Boston College Law Review

Volume 41
Issue 2 *Number 2*

Article 3

3-1-2000

Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?

Hon. Shira A. Scheindlin

Jeffrey Rabkin

ELECTRONIC DISCOVERY IN FEDERAL CIVIL LITIGATION: IS RULE 34 UP TO THE TASK?

HON. SHIRA A. SCHEINDLIN*
JEFFREY RABKIN **

Abstract: *In today's world an increasing proportion of the information subject to discovery under the Federal Rules of Civil Procedure is stored electronically, rather than on traditional media. Despite this development, there has been no widespread debate as to whether the federal discovery rules adequately address the difficult issues that frequently arise during discovery of electronically-stored information. Rather, practitioners and judges have assumed that the same rules applicable to the discovery of traditional forms of evidence are easily applied to electronic data. Our overarching concern is the continuing validity of that assumption. This Article focuses specifically on how discovery of electronic evidence proceeds under Rule 34. We conclude that Rule 34 has shortcomings in this context, and therefore propose two simple but potentially significant changes in the wording of the Rule itself. The Article ends by noting that the legal community must confront several additional complex issues arising from the need to adapt the Federal Rules of Civil Procedure to the new era of electronic information.*

INTRODUCTION

At the close of this millennium, at least this much is clear about the next: Computers will play an increasingly pervasive role in American society. Although the first computer capable of using stored programs was developed little over fifty years ago, its progeny are already ubiquitous in the corporate world, and the number of households that own personal computers continues to rise.[1] As a federal district

* United States District Judge, Southern District of New York.

** Law Clerk, Judge Shira A. Scheindlin (1996–1997); Associate, Gibson, Dunn & Crutcher (1997–1999); Deputy City Attorney, Office of the City Attorney of San Francisco (2000–present).

[1] *See* Diamond v. Diehr, 450 U.S. 175, 194 n.1 (1981) (Stevens, J., dissenting) (describing first general purpose computer). One survey by a leading market research firm estimates that more than half of all American homes now have computers, as compared with 40% two years ago. *See* Mike Tonsing, *Electronic Mail Is Ubiquitous And Its Consequences Are Enormous*, FED. LAW., May 1999, at 56.

court judge wrote over ten years ago, "From the largest corporations to the smallest families, people are using computers to cut costs, improve production, enhance communication, store countless data and improve capabilities in every aspect of human and technological development."[2] Within the last five years, the combination of e-mail and widespread access to the Internet has resulted in the proliferation of electronic communication on an unanticipated scale.[3]

The mushrooming of computers in contemporary life has revolutionized the way we store information and communicate. Increasingly, electronic storage devices have replaced paper document depositories.[4] E-mail and the Internet have begun to replace the telephone as the way people conduct daily personal and business communications.[5] Also, computers are involved in an increasing number of commercial transactions. According to one report, consumer purchases made over the Internet will rise from $289 million in 1996 to $26 billion in 2001.[6] These technological developments have, in turn, had an important effect on civil litigation.[7]

---

[2] Bills v. Kennecott Corp., 108 F.R.D. 459, 461 (D. Utah 1985) (Greene, J.).

[3] One writer noted that there were an estimated 50 million users of the Internet in 1996 and that the number of users is projected to rise to 200 million by the end of 1999. *See* Jack E. Brown, *Obscenity, Anonymity and Database Protection: Emerging Internet Issues,* COMPUTER LAW., Oct. 1997, at 1. Others predict the number of Internet users will rise to 320 million by 2002. *See* DANIEL H. RIMER, HAMBRECHT & QUIST, CRITICAL PATH: CAPITALIZING ON THE NEW E-MAIL PARADIGM 3 (1999). Mr. Rimer also states that the number of e-mail mailboxes currently outnumbers users by a ratio of more than two to one and will continue to outnumber Internet users in the future. *See id.; see also* Donald J. Karl, *State Regulation of Anonymous Internet Use After* ACLU of Georgia v. Miller, 30 ARIZ. ST. L.J. 513, 513–14 (1998) (describing the growth of Internet use).

[4] In May 1997, one commentator estimated that 30% of the information that goes into business computers never appears in paper form. *See* Susan J. Silvernail, *Electronic Evidence: Discovery in the Computer Age,* ALA. LAW., May 1997, at 177; *see also* Paul Frisman, *E-mail: Dial 'E' For 'Evidence,'* N.J. L. J., Dec. 25, 1995, at 12.

[5] Ms. Silvernail has estimated that 40 million e-mail users will send 60 billion messages by 2000. *See* Silvernail, *supra* note 4, at 181. Time magazine estimated that 2.6 trillion e-mailed messages passed through U.S.-based computer networks in 1997 and that the number would increase to 6.6 trillion by 2000. *See* S.C. Gwynne & John F. Dickerson, *Lost In The E-mail,* TIME, Apr. 21, 1997, at 88.

[6] *See* John Rothchild, *Protecting The Digital Consumer: The Limits Of Cyberspace Utopianism,* 74 IND. L.J. 893, 895 (citing BILL BURNHAM, THE ELECTRONIC COMMERCE REPORT 238 (1997) and DEPARTMENT OF COMMERCE, THE EMERGING DIGITAL ECONOMY 38 (1998)). The New York Times reports Internet consumer sales are predicted to jump from $3.9 billion in 1998 to $108 billion in 2003. *See* Leslie Kaufman, *Amazon.com Plans A Transformation To Internet Bazaar,* N. Y. TIMES, Sept. 30, 1999, at A1.

[7] The proliferation of computer technology has also raised difficult issues in the context of criminal law. *See, e.g.,* United States v. Reyes, 922 F. Supp. 818, 832 (S.D.N.Y. 1996) (defendant moved to suppress telephone numbers obtained by government agents from the electronic data storage unit on his paging device); United States v. Paredes, 950 F.

For example, while lawyers may be traditionally slow to adopt technology for their own use, some recognized over a decade ago that discovery should include demands for the production of electronic evidence.[8] And, as society moves decisively in the direction of electronic communication and data storage, lawyers suspect they will find the "smoking guns" in an electronic format rather than in a paper form. Recent experience demonstrates the accuracy of this assumption. For example, Kenneth Starr's team found the infamous "talking points" document that forced Monica Lewinsky to accept an immunity deal in a computer file Lewinsky thought she had deleted from her computer.[9] One need not look far to find e-mail messages that have played crucial roles in the outcome of recent litigation. For example, one scholar reports the settlement of a sexual harassment case after the plaintiff discovered an e-mail from the company president to the head of personnel stating (with regard to the plaintiff): "Get rid of that tight-assed bitch."[10] Another example of e-mail from top-level executives that played an important role in litigation is found in the recent Microsoft anti-trust trial.[11] Exhibits in this case included bickering e-mail correspondence between Bill Gates and Andy Grove, Chief Executive Officers of Microsoft and Intel, respectively.[12]

Supp. 584, 586, 590 (S.D.N.Y. 1996) (dismissing murder-for-hire indictment where sole basis for jurisdiction was intrastate use of tristate paging system); People v. Jovanovic, 700 N.Y.S.2d 156, 159 (App. Div. 1999) (reversing conviction for kidnapping, sexual abuse and assault and ordering a new trial where trial court improperly excluded e-mailed messages from complainant to defendant indicating interest in sadomasochism).

[8] "Computers have become so commonplace that most court battles now involve discovery of some type of computer-stored information." *Bills*, 108 F.R.D. at 462.

[9] *See* J. Gregory Whitehair & Kimberly Koontz, *Discoverability Of Electronic Data*, COLO. LAW., Oct. 1998, at 45; *see also infra* Part I.C.1 (discussing recoverable deleted files).

[10] *See* Heidi L. McNeil & Robert M. Kort, *Discovery of E-mail*, OR. ST. B. BULL., Dec. 1995, at 21.

[11] *See id.*

[12] *See, e.g.*, James V. Grimaldi, *Microsoft Trial–Gates' Spat With Intel Is Revealed By E-mail*, SEATTLE TIMES, June 23, 1999, at E1. Other cases also have involved incriminating e-mail. *See, e.g.*, Vizcaino v. Microsoft Corp., 120 F.3d 1006, 1019 (9th Cir. 1997) (O'Scannlain, J., concurring in part) (noting, in an ERISA decision, that freelancers are treated differently from employees because, among other things, freelancers had different e-mail addresses); Meloff v. New York Life Ins. Co., 51 F.3d 372, 373, 376 (2d Cir. 1995) (denying summary judgment in libel suit based in part on e-mail evidence); Owens v. Morgan Stanley & Co., No. 96 Civ. 9747, 1997 WL 793004 (S.D.N.Y. Dec. 24, 1997) (involving suit by two African-American employees against a large investment banking firm that allegedly circulated racist e-mail message among white employees); Angleton v. Beech Aircraft Corp., No. 96-1027-JTM, 1997 WL 446262, at *2 (D. Kan. July 30, 1997) (involving e-mail sent by plaintiff to supervisor).

The efforts of federal litigants to discover their opponents' e-mail and other forms of electronic evidence raise a fundamental threshold issue: To what extent—if at all—do the Federal Rules of Civil Procedure[13] permit such discovery? A broad majority of practitioners, judges and academics believe "it is black letter law that computerized data is discoverable if relevant"[14] and assume that the Rules permit the discovery of e-mail and other electronically-stored information. Yet the Rules provide no guidance regarding the discovery of e-mail and make almost no reference to electronic evidence. As one practitioner has observed:

> The rules of civil procedure were written at a time when information was stored primarily on paper, in the form of documents; and the discovery rules are thus designed to deal with information stored on paper .... The current rules do not deal adequately with information stored in electronic form .... Astoundingly, [Rule 26(b)(1)] does not even mention information stored in electronic form. Similarly, Rule 30(b)(5) provides a means to compel a deponent to bring with him or her "documents or other tangible things," but makes no provision for data stored in electronic form. Rule 34 makes an extremely awkward attempt to reach electronic information in its definition of documents; but the language is so awkward and convoluted as to be almost completely opaque.[15]

Despite observations of this kind, there is no basis to conclude that the current state of technology has so outpaced the federal discovery rules as to render them unworkable or obsolete. But as e-mail, program files, Web sites, cookies, caches[16] and their ilk replace paper documents as the primary means of data collection, storage and

---

[13] We refer to the Federal Rules of Civil Procedure as the "Rules."

[14] Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also In re* Brand Name Prescription Drugs Antitrust Litig., Nos. 94 C 897 MDL 997, 1995 WL 360526, at *1 (N.D. Ill. June 15, 1995); *Bills*, 108 F.R.D. at 461. Commentators frequently quote *Hasbro* with approval. *See, e.g.*, Joseph P. Zammit & Lynette A. Herscha, *Litigation Issues In A Cyber World*, *in* PRACTISING LAW INSTITUTE, 18TH ANNUAL INSTITUTION ON COMPUTER LAW 122 (1998). These cases specifically dealt with program files or e-mail, and not the newer forms of electronic evidence such as cookies, temporary files, residual data or Web caches.

[15] *Hearings Before the Advisory Committe on Rules of Civil Procedure*, (Baltimore, MD) (Dec. 7, 1998) (testimony of Allen D. Black).

[16] *See infra* Part I.C.2. (describing these common types of electronic evidence).

transmission, the need for a comprehensive overhaul of the federal discovery rules to adapt them to our digitalized society must be debated seriously. Of particular concern is Rule 34, which provides for the discovery of documentary evidence.[17] After all, how well can we expect a discovery rule primarily designed to deal with paper documents to function in an increasingly paperless world?

This Article analyzes the adequacy of Rule 34 with respect to the discovery of electronically-stored information.[18] It also aspires to highlight the intrinsic differences between paper-based and electronically-stored information, and to show how these differences raise new discovery issues not addressed by Rule 34. Part I provides an explanation in lay terms of how computers process and store information electronically, as well as an overview of the types of electronically-stored information that, while subject to discovery, are often invisible (and thus unknown) to lawyers and computer users alike. Part II describes briefly the current framework of document discovery under Rule 34. Part III explains how electronic document discovery under Rule 34 poses challenges that are not analogous to "paper" discovery disputes and evaluates whether the current version of Rule 34 provides adequate guidance to resolve these issues. Part IV proposes two simple but potentially far-reaching amendments to Rule 34 in an effort to adapt the Rule to electronic discovery. Finally, Part V flags key issues regarding electronic discovery that the legal community should address in the near future.[19]

I. Electronic Discovery Terms Defined and Explained

Let us begin with an uncontroversial observation: Electronic devices have begun to replace paper as the primary means of storing

---

[17] *See infra* Part II.B. (describing Rule 34 in greater detail).

[18] By focusing on Rule 34, this Article does not mean to imply that the other Rules are of no concern. To the contrary, the same definitional and logistical problems discussed below regarding Rule 34 present themselves under Rule 30(b)(5), which governs document productions at party depositions, and Rule 45, which permits parties to require non-parties to produce "designated books, documents or tangible things in the possession, custody or control" of those non-parties. *See* FED. R. CIV. P. 30(b)(5), 45(a)(1).

