exchange Commission also adopt such

195. See id.
196. See supra Part II.
197. See supra Part II.
198. See Dietel, supra note 28, § 3:88.
199. See supra Part V.
policy. Corporations must pay close attention to the duty to preserve evidence and the potential consequences that are likely to follow if such duty is breached. A well-developed, uniform federal electronic record retention policy will help minimize these repercussions.

201. See supra Part IV.