[19] For more future-looking and radical proposals for altering the Rules to incorporate modern technology for purposes of conducting more efficient trials, see generally Paul D. Carrington, *Virtual Civil Litigation: A Visit To John Bunyan's Celestial City*, 98 COLUM. L. REV. 1516, 1524–34 (1998) (proposing, among other things, virtual trials and virtual appellate review). Although Professor Carrington's work does not touch in any detail on discovery of electronic data, it does provide a vision of how a more technology-oriented civil justice system might operate.

information, just as the Internet has begun to replace the postal system as the primary means of transmitting information. Where once people typed memoranda on paper and sent them by mail, now they generate word processor files on their computers and send them by e-mail. In a world where paper increasingly takes a back seat to electronic media, prosaic terms such as "document," "possession" and even "evidence" take on an ambiguity in the context of discovery. What types of computerized information are "documents" as the term is used by Rule 34? Does a litigant "possess" computer files after she discards them? This Article attempts to address these questions in Parts IV and V. To begin, however, we must define the universe of evidence with which we are concerned, and the natural starting place is the recently-coined term "electronic evidence."

A. *Basic Definitions*

Electronic evidence has been defined as "information stored in electronic form that . . . is relevant to the issues in a particular litigation."[20] In the context of federal civil litigation, this definition is under-inclusive for two reasons. First, in some circumstances, discovery is permissible before litigation has commenced or even after an action has concluded in a judgment.[21] Second, the Rules currently allow discovery of information both if it is relevant to the subject matter of a lawsuit *or* if it is reasonably calculated to lead to the discovery of admissible evidence.[22] It is therefore more appropriate to define elec-

---

[20] MICHAEL R. OVERLY, OVERLY ON ELECTRONIC EVIDENCE IN CALIFORNIA § 1.01, at 1–2 (1999).

[21] Rule 27(a)(3) offers a method of obtaining inspection of documents and things for use in a future action. *See* FED. R. CIV. P. R. 27(a)(3). The rule was intended "to apply to situations where, for one reason or another, testimony might be lost to a prospective litigant unless take[n] immediately, without waiting until after a suit or other legal proceeding is commenced." *In re* Ferkauf, 3 F.R.D. 89, 91 (S.D.N.Y. 1943). Similarly, Rule 27(b) provides a procedure for perpetuating testimony while a case is on appeal, for use in the event of further proceedings in the district court. *See* FED. R. CIV. P. 27(b); *see generally* 8 CHARLES ALAN WRIGHT ET AL., FEDERAL PRACTICE AND PROCEDURE: CIVIL 2D §§ 2071–76 (1994) (discussing Rule 27 in detail).

[22] *See* FED. R. CIV. P. 26(b)(1). The Advisory Committee on Civil Rules has published an amendment that will alter the wording of Rule 26(b)(1) from "relevant to the subject matter of a lawsuit" to "any matter, not privileged, that is relevant to the claim or defense of any party" but will allow discovery of matters falling within the former category for good cause shown. If approved by the Supreme Court and not rejected by Congress, these proposed changes will take effect at the end of 2000.

tronic evidence as any electronically-stored information subject to pretrial discovery.[23]

In addition, throughout this Article we use the term "electronic document" to refer to a subset of electronic evidence: information intentionally created by a computer user[24] and stored in electronic form. The term electronic document comes about naturally because the word "document" has been defined broadly in other legal contexts as "any physical embodiment of information or ideas."[25] By using the modifier "electronic," the term incorporates the idea that the "physical embodiment of information or ideas" must be kept in electronic form—or, as will be explained below, in the form of binary numbers stored on electric transistors.

B. *How Computers Transform and Store Information in Binary Form*

In order to evaluate the potential difficulties arising from discovery of electronic evidence under Rule 34, one must first have a basic understanding of how computers transform information into an electronic form and how that information is then stored. To this end, this Part briefly explains how all computers convert the myriad forms of information they process into binary numerals. This Part also describes how computers use and record those binary numerals on storage devices and the most common sources of electronic evidence.

We begin with the observation that almost all electronic information is stored in the form of binary numerals.[26] Text, sound and pictures (or "graphics") are all reduced to a series of zeros and ones inside the computer. This is true of all computers, regardless of their size, purpose or design. Therefore, in a fundamental sense, computers are nothing more than a collection of organized switches operat-

---

[23] "Electronically-stored" includes all information stored digitally, optically or in analogue form.

[24] As explained below in Part I.C.1., a computer creates a broad range of electronically-stored information without a user's knowledge. We intend the term "electronic document" to exclude such information.

[25] *See* BLACK'S LAW DICTIONARY 481 (6th ed. 1990) (citing Strico v. Cotto, 324 N.Y.S.2d 483, 486 (1971)). This definition would include pictures or tapes. We note, however, that at least one lay dictionary defines the term "document" to mean simply "a writing conveying meaning." *See* MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 342 (10th ed. 1993).

[26] Some data is stored in analogue form, using continuous variable attributes such as voltages or pressure, instead of binary numbers. This type of storage is not discussed in detail in this Article.

ing at incredibly high speeds.[27] These switches have only two settings, on and off. All computer operations are the result of the manipulation of huge numbers of these switches. Microscopic electronic devices called "transistors" are used to perform the computer's switching functions. Today, approximately sixteen-million transistors can be put onto a chip the size of a thumbnail, and microchip designers are constantly finding new ways of adding more transistors to memory chips. Moreover, computers may soon use transistors built on a molecular scale, radically increasing the number of switches that can fit on to a single chip.[28]

Because they only have two settings, transistors can only hold two types of information. Computer designers refer to this as binary information and assign the values "0" and "1" to the transistor's two possible states. Each "0" or "1" is referred to as a "bit" of information. By combining transistors, computers can process and store any decimal number by using binary notation. Additionally, the letters of the alphabet, as well as commonly-used symbols (such as "&," "$," "§" or "¶") can be processed and stored by assigning a number to each letter and symbol.[29] For example:

Letter	Decimal (Base 10) Number	Binary (Base 2) Number
A	0	0
B	1	1
C	2	10
D	3	11
E	4	100
F	5	101

The chart above also illustrates a concept that becomes important in the context of electronic discovery. A series of zeros and ones stored on a computer's hard drive is meaningless without a key to translate

[27] *See* Ron White, How Computers Work 36 (1997) ("[A] computer is just a collection of On/Off switches.").

[28] *See DNA Computing*, PC Mag., Nov. 2, 1999, at 11; Madeleine Acey, *Chemist Drives Gas Powered Computers*, CMP TechWeb, Oct. 14, 1999, <http.//www.techweb.com/wire/story/TWB19991014S0001>.

[29] The chart below is simply an example of assigning numbers to letters. In fact, most computers use a standardized code called the American Standard Code for Information Interchange ("ASCII") to assign numbers to represent the alphabet, digits 0 through 9, punctuation marks and other commonly-used typographical symbols.

those bits into information. The chart above, for example, indicates that "101" signifies the letter F. Without the chart, however, the information cannot be deciphered.

Bits are the fundamental building blocks of electronically-stored information. In computer terminology, eight bits comprise one "byte" of storage capacity or "memory."[30] Computer storage capacity is usually measured in thousands (or millions) of bytes of information.[31] Although it might appear cumbersome to translate letters and decimals into zeros and ones, computers do it at lightning speed and can store an enormous volume of bits. For example, the floppy disks commonly used a decade ago were capable of storing enough zeros and ones to record up to 180 pages of text. Today's CD-ROM disks can store approximately 325,000 pages of text. The average PC hard disk can store up to two million pages of text.[32] The sheer volume of discoverable electronic evidence—and the trend towards ever greater computer storage capacity—poses logistical challenges to lawyers, litigants and the courts.[33]

C. *Types of Electronic Evidence Subject to Discovery*

Most computer users are aware that word processors, spreadsheets, e-mail programs and other popularly-used "accessories" generate information that is stored electronically in the form of "files." It is also commonly understood that pictures and sound can be stored and transmitted electronically. Computers, however, generate far more information than most users realize. For example, most word processor programs automatically store prior drafts of written documents, as well as the time and dates of past edits and the name of the person who made those edits. Another interesting and unexpected example is the category of deleted, but recoverable, program files. Because these types of "hidden" or unknown computer data comprise a large proportion of the total universe of discoverable electronic evidence,

---

[30] Bytes (or groups of eight bits) are themselves made up of two units of four bits called nibbles. By using binary numerals, each nibble can store up to 16 different arrangements of bits—and thus can represent decimal numbers 1 through 16. A byte, therefore, can represent up to 256 different numbers. *See* RICHARD RABKIN, BITING DEEPER INTO THE APPLE'S CORE 44, 46 (1985).

[31] Metric prefixes are often used in this context. Thus, "64k" may be used to refer to 64 "kilobytes," or 64,000 bits of information.

[32] *See* OVERLY, *supra* note 20, § 1.01, at 1–3.

[33] *See infra* Part III.C.6.

they are addressed. Part III notes that this category of data creates special problems in the context of discovery.

1. Types of Stored Data

Computer storage devices come in a variety of shapes and sizes. Most desktop personal computers ("PCs") store data on removable diskettes, internal or external hard drives and/or CD-ROM devices. Laptops and handheld computers[34] also store information in memory cards powered by miniature batteries.[35] Networked computers, such as those used by most large businesses, both store data on large hard drives and copy the information stored on their system to a backup system (typically using magnetic tapes to store the data) on a regular basis to guard against accidental loss of data. Individual users and small businesses can back up their computer storage devices by sending their files over the Internet to a third party's computer. This means, for example, that a back-up copy of information stored on a computer in San Francisco may exist in Internet storage devices located in Tokyo and New York. In fact, several companies offer computer users free storage space on their Web sites.[36]

The information generated and stored by programs such as word processors and spread sheets (or any other software running on a computer) are typically stored in data files, also known as "program files" because they are generated by specific computer programs. For example, a computer user who generates a document on a word processor and then saves it to disk (either the hard drive on the computer or a removable diskette) has created a data file that contains the document created by the user. Therefore, data files can be stored locally on the computer or remotely, either on a portable diskette or a storage device at another site.

Many people incorrectly believe that once they have deleted a data file it cannot be recovered. Many programs, however, have an

---

[34] Examples of a personal electronic organizer are the popular Palm Pilot and Nino and their recent rival, the Visor; all are typically used to store information such as telephone numbers, calendar and scheduling information and travel expenses. The newer versions of the palm-sized computers are capable of running word processing programs, spreadsheets and Web browsers.

[35] Microchips, or "integrated circuits," and the information they store increasingly are integrated into everyday technology. For example, automobile air bag systems designed to inflate only in specific circumstances may record not only the time of an accident, but also the speed at which the car was traveling and the angle of impact.

[36] For example, the following Web sites allow users to store personal information: www.i-drive.com; www.idrop.com; www.docspace.com; and www.filemonkey.com.

automatic backup feature that creates and periodically saves copies of a file as the user works on it. Such files, referred to by some as "replicant data," "temporary files" or "file clones," are intended to help users recover data losses caused by computer malfunction.[37] For example, if a user accidentally turns off her computer without saving a word processing file, she may be able to recover that file because the computer has saved a recent version of it in a "temporary file." Similarly, networks copy information to removable or offsite storage devices on a regular basis. These backup devices may contain copies of deleted program files.

Recovery is possible even in the case of a deleted program file for which no clone or backup version was created. To explain why this is so requires a short description of the way computer storage devices function. 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.

"Deleting" a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a "not used" status—thus permitting the computer to write over the "deleted" data. Until the computer writes over the "deleted" data, however, it may be recovered by searching the disk itself rather than the disk's directory.[38] Accordingly, many files are recoverable long after they have been deleted—even if neither the computer user nor the computer itself is aware of their existence. Such data is referred to as "residual data."[39]

There is another form of hidden electronic evidence that must be mentioned. As noted earlier, a program file may automatically create and store more information than that entered by the computer user. For example, word processor programs typically store information about when data files are created, who edits them and when, and

---

[37] *See* Joan E. Feldman & Rodger I. Kohn, *The Essentials Of Computer Discovery*, *in* PRACTISING LAW INSTITUTE, THIRD ANNUAL INTERNET LAW INSTITUTE 51, 54 (1999).

[38] An analogy would be removing someone's house address from the phone book. The house still may be located if you know what it looks like, even if you do not know exactly where to look.

[39] *See* Feldman & Kohn, *supra* note 37, at 55.

who accesses them. We refer to such automatically-created information as "embedded" data because it is not normally visible when the document is printed.

Additionally, many networked computer systems require users to "log on" to the system by typing in a password. The computer then typically records which users signed onto the system and when and where they did so, all of which may be relevant in a lawsuit and therefore discoverable. Along the same lines, networked computers are sometimes set up so as to grant certain employees greater access to certain parts of the system. For example, a system might permit the author of a document to limit the number and/or identity of individuals who can edit and view that document to specified individuals. Critical research information might be available only to a small handful of system users. As with the log information, the access control list may be relevant and discoverable information.

Furthermore, some employers set up their computer systems to monitor their employees automatically. Such systems will track and store information such as when users access specific programs, how long they use them and whether users have edited specific documents. Also, employers can keep track of which Web sites employees access and what files they download from those Web sites.

2. Types Of Internet-Related Computer Information

E-mail is fast becoming the primary means of communication between businesses and individuals. Estimates of e-mail volume range as high as one million messages every hour.[40] With the rise of its use in the office, and because of the common tendency to say things in e-mail messages that otherwise would not be reduced to written form,[41]

---

[40] *See* OVERLY, *supra* note 20, § 2.12, at 2–18; *see also supra* note 5.

[41] Several commentators have observed that many people express thoughts and make statements using e-mail that they would not otherwise put down in writing. *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 410, 412 (C.A.A.F. 1996) (involving Air Force Colonel accused of transmitting child pornography through graphic files attached to e-mailed messages); Owens v. Morgan Stanley & Co., No. 96 Civ. 9747, 1997 WL 793004 (S.D.N.Y. 1997) (involving suit by two African-American employees against large investment banking firm that allegedly circulated racist e-mail messages among white employees); Miller v. U.S.F.& G., No. 93-1968, 1994 WL 395718, at *2, 5 (D. Md. 1994) (involving suit against corporation by Human Resources Manager, claiming discrimination in discharge for participation with male co-workers in using numeric code system in e-mailed messages to refer to profanity); United States v. Charbonneau, 979 F. Supp. 1177, 1179 (S.D. Ohio 1977) (involving participant in America Online chat-room accused of sending e-mail messages containing graphic files of child pornography). Mr. Overly attributes this phenomenon to the ease and speed with which e-mail can be generated and sent, lending to "heat of the moment"

e-mail has proven to be the source of the "smoking gun" in high profile cases and, as might be expected, the focus for much discovery litigation.[42] E-mail programs typically store a copy of every message that is received and sent by the user. Thus, multiple copies of an e-mail message are often stored on the computer of both the sender and receiver—even if they are deleted by both. E-mail messages also embed within them information about the time they were generated, received and read, as well as the identity of the author and recipient.

It is fairly easy for knowledgeable computer users to create e-mail messages that falsify this information, an activity that is sometimes referred to as "spoofing." As one commentator has explained, senders of bulk commercial e-mail use spoofing to disguise their identity. The sender need only use a false identity and invalid credit card number to activate an Internet account that enables her to send e-mail under a false name; the account is opened before the information is verified, allowing the sender to send numerous e-mail messages before abandoning the account.[43] "Spoofing" is in part enabled by retail Web sites that now allow their users to send e-mail anonymously ("anonymous remailers"). Although some law makers have attempted to limit the availability of anonymous remailers,[44] they continue to exist and to attract users who wish to take advantage of this feature of the Internet.[45]

Another innovation experiencing rapid acceptance in both the home and office is the World Wide Web. The World Wide Web is a

---

messages, as well as the general (and incorrect) belief among e-mail users that once e-mailed messages are deleted they are gone forever. *See* OVERLY, *supra* note 20, § 2.12, at 2–18.

[42] *See* Karen Donovan, *E-Mails Helped Microsoft In Connecticut Victory*, NAT'L L. J., Aug. 2, 1999, at A1 (e-mailed messages showing plaintiff deliberately extended litigation against Microsoft to inflict discovery costs in the hope of achieving a high settlement played central role in jury's deliberations); *see also supra* notes 12–14 and accompanying text.

[43] *See* Rothchild, *supra* note 6, at 927. The author notes, "It is likewise trivially easy for the owner of a Web site to disguise her identity." *Id.* at 928.

[44] In *ACLU v. Miller*, a district court struck down, on First Amendment grounds, a Georgia law prohibiting all electronic communications that did not truthfully identify the sender. *See* 977 F. Supp. 1228, 1230, 1232 (N.D. Ga. 1997). In reaching its decision, the court relied upon Supreme Court precedent recognizing a right to distribute pamphlets anonymously. *See id.* at 1232 (citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995)).

[45] *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 167–69 (1996) (defending usefulness of anonymous remailers). *See generally Developments in the Law–The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1607–08 (1999) (describing anonymity of Internet and anonymous remailers).

collection of electronic documents that are organized and located at "Web sites" residing in computers throughout the world.[46] Each Web site can contain information stored in textual, graphical or audio format and can link to any other Web site. Therefore, users can quickly and easily move between various Web sites, viewing and collecting information without regard to which particular Web sites are actually storing the information sought. Web sites are viewed by means of computer programs called "Web browsers," which translate data received from a Web site into readable form on the user's or "browser's" computer.[47] Browsers typically store popular or frequently-visited Web sites on the user's hard drive in "cache files" so the next time those sites are visited the computer can access them directly from locally-stored memory.[48] This saves time and reduces traffic on the Internet. Computer users, however, are typically unaware of the cache files stored on their computers because they are stored by the browser without the users' express approval. History files are automatically created by the Internet browser. As their name indicates, these files record the various Web sites visited by the user, as well as the time they were visited.[49] Similarly, Web site operators typically keep records of the site's visitors, called Web site log files.[50]

"Cookies" are another type of file generated by Web sites and stored on the computers of the users that access those Web sites.[51] For example, a weather forecasting Web site might install a "cookie" onto a visitor's hard drive recording the visitor's zip code, so that the next time the visitor logs onto the Web site she can automatically receive local weather information. Cookies are a way of determining which Web sites the user has visited in the past. As Michael Overly notes, "The directory containing the various cookie files may be a source of very revealing information concerning the user's activities on the

---

[46] *See* Brookfield Communications, Inc. v. West Coast Entertainment Corp., 174 F.3d 1036, 1044 (9th Cir. 1999) (describing the Internet and the World Wide Web); ACLU v. Reno, 929 F. Supp. 824, 836–38 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (providing an overview of the World Wide Web).

[47] *See* Rothchild, *supra* note 6, at 900 (describing Web sites in greater detail).

[48] *See* OVERLY, *supra* note 20, § 2.12[H], at 2–14. On larger networked systems, Internet caches may be stored locally on the hard drive of a specific workstation or at the server level.

[49] *See id.* § 2.12[I], at 2–15.

[50] *See id.* § 2.12[G], at 2–14.

[51] *See id.* § 2.12[F], at 2–13 to 2–14.

Internet."[52] Furthermore, some cookies may automatically keep a list of each of the Web sites the user visits.

D. *The Predictable Rise of Discovery Disputes Regarding Electronic Evidence*

The explosion of electronic evidence has not been ignored by litigators or commentators. A host of articles (largely written by practicing attorneys), and at least one book, discuss the value of obtaining discovery of electronic evidence, and how to go about it.[53] In addition, at least two scholars have written on the issue of how the Federal Rules of Evidence apply to electronic evidence.[54] Given the central role of discovery in most civil litigation, as well as the increasingly common use of computers to generate, store and transmit information, it is safe to predict that federal courts will see a surge in the number of discovery disputes arising from electronic discovery. The next parts of this Article explain how discovery proceeds under Rule 34 and discuss why electronic discovery disputes will generate new issues that courts may not be able to address easily under that Rule.

---

[52] *Id.* § 2.12[F], at 2-14.

[53] *See, e.g.*, OVERLY, *supra* note 20; Feldman & Kohn, *supra* note 37; Ronald L. Plesser & Emilio W. Cividanes, *Discovery And Other Problems Related To Electronically Stored Data And Privacy*, *in* PRACTICING LAW INSTITUTE, COMPUTER SOFTWARE AND THE INTERNET 227 (1995); Zammit & Herscha, *supra* note 14, at 107; Matthew J. Bester, *A Wreck On The Info-Bahn: Electronic Mail And The Destruction Of Evidence*, 6 COMMLAW CONSPECTUS 75 (1998); Patrick R. Grady, *Discovery Of Computer Stored Documents And Computer Based Litigation Support Systems: Why Give Up More Than Necessary*, 14 J. MARSHALL J. COMPUTER & INFO. L. 523 (1996); Gregory S. Johnson, *A Practitioner's Overview Of Digital Discovery*, 33 GONZ. L. REV. 347 (1997–98); Susan E. Davis, *Elementary Discovery, My Dear Watson: Today's Evidence Comes In Bytes And Megabytes*, CAL. LAW., Mar. 1996, at 53; Debra S. Katz & Alan R. Kabat, *Electronic Discovery In Employment Discrimination Cases*, TRIAL, Dec. 1998, at 28; Joseph L. Kashi, *How To Conduct On-Premises Discovery Of Computer Records*, LAW PRAC. MGMT., Mar. 1998, at 255; Peter V. Lacouture, *Discovery And The Use Of Computer-Based Information In Litigation*, R.I. B. J., Dec. 1996, at 9; Charles A. Lovell & Roger W. Holmes, *The Dangers Of E-Mail: The Need For Electronic Data Retention Policies*, R.I. B. J., Dec. 1995, at 7; Heidi L. McNeil & Robert M. Kort, *Discovery Of E-Mail And Other Computerized Information*, ARIZ. ATT'Y, Apr. 1995, at 16; Heidi L. McNeil & Robert M. Kort, *Electronic Mail And Other Computer Information Shouldn't Be Overlooked*, OR. ST. B. BULL., Dec. 1995, at 21; Clifford Miller, *Electronic Evidence—Can You Prove The Transaction Took Place?*, COMPUTER LAW., May 1992, at 21; Silvernail, *supra* note 4; Whitehair & Koontz, *supra* note 9, at 45; Stephen Zovickian & Geoffrey Howard, *Electronic Discovery In Construction Litigation*, CONSTRUCTION LAW., July 1998, at 8.

[54] *See* James E. Carbine & Lynn McLain, *Proposed Model Rules Governing the Admissibility of Computer-Generated Evidence*, 15 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (1999); Anthony J. Dreyer, *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 (1996).

II. The Current Framework of Rule 34 Discovery

A. *An Overview of Federal Discovery Tools*

Rules 26 through 37 govern discovery procedures in federal civil actions. As a general matter, they are designed to enable litigants to obtain all the evidence necessary to evaluate and resolve their dispute as well as to prepare for trial.[55] The Supreme Court describes the underlying goals of these Rules in *Hickman v. Taylor:*

> The pre-trial deposition-discovery mechanism established by Rules 26 to 37 is one of the most significant innovations of the Federal Rules of Civil Procedure. Under the prior federal practice, the pre-trial functions of notice-giving issue-formulation and fact-revelation were performed primarily and inadequately by the pleadings. Inquiry into the issues and the facts before trial was narrowly confined and was often cumbersome in method. The new rules, however, restrict the pleadings to the task of general notice-giving and invest the deposition-discovery process with a vital role in the preparation for trial. The various instruments of discovery now serve (1) as a device, along with the pre-trial hearing under Rule 16, to narrow and clarify the basic issues between the parties, and (2) as a device for ascertaining the facts, or information as to the existence or whereabouts of facts, relative to those issues. Thus civil trials in the federal courts no longer need to be carried on in the dark. The way is now clear, consistent with recognized privileges, for the parties to obtain the fullest possible knowledge of the issues and facts before trial.[56]

Such an approach reflects a significant change from the traditional Anglo-American approach of severely limited pre-trial discovery. As one treatise explains, the formulation of Rules 26 to 37 reflects a shift to thinking of trials as a search for truth rather than a battle of wits.[57]

---

[55] *See, e.g.*, Herbert v. Lando, 441 U.S. 153, 177 (1979); *see also* Fed. R. Civ. P. 1 (the Rules should be "construed and administrated to secure the just, speedy, and inexpensive determination of every action.").

[56] 329 U.S. 495, 500–01 (1947) (*cited in* 8 Wright et al., *supra* note 21, § 2001, at 39).

[57] *See* 8 Wright et al., *supra* note 21, at 40 (describing liberalization of the discovery rules). Professors Wright, Miller and Marcus identify three distinct purposes of the current discovery rules: "(1) To narrow the issues, in order that at the trial it may be necessary to produce evidence only on a residue of matters that are found to be actually disputed and

The fundamental tools of discovery in federal courts are mandatory initial disclosure,[58] oral and written depositions,[59] interrogatories,[60] requests for production of documents and things,[61] requests for physical and mental examination of persons,[62] expert disclosure,[63] requests for admissions[64] and subpoenas to non-parties.[65]

Rule 26(b)(1) defines the scope of discoverable information:

> Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or the claim or defense of any other party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. The information sought need not be admissible at trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.[66]

Rule 26 also requires the initial disclosure of "data compilations" and "tangible things" relevant to disputed facts alleged with particularity in the pleadings.[67] While Rule 26 and the Advisory Committee Notes ("Notes") that follow it contain no language to indicate whether electronic evidence was intended to fall within these categories, the Committee comments regarding the definition of "documents" under Rule 34 arguably indicate that use of the term "data compilation" in Rule 26 was intended to include electronically-stored (or "computerized") data. It also could be argued, however, that the Advisory Com-

---

controverted. (2) To obtain evidence for use at the trial. (3) To secure information about the existence of evidence that may be used at the trial and to ascertain how and from whom it may be procured . . . ." *Id.* at 41.

[58] *See* FED. R. CIV. P. 26(a)(1). An amendment of this Rule is also slated to take effect in December 2000. *See* discussion *supra* note 22.

[59] *See* FED. R. CIV. P. 30, 31.

[60] *See* FED. R. CIV. P. 33.

[61] *See* FED. R. CIV. P. 34 (also allowing entry upon land for inspection and other purposes).

[62] *See* FED. R. CIV. P. 35.

[63] *See* FED. R. CIV. P. 26(a)(2).

[64] *See* FED. R. CIV. P. 36.

[65] *See* FED. R. CIV. P. 45.

[66] FED. R. CIV. P. 26(b)(1).

[67] *But see supra* note 22 (quoting language of revised Rule 26(b)(1), to take effect at the end of 2000).

mittee ("Committee") knew how to make express reference to computerized data when it wished to (such as in the case of its comments regarding Rule 34) and that the lack of any such reference in Rule 26 and its comments indicates that the Committee did not wish to incorporate computerized data within the scope of Rule 26.

B. *A Basic Description of Rule 34*

In addition to the limits of discovery set by Rule 26, Rule 34 describes both the scope of documentary discovery and the procedure by which litigants may obtain that discovery. Rule 34(a) allows any party to serve on any other party a request

> 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 writings, drawings, graphs, charts, photographs, phonorecords, *and other data compilations from which information can be obtained,* translated, if necessary, by the respondent through detection devices into reasonably usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served[.][68]

The Notes to the 1970 Amendment to Rule 34 include the following explanation:

> The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when that data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use [its] devices to translate the data into usable form. In many instances, this means that respondent will have to supply a print-out of computer data .... Similarly, if the discovering party needs to check the electronic source itself, the court may protect respondent

[68] FED. R. CIV. P. 34(a) (emphasis added).

> with respect to preservation of [its] records, confidentiality of nondiscoverable matters, and costs.[69]

This Note implies that a respondent satisfies its Rule 34 production obligations by providing a "print-out" of electronic evidence, thereby minimizing the importance of the manner in which electronic evidence is produced. For reasons discussed in Parts III and IV, the differences between producing electronic evidence in electronic format versus hard copy are more significant than the 1970 Note suggests.

Rule 34 (b) sets forth the required procedure for documentary discovery:

> The request shall set forth, either by individual item or by category, the items to be inspected and describe each with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. Without leave of court or written stipulation, a request may not be served before the time specified in Rule 26(d).
>
> The party upon whom the request is served shall serve a written response within 30 days after the service of the request. A shorter or longer time may be directed by the court or, in the absence of such an order, agreed to in writing by the parties, subject to Rule 29. The response shall state, with respect to each item or category, that inspection and related activities will be permitted as requested, unless the request is objected to, in which event the reasons for the objection shall be stated. If objection is made to part of an item or category, the part shall be specified and inspection permitted of the remaining parts. The party submitting the request may move for an order under Rule 37(a) with respect to any objection to or other failure to respond to the request or any part thereof, or any failure to permit inspection as requested.
>
> A party who produces documents for inspection shall produce them as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request.[70]

---

[69] FED. R. CIV. P. 34 advisory committee's note (1970).

[70] FED. R. CIV. P. 34(b).

Stated more simply, Rule 34(b) allows a party seeking to inspect the documents or things of another party to do so by serving a request that specifically identifies what is to be inspected, as well as where and when.[71] The respondent must serve a response within a specified period of time, indicating that the request will be granted or setting forth an objection to the request (for example, on the basis that the requested material is privileged). If the parties cannot resolve the respondent's objections, the requesting party must seek the presiding court's intervention under Rule 37(a).[72]

There are no special rules governing discovery of electronic information; rather, it proceeds under the same framework as discovery of any other information under Rule 34. The responding party confronts threshold issues as to whether the requested information is discoverable—within the scope of Rule 26(b)(1)—and if so, whether it is privileged. For non-privileged, discoverable information, secondary issues arise as to the way in which the information is produced to the requesting party, including when, where and how the production takes place, and who bears the costs associated with the discovery.

III. Is Rule 34 Capable of Governing Electronic Discovery?

As discussed above, the Rules provide only limited guidance with respect to electronic data and the extent to which it is discoverable. The legal community must squarely address the question of whether the current Rules are adequate to govern the discovery of electronic evidence or whether the Rules need to be revised to account for the differences between electronic and paper evidence.[73] In this Part, we focus specifically on the question of whether Rule 34 provides an adequate framework for the discovery of electronic evidence.

A. *New Issues Generated By Electronic Evidence*

Efforts to discover electronic documents have generated a host of new discovery issues with which courts are only beginning to grapple.

---

[71] *See* Fed. R. Civ. P. 34(b).

[72] *See* Fed. R. Civ. P. 37(a).

[73] The same question has been asked more broadly in related contexts. For example, Professor Lawrence Lessig questioned whether cyberspace may be regulated by analogy to the regulation of other space, or whether "the old analogies just don't cut it." *See* Lawrence Lessig, *The Path Of Cyberlaw*, 104 Yale L.J. 1743, 1743 n.1 (1995) (quoting Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. Pitt. L. Rev. 993, 994 (1994)).

As an initial matter, it is unclear whether the newest forms of electronic evidence described above fall within the rubric of discoverable "documents" under Rule 34—even when taking into consideration the Rule's express inclusion of "data compilations" within the definition of that term.[74] For example, is a cookie or cache file created by a Web site and automatically downloaded onto a user's computer, without her knowledge or consent, a "document" within the scope of Rule 34(a)? What about embedded data, such as that which is automatically created by most word processing programs to record the date specific documents are edited? While presumably these types of evidence are "data" in a generic sense, they are not "compilations" in the ordinary sense of something composed out of materials taken from other preexisting documents.[75] Rather, temporary, backup, cookie, cache and history files all represent examples of a *sui generis* family of computer-created information.

Beyond this type of basic definitional quandary, Rule 34 discovery of electronic evidence also presents logistical difficulties. Consider, for example, two quite basic questions relating to the production of electronic documents pursuant to Rule 34:

> 1) If a producing party[76] elects to produce electronic documents in hard copy, does this comply with Rule 34(b)'s requirement that the documents be produced "as they are kept in the usual course of business" or be organized and labeled to correspond to the categories of the request?; and
>
> 2) If a litigant requests the production of electronically-stored information in hard copy as well as electronic format, should it bear the cost of producing the duplicate hard copies?

These two questions may appear mundane, but we choose them to illustrate problems that often arise when dealing with discovery: given the growing presence of computers in the American workplace,[77] it is fair to assume that all Rule 34 document demands propounded to

---

[74] *See* FED. R. CIV. P. 34(a).

[75] *See* OXFORD ENGLISH DICTIONARY 605 (2d ed. 1989) (defining compilation as "heaping or piling together; accumulation").

[76] In accordance with common usage, we use the terms "producing party" and "respondent" interchangeably to refer to a litigant that produces documents pursuant to a Rule 34 document demand. Similarly, we use the term "requesting party" to refer to a litigant that propounds discovery requests or demands.

[77] *See* Feldman & Kohn, *supra* note 37, at 56 (reporting that 90% of organizations with over 1000 employees use e-mail).

corporate litigants will include a request for non-privileged electronic documents.

Consider the first question. In producing electronic documents, the respondent must choose between allowing the requesting party to copy the documents in their electronic form (or providing such a copy)[78] and allowing the requesting party to print a hard copy of the electronic documents (or providing such hard copies). The former method of production may be impracticable because it necessarily allows an adversary access to the respondent's computer files and therefore, perhaps, access to trade secrets, privileged material or proprietary information about the way the responding party uses computers to run its business that is not discoverable.[79] The latter method may be distasteful because it is expensive, time-consuming and potentially disruptive.[80] Assuming, however, that the respondent prefers one method over the other, is it entitled to elect which method it uses to produce responsive documents? And where producing hard copies of electronic documents in addition to producing those documents in electronic format consumes valuable resources and generates burdensome expenses, may the respondent shift the cost of that discovery to the requesting party?

Courts have addressed similar issues in the context of traditional discovery. But hard copies of electronic documents do not display embedded data—for example, the date and time the document was created.[81] Also, for reasons explained further in Part III.C.2., the production of electronic documents may infringe the proprietary or trade secret interests of the respondent. Courts must therefore recognize that the choice between producing a document in electronic format or hard copy is not necessarily analogous to choosing between

---

[78] Electronic storage devices typically permit users to replicate the information they store by copying data directly onto another electronic storage device, such as a floppy disk (which can fit in a shirt pocket without difficulty).

[79] For example, consider a Rule 34 request for any documents concerning the respondent's financial condition in 1999. The respondent might store that information in a customized spreadsheet program file. Producing the program file would not only reveal the financial information sought by the document request, but also might provide the requesting party with portions of the customized spreadsheet software and reveal how the respondent organized its program files to use financial information in the course of its business operations. *See also infra* Part III.C.2. for another example of how producing information in electronic form may infringe the proprietary rights of the respondent.

[80] Document requests may implicate such massive quantities of documents that printing those documents from the computer system would tie up printers for extended periods, thereby preventing others from using them and requiring extensive supervision.

[81] *See supra* Part I.C.1. (discussing embedded data).

the production of original and duplicate versions of a paper document. Given the technological differences between paper and electronic evidence, decisional law governing paper discovery may not shed much light upon how electronic discovery disputes should be resolved.

Because the volume of electronic evidence maintained by a party can be staggering, the questions raised above are not merely logistical details. In many cases they are of paramount importance, because the cost of electronic discovery may become the decisive factor in developing a comprehensive litigation strategy. Consider a Rule 34 demand asking that a corporation produce all written communications, including e-mail, in which the research and development of a specific product is discussed.[82] Assuming an objection to the scope and burden of such a request, a court may be required to apply the seldom-used "proportionality" limitations of Rule 26(b)(2).[83] Again, the phenomenon of massive document productions is not unique to electronic discovery. Computers, however, enable individuals and small businesses to store immense quantities of data—thus exposing them to the risk of litigation costs substantially out of proportion to their ability to bear those costs.

It is also easy to hypothesize situations in which courts will be faced with other difficult questions that have not previously been raised during discovery battles over paper-based evidence. For example, must a litigant search for embedded and backup files[84] to satisfy its mandatory initial disclosure obligations? Must a respondent search for and produce residual data—that is, documents or program files that were deleted but which remain at least partially intact? To what extent are computerized litigation support systems consisting of electronic documents created before litigation commenced protected by the work-product doctrine? Should there be limits on the extent to

---

[82] The Intel Corporation was required to respond to such a document demand propounded by the Federal Trade Commission in 1997.

[83] Rule 26(b)(2) allows courts to limit discovery in three specific circumstances: (i) where "the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive;" (ii) where "the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought;" or (iii) where "the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues." FED. R. CIV. P. 26(b)(2); *see infra* notes 164–66 and accompanying text (discussing proportionality provisions).

[84] *See supra* Part I.C.1. (explaining and defining these terms).

which non-parties may be required to produce electronic evidence and to bear the cost of that production?

While this Article cannot provide a thorough consideration of each of these issues, we raise them to underscore our concern that the nature of electronic evidence, and the logistics of its discovery, raise issues that may not be adequately addressed by Rule 34. That said, we turn to an examination of how courts currently address electronic discovery issues and specifically how Rule 34 has been applied to the two issues highlighted above—the manner in which electronic documents are produced and whether the costs of duplicate hard copy production of electronic evidence may be shifted to the requesting party.

B. *How Courts Currently Address Electronic Discovery*

Courts and commentators have generally interpreted Rule 34 and its accompanying Advisory Committee Note to allow the discovery of electronic evidence.[85] As Magistrate Judge Andrew Peck concluded in an oft-quoted phrase several years ago, "[T]oday it is black letter law that computerized data is discoverable if relevant."[86] And, one leading treatise on federal civil procedure states that "[t]he rule now clearly allows discovery of information even though the information is on computer."[87] The absence of any recent decisional law or commentary taking a contrary position illustrates that if there were doubts as to whether Rule 34 permitted discovery of electronic documents such as e-mail when it was amended in 1970, those doubts

---

[85] *See, e.g.*, Sanders v. Levy, 558 F.2d 636, 648 (2d Cir. 1977) (en banc) ("The 1970 Amendments to the Federal Rules rendered Rule 34 specifically applicable to the discovery of computerized information . . ."), *rev'd on other grounds sub nom.* Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340 (1978); *see also* Crown Life Ins. Co. v. Craig, 995 F.2d 1376, 1382–83 (7th Cir. 1993) (holding computerized data discoverable under Rule 34 even where discovery demand seeks "written documents"); Williams v. E.I. du Pont de Nemours & Co., 119 F.R.D. 648, 651 (W.D. Ky. 1987) (computerized database on disk and related explanatory description within scope of Rule 34 discovery); National Union Elec. Corp. v. Matsushita Elec. Indus. Co., 494 F. Supp. 1257, 1261–62 (E.D. Pa. 1980) (ordering plaintiff to produce computer tape in readable form); Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 221–22 (W.D. Va. 1972) (computer cards or tapes from master payroll file and computer printouts for W-2 form within scope of Rule 34).

[86] Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94 Civ. 2120, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995).

[87] 8 WRIGHT ET AL., *supra* note 21, § 2218, at 450 (the 1970 amendment to Rule 34 "brought the federal rules . . . into the computer age"); *see also* 7 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE § 34.12[3][a], at 34–37 (3d ed. 1999) ("Computer records and other electronically stored data are clearly within the permissible scope of discovery.").

now have been universally dispelled. As stated earlier, however, whether the Rules permit discovery of the newest forms of electronic evidence such as cookies, temporary files and residual data remains an open question.

A scattered body of case law dealing with electronic discovery disputes under Rule 34 has developed throughout the federal courts during the last fifteen years. Unfortunately, these opinions provide a less-than-crystalline legal framework regarding the issues presented by electronic discovery. For example, although it is widely agreed that Rule 34 permits discovery of electronic documents such as e-mail messages, little consensus exists on the manner in which such discovery should be conducted.[88]

There are several reasons why courts have failed to produce a coherent body of case law on these issues. First, district court opinions resolving discovery disputes are interlocutory in nature and thus not subject to immediate appeal.[89] Rather, the losing party must wait until final judgment has been entered before appealing a discovery order and then must show prejudice from pretrial rulings on discovery matters. Because discovery orders are rarely reviewed by the appellate courts, this body of law has been developed almost entirely by decisions of district and magistrate judges that are not controlling precedent even within their own district—a fact that disfavors uniformity. As one commentator recently noted:

> [C]ourts are hindered not only by technological obstacles to understanding the issues but also by the lack of any coherent body of law organizing the handful of relevant precedents in this largely-discretionary realm of adjudication. Thus, in recent cutting edge decisions over discovery into an opponent's computer system, courts write as if on a blank slate,

---

[88] *See, e.g., infra* text notes 104–11 (discussing conflict between the holdings of, *inter alia*, *Hasbro*, 1995 WL 649934, at *1 and Williams v. Owens-Illinois, Inc., 665 F.2d 918, 932–33 (9th Cir. 1982) on the issue of whether respondent must produce both hard copy and electronic version of discoverable information).

[89] *See, e.g.*, City of Las Vegas v. Foley, 747 F.2d 1294, 1297 (9th Cir. 1984) ("A discovery order, unlike a final order, is interlocutory and non-appealable under 28 U.S.C. § 1291.") (citing Hartley Pen Co. v. United States District Court, 287 F.2d 324, 326–27 (9th Cir. 1961)). Indeed, the vast majority of discovery decisions are issued orally rather than by written opinion.

> without acknowledging other decisions involving discovery of the same or analogous types of materials.[90]

Without any language in Rule 34 to guide them, courts have instead drawn on established discovery principles to resolve the disputes arising from electronic discovery, with varying degrees of clarity, consistency and persuasiveness.

1. Cases Addressing the Manner in Which Documents Are Produced Pursuant to Rule 34

In 1980, the Advisory Committee observed that "[i]t is apparently not rare for parties deliberately to mix critical documents with others in the hope of obscuring significance."[91] To prevent such discovery abuse, Rule 34 was amended to state that a party shall produce documents for inspection "as they are kept in the usual course of business or shall organize and label them to correspond with the categories in the request."[92] The language of the amendment is ambiguous, however, as to who is entitled to elect the manner of production. This ambiguity raises the following question: If the requesting party demands that the respondent produce documents in an organized and labeled manner, may the respondent nevertheless produce the requested documents as they are kept in the ordinary course of business? At least one early commentator argued the responding party has that option and could ignore a request specifying the manner of pro-

---

[90] Mark D. Robins, *Computers And The Discovery Of Evidence—A New Dimension To Civil Procedure*, 17 J. MARSHALL J. COMPUTER & INFO. L. 411, 412 (1999) (citing Fennel v. First Step Designs, Ltd., 83 F.3d 526 (1st Cir. 1996)); *see* Strasser v. Yalamanchi, 669 So. 2d 1142 (Fla. Ct. App. 1996). In an effort to organize this body of law, Mr. Robins divides the decisions related to electronic discovery into four categories: (1) cases resolving disputes over computer-related materials pertaining to trial testimony, such as electronically-stored data underlying an expert's conclusions; (2) cases resolving disputes over computer-related materials whose discovery will facilitate trial preparation, such as the electronic version of documents that have already been produced in hard copy; (3) cases resolving disputes over computer-related materials that have independent significance, such as electronic evidence relevant to a party's claim or defense; and (4) cases resolving disputes over discovery into the nature of an opponent's computer-storage media, such as efforts to discover the flaws in a party's procedures for inputting and processing information. *See* Robins, *supra*, at 428.

[91] Advisory Committee Note to Rule 34(b), in *Amendments to the Federal Rules of Civil Procedure*, 85 F.R.D. 521, 532 (1980).

[92] *See* FED. R. CIV. P. 34(b).

duction.[93] The few courts that have addressed the issue, however, generally have adopted a more flexible view.

The earliest reported decision regarding Rule 34's 1980 amendment is *Board of Education of Evanston Township High School v. Admiral Heating and Ventilating, Inc.*, in which three class actions were brought charging various piping construction companies and individuals with bid-rigging and price-fixing in the Chicago area from 1956 to 1977.[94] Plaintiffs requested documents relating to: (1) rewards for fictitious or complementary bids, or (2) proof that parties refrained from bidding. The issue arose as to whether defendants were required to segregate the requested documents to correspond to the terms of this request. In its opinion, the court noted that the very purpose of the 1980 amendment—preventing respondents from deliberately burying incriminating information among masses of irrelevant or unimportant documents—would be undermined if defendants were not required to produce their documents in a form that was usable by plaintiffs and ruled in plaintiffs' favor.[95]

This issue was litigated more recently in *T.N. Taube Corp. v. Marine Midland Mortgage Corp.*, which arose from a breach of contract claim brought by a microfilming service provider against a mortgage company.[96] In response to document requests, defendant produced 789 pages of unlabeled documents in no apparent order. Plaintiff then followed up with an interrogatory asking defendant to identify which documents responded to which document request, and defendant moved for a protective order contesting the interrogatory as overly broad, harassing and burdensome.[97]

Expressing doubt that defendant kept its records in the same state in which they were produced, the court ruled that defendant's initial document production did not meet the requirements of Rule 34:

> It is certainly improbable that Marine Midland routinely haphazardly stores documents in a cardboard box. As such, the Court believes the purposes of discovery, and basic considerations of fairness, require Defendant to organize the

---

[93] *See* Michael A. Pope, *Rule 34: Controlling the Paper Avalanche*, LITIG., Spring 1981, at 57 *cited in* Edward F. Sherman & Stephen O. Kinnard, *Federal Court Discovery In The 80's—Making The Rules Work*, 95 F.R.D. 245, 255 n.41 (1982).

[94] *See* 104 F.R.D. 23, 25 (N.D. Ill. 1984).

[95] *See id.* at 36 n.20 (citing Sherman & Kinnard, *supra* note 93, at 255–58).

[96] *See* 136 F.R.D. 449, 451 (W.D.N.C. 1991).

[97] *See id.* at 451.

> documents produced on 1 October 1990 in a manner clearly indicating which of these documents respond to Plaintiff's specific requests for production.[98]

The *T.N. Taube Corp.* decision is now cited as authority for the proposition that requesting parties can require respondent to label and organize documents if doing so is necessary to make the documents usable by the requesting party.[99]

A similar approach was taken by the District Court of Puerto Rico in *Bonilla v. Trebol Motors Corp.*, which involved a complex RICO claim against Trebol Motors Corporation ("Trebol") regarding its sales of Volvo cars.[100] Trebol produced over 100 boxes of documents concerning all types of car makes, models and years. The plaintiffs moved to compel Trebol to produce the documents in an orderly fashion with an index.[101] In granting the motion, the court found that case law "makes it clear that discovery must be produced in a manner to facilitate the mandates of Rule 1 regarding the just, speedy and efficient resolution of disputes."[102] The court, therefore, held that "[e]ven if Trebol Motors is producing the documents as they are kept in the normal course of business[,] . . . . [p]laintiffs are entitled to ask that they be produced in an orderly fashion consistent with the goals of the Federal Rules to determine all relevant facts quickly and efficiently."[103]

As these cases demonstrate, the ambiguity of the 1980 amendment to Rule 34(b) allowing the responding party initially to elect the manner in which it produces non-privileged, responsive documents. However, upon a showing of necessity, courts will direct the responding party to identify which documents are responsive to which requests. Yet only a few courts have addressed the application of the

---

[98] *See id.* at 456.

[99] *See, e.g.*, O'Connor v. Boeing N. Am., Inc., 185 F.R.D. 272, 277 (C.D. Cal. 1999); Capacchione v. Charlotte-Mecklenberg Sch., 182 F.R.D. 486, 490 (W.D.N.C. 1998); First Options of Chicago v. Wallenstein, No. 92–5770, 1994 WL 451160, at *4 (E.D. Pa. Feb. 14, 1994); Herdlein Techs., Inc. v. Century Contractors, Inc., 147 F.R.D. 103, 105 (W.D.N.C. 1993).

[100] No. 92–1795, 1997 WL 178844, at *1 (D.P.R. March 27, 1997), *partially rev'd on other grounds*, 150 F.3d 88 (1st Cir. 1998).

[101] *See id.* at *67.

[102] *See id.*

[103] *Id.* at *68 (citing Kozlowski v. Sears, Roebuck & Co., 73 F.R.D. 73, 76 (D. Mass. 1976)) (holding "to allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules").

1980 amendment to Rule 34 in the context of electronic discovery. In the case of *Anti-Monopoly v. Hasbro, Inc.*, a party resisted a request that it produce electronic evidence in the electronic form in which it was stored on the ground that it had already been produced in hard copy.[104] The reasons for the dispute were apparent: in order to best analyze the hard copy data, the requesting party would need to reenter it manually into computerized form—a time-consuming and expensive process. Obtaining the data in electronic form eliminates this step, allowing the requesting party immediately to analyze the data with the aid of a computer.

The court concluded that "[t]he law is clear that data in computerized form is discoverable even if paper 'hard copies' of the information have already been produced, and that the producing party can be required to design a computer program to extract the data from its computerized business records."[105] The opinion cites to *National Union Electric Corp. v. Matsushita Electronic Indus. Co.*, one of the earliest cases to touch on this issue.[106] The *Matsushita* court noted the Committee's comment: "[W]hen the [computerized] data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use [its] devices to translate the data into usable form[.]"[107] Based on this comment, the *Matsushita* court concluded that Rule 34 required a party to produce electronic evidence in an electronic format as well as in hard copy.[108]

The *Hasbro* court made no effort to distinguish *Williams v. Owens-Illinois, Inc.*, in which the Ninth Circuit came to a very different result.[109] The *Williams* case involved a claim of employment discrimination and the court held that plaintiffs could not discover defendant's computer tapes if defendant produced the information they contained on hard copy "wage cards." Without extensive discussion, the Ninth Circuit wrote:

> All information contained on the computer tapes was included in the wage cards which [plaintiffs] discovered. [Plaintiffs] were therefore not deprived of any data. While using the cards may be more time consuming, difficult and expensive, these reasons, of themselves, do not show that the

---

[104] *See* 1995 WL 649934, at *1.

[105] *Id.*

[106] *See* 494 F. Supp. 1257, 1261 (E.D. Pa. 1980).

[107] *Id.* at 1262.

[108] *See id.*

[109] *See Williams*, 665 F.2d at 932–33.

> trial judge abused his discretion in denying [plaintiffs] the tapes.[110]

Since it was published, the *Williams* opinion has been cited with approval and followed by at least two district courts outside the Ninth Circuit.[111]

The *Hasbro, Matsushita* and *Williams* line of cases provide examples of how courts must analogize to paper discovery in order to resolve electronic discovery issues that are not specifically addressed in Rule 34. Their failure to agree on whether respondents must produce both hard copy and electronic versions of discoverable information represents an example of the conflicting case law that exists with respect to crucial electronic discovery issues. As discussed below, to resolve such conflict, Rule 34 may require some revision.

2. Case Law Addressing the Cost of Producing Documents Under Rule 34

Ordinarily, the respondent bears the cost of gathering and reviewing documents while the requesting party bears the cost of copying responsive documents.[112] Rule 34, coupled with Rule 26(c), however, allows courts to shift costs between litigants upon a showing of "undue burden or expense."[113] For example, one court found that where a bank's microfilmed documents were not readable unless photocopied by special equipment, the bank was required to bear the costs of producing the documents in that fashion.[114] There is also at least one reported case that found a large Japanese manufacturing firm was required to pay plaintiff's reasonable expenses for translating certain of the firm's documents from Japanese to English on the theory that such expenses were reasonable costs of doing business in the United States.[115]

---

[110] *Id.* at 933.

[111] *See, e.g.*, Torrington Co. v. United States, No. 91–08–00568, 1992 WL 40699, at *2 (Ct. Int'l Trade Feb. 21, 1992) (citing *Williams* and deciding that plaintiffs were not entitled to discover database where defendant produced hard copies); Malone v. Ford Motor Co., No. 12539, 1992 WL 885097, at *2–3 (Va. Cir. Ct. Dec. 31, 1992) (same).

[112] *See, e.g.*, Continental Ill. Nat'l Bank & Trust Co. v. Caton, 136 F.R.D. 682, 685 (D. Kan. 1991); Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985).

[113] *See* FED. R. CIV. P. 26(c); *see also* Sanders v. Levy, 558 F.2d 636, 639 (2d Cir. 1977).

[114] *See* Delozier v. First Nat'l Bank of Gatlinburg, 109 F.R.D. 161, 164 (E.D. Tenn. 1986).

[115] *See* Stapleton v. Kawasaki Heavy Indus., Ltd., 69 F.R.D. 489, 490 (N.D. Ga. 1975). *But see In re* Puerto Rico Elec. Power Auth., 687 F.2d 501, 505–09 (1st Cir. 1982) (producing party not required to pay for English translations of documents written in another lan-

The distinct features of electronic documents and the novel logistical challenges of their production have required courts to address new questions regarding the application of the "undue burden or expense" standard established in Rule 26(c). One such question arises from the fact that, unlike paper-based information, computerized information may be encoded in such a way that special programs are needed to extract specific information from a respondent's data files. In such a situation, litigants often dispute who must pay for the creation and application of the special retrieval program.

This issue was addressed as early as 1980 in the case of *Dunn v. Midwestern Indemnity,* which arose from discrimination claims brought by an African-American couple against an insurance company.[116] Plaintiffs propounded discovery requests seeking information regarding defendant's computer capabilities, including raw data, programs and data management systems.[117] Defendant claimed such discovery was unduly burdensome and expensive because responding to it would require a "full person/year" to do the necessary research and investigation.[118] The *Dunn* court held an evidentiary hearing to evaluate the conflicting accounts of how great a burden responding to the discovery would actually impose and, in doing so, stressed "that impracticability is not to be equated with impossibility in this context."[119] The court then quoted the following language from *Kozlowski v. Sears, Roebuck & Co.*:

> The defendant may not excuse itself from compliance with Rule 34 by utilizing a system of record-keeping which conceals rather than discloses relevant records, or makes it unduly difficult to identify or locate them, thus rendering the production of documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery, by creating an inadequate filing system, and then claiming undue burden, would defeat the purposes of the discovery rules.[120]

---

guage); *In re* Korean Air Lines Disaster, 103 F.R.D. 357, 358 (D.D.C. 1984) (same); Cook v. Volkswagen of America, Inc., 101 F.R.D. 92, 92 (S.D.W. Va. 1984) (same).

[116] *See* 88 F.R.D. 191, 192–93 (S.D. Ohio 1980).

[117] *See id.* at 193.

[118] *See id.* at 197.

[119] *See id.*

[120] 88 F.R.D. at 198 (citing *Kozlowski*, 73 F.R.D. at 76).

Unfortunately, the *Dunn* court never published its decision following the evidentiary hearing.

In *Oppenheimer Fund, Inc. v. Sanders*, the Supreme Court addressed a related issue involving electronic discovery.[121] The *Sanders* decision arose from a class action brought against an open-end investment fund and its management corporation to recover damages caused by artificially inflated share values.[122] A dispute arose as to whether plaintiffs or defendants would be required to bear the expense of identifying class members by searching defendants' computerized records.[123] The District Court ruled that the cost of sorting lists of class members was defendants' responsibility,[124] and the Second Circuit, sitting *en banc*, affirmed that decision.[125] The Court of Appeals wrote:

> Here, the demand for computerized information creates a necessity for special programming, entailing the substantial expenditure of $16,000 by the [defendants] . . . . If the information demanded is such as the respondent might reasonably have expected to be required to make available for public examination or for use in the judicial process, it seems not unfair to require production of the information albeit necessitating special programming. In this and other respects, computer technology presents discovery problems with which the courts have developed relatively little familiarity.[126]

In reversing, the Supreme Court rejected this logic.[127] The Court wrote:

> There is no indication or contention that [defendants] acted in bad faith to conceal information from respondents. In addition, although it may be expensive to retrieve information stored in computers when no program yet exists for the particular job, there is no reason to think that the same information could be extracted any less expensively if the records were kept in less modern forms. Indeed, one might expect the reverse to be true, for otherwise computers would

---

[121] *See* 437 U.S. 340, 342 (1978).
[122] *See id.* at 342–43.
[123] *See id.* at 344–47.
[124] *See id.* at 346.
[125] *See id.* at 347.
[126] Sanders v. Levy, 558 F.2d 636, 649 (2d Cir. 1977).
[127] *See Oppenheimer Fund, Inc.*, 437 U.S. at 362–63.

> not have gained such widespread use in the storing and handling of information. Finally, the suggestion that petitioners should have used "different systems" to keep their records borders on the frivolous. Apart from the fact that no one has suggested what "different systems" petitioners should have used, we do not think a defendant should be penalized for not maintaining [its] records in the form most convenient to some potential future litigants whose identity and perceived needs could not have been anticipated.[128]

Plaintiffs were therefore required to shoulder the burden of paying for the cost of identifying class members.

The case of *Bills v. Kennecott Corp.* represents another early decision dealing with the allocation of electronic discovery costs.[129] In *Bills,* plaintiffs sought production of documents containing detailed information regarding defendant's employees.[130] Defendant offered to produce the information either in electronic form (i.e., on a computer storage device) or in hard copy (i.e., the printout of the computer tape). Defendant, however, conditioned its offer on the requirement that plaintiffs pay the costs of generating the information, approximately $5400.[131] Plaintiffs elected to receive the requested data in hard copy, but stated they would not pay for the cost of its production unless ordered to do so by the court.[132] Defendant produced the hard copy and then moved the court to shift costs under Rule 26(c).[133]

Observing that a producer had in the past been able to shift discovery costs to a requestor by making records available for inspection, the court noted that that option was often both undesirable and impractical with regard to electronic evidence. It was undesirable because of the dangers associated with allowing an opponent to range freely within one's computer system and impractical because of the lack of expertise needed to conduct such an inspection.[134] Thus, the court commented that "the requested party most often has no reasonable choice other than to produce the documentation in a com-

---

[128] *Id.*

[129] *See* 108 F.R.D. 459, 459 (D. Utah 1985).

[130] *See id.* at 460.

[131] *See id.*

[132] *See id.*

[133] *See id.*

[134] *See Bills,* 108 F.R.D. at 462.

prehensible form by use of its own computer technicians"[135] and also must "shoulder the burden of showing 'undue' expense" under Rule 26 before courts shift the costs to the requesting party.[136] Finding that Rule 26 required such issues to be resolved on a case-by-case basis rather than by "iron-clad formula,"[137] the court denied the defendant's request to shift costs for four reasons: (1) the amount of money involved was not excessive or inordinate; (2) the relative expense or burden would be substantially greater to the plaintiffs than it would to the defendant; (3) the costs would be a substantial burden to plaintiffs; and (4) the responding party derived some benefit by producing the data in question.[138]

The Seventh Circuit addressed a similar discovery issue in *Sattar v. Motorola*.[139] Plaintiff Sattar filed a motion that in effect asked the court to require Motorola to produce 210,000 pages of e-mail in hard copy.[140] Motorola had produced these e-mail messages in electronic form on tapes, but Sattar lacked the software necessary to read them.[141] The Court of Appeals affirmed the District Court's order requiring Motorola to provide Sattar with the electronic devices or software necessary to read the produced material or, in the alternative, to pay for half the cost of producing the e-mail messages in hard copy.[142]

Courts appear to have been reluctant to force requesting parties to bear the costs of gathering and producing in usable form electronic evidence responsive to a Rule 34 document request. Particularly, the *Bills* and *Sattar* decisions have been followed in cases involving substantially-greater discovery costs. Indeed, parties responding to discovery requests have been required to search through thirty-million pages of documents, at costs as high as $70,000, in order to retrieve and produce e-mail data.[143] The guiding principle in such cases appears to be the concern that technological advancements should not alter the framework of civil litigation by shifting costs of discovery. As one court explained:

---

[135] *See id.*

[136] *See id.*

[137] *See id.* at 463.

[138] *See id.* at 464,

[139] *See* 138 F.3d 1164, 1171 (7th Cir. 1998).

[140] *See id.*

[141] *See id.*

[142] *See id.*

[143] *See In re* Brand Name Prescription Drugs Antitrust Litig., No. 94 C 897, 1995 WL 360526, at ** 1, 3 (N.D. Ill. June 15, 1995).

> It would be a dangerous development in the law if new techniques for easing the use of information became a hindrance to discovery or disclosure in litigation. The use of excessive technical distinctions is inconsistent with the guiding principle that information which is stored, used or transmitted in new forms should be available through discovery with the same openness as traditional forms . . . . The normal and reasonable translation of electronic data into a form usable by the discovering party should be the ordinary and foreseeable burden of a respondent in the absence of a showing of extraordinary hardship.[144]

While there are too few decisions on point to predict a trend in the case law with any real confidence, it would appear the *Bills, Brand Name Prescription Drugs* and *Daewoo Electronics Co.* decisions, in conjunction with the Supreme Court's holding in *Sanders*, represent an emerging majority position that places a fairly heavy burden of persuasion on the party seeking to shift the costs of electronic discovery.

The *Dunn, Bills* and *Sanders* decisions represent only a few examples of how cost-shifting problems raised in the context of electronic discovery are handled under the current discovery rules. These cases, like *Hasbro, Williams* and their progeny, show that while courts have managed to resolve motions that raise Rule 34 questions in the context of electronic discovery, they have generally approached these questions in a highly fact-specific manner, producing few general principles to aid in the resolution of similar disputes. The courts are left to develop procedural standards regarding electronic discovery under Rule 34 in the absence of express guidance from the Rules themselves. To date, however, little consensus has developed as to what these principles should be.

C. *The Differences Between Paper and Electronic Evidence*

Rule 34, its Note and the case law cited above suggest courts should resolve electronic discovery disputes by drawing analogies to traditional discovery disputes. Yet electronic evidence is intrinsically different from paper evidence in ways that become important to the analysis of discovery disputes. These differences may be summarized by observing that, unlike paper evidence, electronic evidence is typi-

---

[144] Daewoo Elecs. Co. v. United States, 650 F. Supp. 1003, 1006 (Ct. Int'l Trade 1986), *cited in Brand Name Prescription Drugs*, 1995 WL 360526, at *2.

cally *encoded, processable, invisible, emulatable, proprietary* and *voluminous.* Each of these terms and the concepts they summarize are discussed below.

1. Electronic Evidence Is Always Encoded

Relatively few paper documents are encoded in the way computers code electronic data.[145] As explained in Part I.B. above, electronic data are stored in binary form in electronic transistors, each of which constitutes a "bit" of information. Making those bits of data meaningful requires the knowledge of how the bits are grouped into letters, symbols, visual images or sound—in other words, knowledge of the "code" to the particular piece of electronic evidence. The ASCII code discussed in Part I.B. is a simple example of how even the most basic electronic information is coded. Without knowledge of the ASCII code, English letters stored in the form of binary numerals remain nothing more than a series of unintelligible zeros and ones. This is particularly true of digitalized audio, video and compressed data and information in a database.

Thus, from a technological perspective, electronically-stored information has two components: the raw data, stored in binary format, and the code necessary to make use of that data, which is also stored in binary format. This method of data storage raises the question of whether the term "document" as used in Rule 34 encompasses both data and code, or simply the data alone. Drawing on the text of Rule 34, the data comprises the "document," while the code is the "detection device" by which that document is "translated" into "usable form." Rule 34 currently does not recognize this distinction.

2. Electronic Evidence Often Contains Proprietary Characteristics

The difference between "documents" and "data" has practical ramifications because, in some cases, it may not be possible to require a litigant to provide the codes needed to use or "translate" electronic documents. By turning over the code for reading discoverable electronic documents, a litigant may also, knowingly or not, provide at the very least a clue (if not a complete road map) to its computer system

[145] We recognize that paper evidence can be, and sometimes is, encrypted just like computerized data. For example, a confidential letter might be written in code, which would require any reader to know that code before the letter could be understood. However, whereas the bulk of paper evidence used in everyday life is not encoded, electronic evidence is necessarily coded because of the way computers store information.

and the way that computer system is used. In some situations, providing such information may be both unacceptable to the respondent and not authorized by Rule 34.

By way of example, imagine a lawsuit between two pizza companies involving a garden-variety commercial dispute. A request is made for all documents regarding the time and location of sales of delivered pizzas during 1999. The respondent, unbeknownst to its competitors in the industry (including the propounding party), keeps a fully-customized computerized data base of its customers, including not only the information sought by the document request (the time and location of pizza sales), but also related information about the customer's drink and dessert of preference. This information is used to increase customer goodwill, the efficiency of the pizza delivery system and forms the backbone of the respondent's direct marketing initiative. Furthermore, this information is collected by way of a Web site that allows customers to order their delivered pizzas on-line. For purposes of the example, let us assume the idea of using computers to increase pizza sales in this manner is both startlingly innovative and remarkably effective.

In this example, the data regarding the time and location of pizza sales are discoverable. However, the respondent's "code," and indeed, the very existence of a computerized customer information data base, represents a valuable trade secret. If the respondent is required to produce its discoverable electronic documents as well as the code used to translate those documents into usable form, it will in effect be producing its most closely protected proprietary information.[146] Alternatively, it might be that the respondent pizza company's custom data base was sold to it by a third party under a licensing agreement that prohibits disclosure of the data base program to a third party without additional payments to its author.

This example demonstrates that the requirement that a respondent provide the translating mechanism under Rule 34,[147] when ap-

---

[146] Computer programs are afforded intellectual property protection under copyright and patent law. *See, e.g.*, Computer Assocs. Int'l v. Altai, Inc., 982 F.2d 693, 701 (2d Cir. 1992). Also, customer lists are clearly entitled to protection. *See* North Atl. Instruments, Inc. v. Haber & Apex Signal Corp., 188 F.3d 38, 44–46 (2d Cir. 1999).

[147] Rule 34(a) allows a party to serve a document request for designated documents "translated, if necessary, by the respondent through detection devices into reasonably usable form." *See* FED. R. CIV. P. 34(a) The Committee's Note also explains that respondents may be required to use their own devices to translate "data compilations" if necessary to allow the discovering party to make use of those data compilations. *See* FED. R. CIV. P. 34(a) advisory committee's note (1970).

plied in the context of electronic documents, may well infringe the proprietary characteristics of computer programming codes. As a result, Rule 34 document requests may require production of electronically-stored information beyond the proper scope of discovery, requiring respondents to seek the protection of Rule 26(c).

3. Electronic Evidence Is Always Processable

Rule 34 does not contemplate another important distinction between paper evidence and electronic evidence. The latter is, by nature, computer processable and this characteristic has vital practical ramifications. For example, consider a set of 100,000 pages of paper documents and the same set of documents stored in electronic format. The paper documents will take up at least fifty boxes worth of storage space and require significant time and money to move from place to place. Duplicating that many documents would cost thousands of dollars. More to the point, it would be extremely difficult to search through so many documents for specific information. Assuming, for example, the average associate or paralegal can carefully review 100 pages an hour (surely an optimistic estimate), it would take 1000 hours of billable time to review this set of documents. By comparison, the average office computer could search all of the documents for specific words or combination of words in minutes, perhaps less.[148]

Despite the practical distinctions between electronic and paper evidence, the Notes following Rule 34 imply that a hard copy printout of electronic evidence is the working equivalent of the evidence itself.[149] The unfortunate result is that courts, such as the Ninth Circuit in the *Williams* decision, may view a litigant's attempt to obtain the electronic version of information it already possesses in hard copy as overreaching.

---

[148] The comparative value of electronically-stored information, as compared with information stored on paper, was discussed by the D.C. Circuit in *Public Citizen v. Carlin*. *See* 184 F.3d 900, 908–10 (D.C. Cir. 1999) (upholding regulations issued by United States Archivist permitting disposal of electronic records created by federal agencies if hard copy versions existed).

[149] "The inclusive description of 'documents' . . . makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use [its] devices to translate the data into usable form. *In many instances, this means that respondent will have to supply a print-out of computer data.*" FED. R. CIV. P. 34. advisory committee's note (1970) (emphasis added).

4. Electronic Evidence Is Often Invisible

For reasons discussed in Part I.C., a large amount of electronic information remains unknown and unseen by computer users because it is created by the computers themselves. Examples of such computer-created information include backup and temporary files, as well as embedded information.[150] Alternatively, electronic information might be unknown to users because it exists in residual form after being deleted by the user. Such information cannot typically be viewed or even located by the average computer user (indeed, the average computer user does not know such data exists at all) but it is recoverable and usable nonetheless.

The existence of a growing universe of "invisible" evidence raises the question of whether litigants responding to a Rule 34 request are required to search for it. It raises new definitional questions as well. For example, are embedded data or backup data "documents" or simply addenda and duplicates? Does a deleted document that continues to exist in residual form constitute a "document" for purposes of Rule 34?

Residual data raises another definitional question. Rule 34 requires respondents to produce responsive, discoverable documents in the manner in which they are "kept in the usual course of business" or labeled to indicate the document request to which they respond. Because residual data is information that was discarded by its creator—but nevertheless remains in a computer's storage device—how can it be produced as it is "kept in the ordinary course of business?" Respondents are presumably not required to produce the shredded remains of what once were documents falling within the scope of a proper document demand; by analogy, they might not be required to produce residual data in electronic format. Also, may a respondent be said to be in the "possession, custody or control" of the residual data stored on the computer?[151] The resolution of that question is important because it determines whether a respondent is obliged to search for and produce such information under the terms of Rule 34(a).

5. Electronic Evidence Is Perfectly and Easily Emulatable

By the term "emulatable" we intend to describe two related qualities of electronic information. The first quality relates to the ease and

---

[150] *See supra* Part I.C.1.(describing backup, temporary and embedded computer files).
[151] *See* FED. R. CIV. P. 34(a).

speed with which electronically-stored data may be reproduced. Although copy and facsimile machines have made it relatively easy to duplicate and transmit paper-based information quickly and inexpensively, computerized information may be duplicated and transmitted many times more quickly and inexpensively. Consider the 100,000 pages of paper documents discussed above. Assuming the average copy machine can copy one page per second at a cost of ten cents per page, it would take just over twenty-seven hours and $10,000 to reproduce every page. By comparison, copying an equivalent amount of electronically-stored information to a portable storage device such as a floppy disk could be done in minutes for very little cost.

The second quality we mean to describe by the term "emulatable" relates to the usual differences—or lack thereof—between original versions of electronic evidence and duplicate copies. Even the best color copy machines cannot reproduce every detail of an original; slight tears in the paper, smudges in the margin or even highlighted portions of text will not necessarily be perfectly reproduced, if they are reproduced at all, on the duplicate. Consequently, it is often easy for the average person to notice differences between original and duplicate copies of paper documents. In contrast, because electronic evidence at its elemental level consists of nothing more than zeros and ones in a specific pattern, there is usually no way to distinguish between an original and a copy. For example, because a lay person cannot distinguish between different versions of electronic evidence, it is relatively easy for litigants (or prospective litigants) to tamper with evidence stored in electronic format in an effort to bolster their claims. Indeed, the New York City police recently arrested Christian Curry, a junior financial analyst at Morgan Stanley, for attempting to do just that.[152] Mr. Curry allegedly paid an undercover police officer to plant false homophobic and racist e-mail messages in Morgan Stanley's computer system to bolster Mr. Curry's wrongful termination lawsuit against the company.[153]

6. Electronic Evidence Exists in Voluminous Quantities

Computer technology has produced a society in which information is constantly demanded, created, transmitted and digested in quantities that would have been unthinkable twenty-five years ago. Certainly there is no question that the storage capacity of desk-top

[152] *See* Howard W. Goldstein, *Corporate Crime*, N.Y. L.J., July 29, 1999, at 5.
[153] *See id.*

computers has rapidly increased over the last decade and continues to do so. Today's floppy disks, which are the slowest and smallest electronic storage devices, can store between 700 kilobytes and 2.88 megabytes of information. Hard drives that store 3000 to 4000 megabytes (or three to four "gigabytes") are commonplace.[154] This means that the average desk-top computer can store millions of pages of text.

The use of computers in everyday life and the concomitant increase in computer data storage capacity has exponentially inflated the universe of discoverable information. In today's world, the mandatory disclosure rules or routine discovery requests in the simplest federal lawsuit can easily implicate thousands of pages of electronic documents. As noted earlier, the phenomenon of massive document productions are not new. Computer technology, however, all but ensures that such discovery burdens will become more commonplace as even the smallest lawsuits may begin to generate immense quantities of discoverable documents.

D. *Rule 34 Fails to Utilize Computer Technology to Prevent a Rise in Discovery Costs*

Rule 34 discovery costs, measured in both time and money, will continue to rise as the universe of discoverable documents expands. Any evaluation of the application of Rule 34 to electronic records must take this fact into consideration. The architects of the Anglo-American civil justice system have long addressed complaints regarding the speed with which litigation progresses.[155] In more recent years, the cost of litigation has become a central concern.[156] Yet despite procedural reforms, the costs of litigation continue to rise.[157] Computer technology and the increase in electronically-stored information pre-

---

[154] WHITE, *supra* note 27, at 83. Data storage capabilities are rapidly increasing; some of today's personal computers can store as much as fifty gigbytes of information.

[155] "To no one will We sell, to none will We deny or delay, right or justice." MAGNA CARTA (1215); *see also* Judge Irving R. Kaufman, *The Philosophy Of Effective Judicial Supervision Over Litigation*, 29 F.R.D. 207, 215-16 (1961) (stating in reference to the Magna Carta that "almost 750 years later, that great and simple pledge has not yet been completely fulfilled" and noting the late Chief Justice Earl Warren had appealed to each judge "to bring the full prestige of his judicial office to bear 'at every stage of litigation in order to ensure promptness and efficiency.'").

[156] *See* FED. R. CIV. P. 1 (Rules should be interpreted to ensure the "just, speedy, and inexpensive determination of every action.").

[157] *See, e.g.*, Boston & Maine Corp. v. Town of Hampton, 987 F.2d 855, 865 (1st Cir. 1993) (noting rising cost of litigation); Mitchell A. Orpett, *The Litigation Cost Crisis: Is There A Professional In The House?*, BRIEF, Fall 1998, at 33 (same).

sent an unprecedented opportunity to harness technology so as to prevent a rise in the delays and costs of discovery under Rule 34.

A simple example illustrates the point. Computers allow litigants to locate, copy and transmit discoverable electronic information thousands of times more efficiently than traditional document review methods. For example, consider a document request propounded to a large corporation asking for all communications between members of a specific division of the company and a third party. If the responding party kept electronic versions of correspondence (all transmitted by e-mail or documents generated by computer) it could conduct a computerized search through thousands of communications for documents matching that description in minutes. Assuming there were no need to review the documents for privileged material—an assumption addressed below—responsive communications could then be duplicated at almost no cost and transmitted instantly to the requesting party. As a natural by-product of this discovery process, both parties would have created a computerized database of potentially-relevant evidence, that eventually could be used to marshal evidence in preparation for motion practice or trial.

If the same document request were directed to paper documents, the responding party would be required to use its attorneys or paralegal staff to search for, identify, gather and review thousands, if not millions, of responsive documents. These documents would then be duplicated and shipped at the requesting party's expense. As a result, both parties would incur significant discovery costs.[158]

This idealized picture of electronic discovery remains unrealistic under the current discovery rules. The prevailing rules of privilege require a responding party to review each of its documents before production in order to preserve the right to assert an objection based on a privilege. The inadvertent production of privileged material may in some cases waive the privilege forever[159]—not only for that material but also for the subject matter addressed in that material. Thus, even if computers can locate responsive materials, respondents must then

---

[158] Assuming the responding party reviewed 10,000 pages of documents at a cost of $100 per hour (a low estimate), and assuming the review of 100 pages per hour, the total fees for the document review would be $10,000. The requesting party would incur copying charges in the neighborhood of $1000 (assuming a cost of ten cents per page) as well as shipping costs simply to get the requested documents to its attorneys and then would incur additional fees for its own attorneys' review of documents.

[159] *See, e.g.*, S.E.C. v. Cassano, 189 F.R.D. 83, 86 (S.D.N.Y. 1999); Aramony v. United Way of America, 969 F. Supp. 226, 235 (S.D.N.Y. 1997); Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985).

manually review those responsive documents to determine if they are privileged.[160]

The current Rules pose at least two additional obstacles to speedy and inexpensive production of electronic documents. Under Rule 34(b), a responding party need not produce requested documents for thirty days even if it is able to locate those documents within minutes.[161] Furthermore, as we have discussed above, a respondent may elect to produce only the hard copy of responsive documents, thereby potentially forcing the requesting party both to incur the cost of duplicating those documents (unless the requesting party prevails on a cost-shifting motion) and to forego the benefit of being able to conduct computerized searches without manually entering the hard copy documents into electronic form.

E. *Rule 34 Does Not Address Cost Issues*

Cost-shifting is now the exception to the general rule that litigants bear the cost of preparing their own case. The Rules now allow litigants to shift the cost of responding to discovery only upon a showing of "oppression" or "undue burden or expense."[162] Yet neither Rule 26(c) nor Rule 34 defines those terms and the Notes shed no further light on their precise meaning.[163] Judges are left to determine cost-shifting motions on a fact-intensive basis by drawing on the often-ignored "proportionality" provisions of Rule 26(b)(2).[164] However, as

---

[160] We are unaware of any computerized search programs capable of determining whether a document contains privileged communications. Computers, however, could easily assist reviewers in the process. For example, computers could be used to identify whether the author or recipient of any given communication was an attorney employed by the client at the time the communication was made. Computers also could be used to quickly flag documents containing key words likely to indicate a document that contained an attorney-client privileged communication.

[161] *See* FED. R. CIV. P. 34(b).

[162] Rule 26(c) allows the shifting of discovery costs "to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense[.]" FED. R. CIV. P. 26(c). *See, e.g.*, Playboy Enters., Inc. v. Welles, 60 F. Supp. 2d 1050, 1053–54 (S.D. Cal. 1999); *In re* First Am. Corp., 184 F.R.D. 234, 239 (S.D.N.Y. 1998).

[163] *See* FED. R. CIV. P. 26(c), 34(a) and advisory committee's note (1970).

[164] These provisions state: "The frequency or extent of use of the discovery methods otherwise permitted under these rules and by any local rule shall be limited by the court if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or is obtainable from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the

at least one prominent scholar has noted, the proportionality provisions "were something of a dud" because judges rarely have the familiarity with any given case to apply them accurately.[165]

An implicit financial calculation underlies this approach to cost-shifting. Where discovery costs are relatively low, the comparative expense of litigating a cost-shifting motion is difficult to justify. Thus, while the Rules require judicial intervention to resolve disputes over discovery that is perceived to be unduly burdensome or expensive, the real-world economics of litigation limits the need for such intervention to cases where discovery costs greatly exceed the expense of litigating a motion to shift costs. Until recently, such cases were relatively rare.

An increase in the discovery of electronic evidence, however, may lead to a rise in the costs of discovery for several reasons. First, there is the sheer increase in the amount of discoverable information. In a world where even the most rudimentary computerized devices have massive storage capacity, it seems inevitable that a typical Rule 34 document request (or even mandatory initial disclosures) will require litigants and their attorneys to review thousands, if not millions, of pages of electronically-stored information. Thus, where yesterday's document production involved a box of paper, today's may involve a roomful.[166]

Second, because computerized information tends to exist in duplicate form in various locations,[167] litigants may legitimately cast their

---

litigation, and the importance of the proposed discovery in resolving the issues." FED. R. CIV. P. 26(b)(2).

[165] *See* Richard L. Marcus, *Retooling American Discovery For The Twenty-First Century: Toward A New World Order?* 7 TUL. J. INT'L & COMP. L. 153, 162–63 (1999). Professor Marcus recognizes, however, that the proportionality provisions of Rule 26(b)(2) have made it "'clearer than it was before that [judges] should take responsibility for the amount of discovery in the cases they manage.'" *Id.* at 163 (quoting 8 WRIGHT ET AL., *supra* note 21, § 2008.1, at 121); *see also* Richard L. Marcus, *Discovery Containment Redux*, 39 B.C. L. REV. 747, 773–74 (1998) (discussing the failure of the proportionality provisions of Rule 26 to change significantly federal discovery).

[166] *See, e.g.*, *In Re* Brand Name Prescription Drugs Antitrust Litig., No. 94 C 897, 1995 WL 360526, at *2 (N.D. Ill. June 15, 1995) (litigant required to search 30 million pages of documents at a cost of $70,000 to retrieve and produce e-mail data).

[167] *See supra* Part I.C.1. (describing backup and temporary files, as well as residual data). Duplicate versions of information exist for another reason as well. Most e-mail programs allow users to automatically reply to an e-mail communication in a manner that sends both the reply and the original message. Similarly, the text of e-mail communications can be forwarded to multiple individuals along with additional comments. The result is commonly referred to as "e-mail chains" where a critical communication may be passed on to many users and stored on their computer as a data file.

discovery nets wider to search for relevant information. One expert in the field recommends the following:

> In many cases, one of the first witnesses to be deposed should be a member of the opposing party's information technology (IT) department. Such a witness can provide valuable insight into the topology and operation of the party's computer system and network, the methods used to insure security of data, sources of potential physical evidence . . . .[168]

The same expert recommends that the attorney conducting such a deposition bring a computer expert to assist.[169] The need to employ computer experts to assist with discovery will inevitably increase its cost. Third, the tendency of computerized information to exist in duplicate form will require respondents to search multiple locations to ensure they comply with their obligations to produce all discoverable information. As the average cost of responding to Rule 34 document requests rises, the calculus of discovery costs to motion costs will shift, and it is almost certain that the incidence of cost-shifting motions will increase as well.

IV. Streamlining Electronic Discovery Under Rule 34

This Part offers two practical solutions to some of the definitional and logistical difficulties arising from electronic discovery under Rule 34. First, it proposes to amend Rule 34(a) so as to allow discovery of all forms of electronic evidence that are within the respondent's possession, custody and control. Second, this Part suggests an addition to Rule 34(b) to assist in streamlining electronic discovery and reducing cost-shifting disputes. After explaining these proposals in detail, this Part also discusses why these revisions are necessary and why the same results cannot be achieved by way of decisional law.

A. *Defining the Scope of Rule 34(a) to Include All Forms of Electronic Evidence That Are Within the Respondent's Possession, Custody or Control*

The Notes following the 1970 amendments to Rule 34 explain that the Rule was revised "to accord with changing technology."[170] To

---

[168] Overly, *supra* note 20, § 1.01, at 3–10.

[169] *See id.*

[170] *See* Fed. R. Civ. P. 34(a) advisory committee's note (1970).

that end, as explained above, Rule 34(a) expressly defines the term "documents" to include not only "writings, drawings, graphs, charts, photographs, [and] phonorecords[,]" but also "other data compilations from which information can be obtained."[171] The Notes envision that respondents may be required to print "data compilations" in hard copy in order to translate that information into usable form.[172]

Now, thirty years after these revisions to Rule 34, the Rule must be revised once again "to accord with changing technology."[173] Forms of electronic evidence that could not have been foreseen in 1970 and that do not easily fall within the category of "data compilations" are now commonplace. Embedded data, Web caches, history, temporary, cookie and backup files—all of which are forms of electronically-stored information automatically created by computer programs rather than by computer users—do not obviously fall within the scope of the term "documents." Certainly they are not "documents" in any traditional sense. Furthermore, they arguably do not constitute "compilations" of data, as that term is commonly understood.[174] They are, in essence, a new breed of information, a breed not easily categorized within the scope of Rule 34(a).

Excluding such computer-created electronic evidence from the scope of Rule 34(a) would effectively shield it from the discovery process. Yet such information represents a potentially fruitful means by which litigants may discover important facts. Thus, for the Rules to ignore such evidence does violence to a fundamental goal of the civil justice system—to find the truth of disputed events.

For these reasons, Rule 34(a)(1) should permit litigants to request the production of any form of electronic evidence—whether it was originally created by a person or a computer and whether it is a "compilation" or newly-created information—so long as the respondent has "possession, custody or control" of the requested evidence. As shown below, only minor revisions to Rule 34(a) would be needed to effect such a change:

> (a) 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

---

[171] *See* FED. R. CIV. P. 34(a).

[172] *See* FED. R. CIV. P. 34(a) advisory committee's note (1970).

[173] *See* FED. R. CIV. P. 34(a).

[174] A cookie file, for example, constitutes newly-created information generated by a Web site and stored by a computer's browser program without the involvement of the computer user and therefore arguably is not a "compilation" at all.

> copy any designated documents ***or any designated data*** (including writings, drawings, graphs, charts, photographs, phonorecords, and **electronically-stored information** ~~other data compilations from which information can be obtained~~, translated, if necessary, by the respondent through detection devices into reasonably-usable form), or to inspect and copy, test, or sample any tangible things which constitute or contain matters within the scope of Rule 26(b)~~, and~~ which are in the possession, custody or control of the party upon whom the request is served [. . . .][175]

The addition of the phrases "or any designated data" and "electronically-stored information" would eliminate the need to define "documents" to include "data compilations." The deletion of the term "and" and addition of a comma after "Rule 26(b)" clarifies that respondents are only required to produce documents, data and tangible things which are within their "possession, custody or control." This limitation balances the broad inclusion of "any designated data" and protects respondents from requests for data that would require them to search for information outside of their own computer systems or immediate control.[176]

Under the revised Rule, embedded data, history, cookie and cache files, as well as clone, temporary and backup files would be within the scope of Rule 34(a), so long as they were within the "possession, custody or control" of the respondent.[177] Rule 34(a) would also include computer logs and access control lists, as well as data created by employee monitoring software (again on the condition that they were within the respondent's possession, custody or control).

---

[175] Additions to the current Rule are set forth in bold text (including the comma following ". . . the scope of Rule 26(b)"), deletions in strike-through text.

[176] As explained in Part IV.C., if and when residual data is within a respondent's "possession, custody or control" is a complex issue that, while beyond the scope of this Article, will have to be addressed in the future.

[177] In the context of paper discovery, a reasonableness test is used to determine whether a record is in the "possession, custody or control" of a party, and parties are not required to produce material when doing so would be unduly burdensome. *See, e.g.*, Chaveriat v. Williams Pipe Line Co., 11 F.3d 1420, 1426–27 (7th Cir. 1993) (party need not produce documents simply because it could obtain that document "if it tried hard enough"); Bank of N.Y. v. Meridien BIAO Bank Tanzania Ltd., 171 F.R.D. 135, 146 (S.D.N.Y. 1997) (document is considered to be within a party's "control" if that party reasonably can obtain the document from a non-party); Wardrip v. Hart, 934 F. Supp. 1282, 1286 (D. Kan. 1996) (defendant must produce records in possession of his accountant, because defendant had a legal right to obtain those records).

More significantly, the proposed Rule allows the discovery of both "documents" and "data" but distinguishes between the two. This revision would provide a textual basis for developing separate bodies of case law for discovery of "documents" and "data." In turn, this would allow courts to acknowledge the special characteristics of electronic evidence when dealing with questions such as privilege, proprietary interests and protective orders, "undue burden" or possession, custody and control.

B. *Amending Rule 34 to Reduce Judicial Intervention and to Harness the Potential of Computerized Document Productions*

Defining Rule 34(a) to allow discovery of all forms of electronic evidence that are within the respondent's possession, custody or control is a step in the right direction. Such refinements to the Rule, however, do not address the logistical issues discussed in Part III. To do so, another revision to the Rule is necessary. We propose the following addendum to the final paragraph of Rule 34(b):

> All electronically-stored information shall be produced in the same form in which it is stored, presumptively subject to a protective order under Rule 26(c)(7) barring the release of such information to third parties other than the requesting party's expert witnesses. Any party represented by counsel requesting the production of electronically-stored information in printed form in addition to, or instead of, its electronic form shall bear all costs associated with the requested production.

This brief addition to the Rule would have several advantages, as discussed below.

To begin, the proposed addition to Rule 34(b) directly addresses the existing ambiguity[178] as to the manner in which electronic evidence must be produced by laying down a clear and simple rule that practitioners should not have difficulty following and judges should not have difficulty applying. The requirement that electronic evidence be produced in electronic form accords with the persuasive holding of the *Hasbro* decision, which reasoned that by requiring the respondent to translate discoverable data into "reasonably-usable form," Rule 34 mandates the production of electronic evidence in

---

[178] *See supra* Part III.B.1. (describing conflicting case law on this issue).

electronic form.[179] The contrary position endorsed by the Ninth Circuit's *Williams* decision simply fails to recognize that, as a practical matter, the electronic version of discoverable information is often more useful than its hard copy version because it may be processed by computer without incurring the cost of transforming it from hard copy to electronic format.[180]

Also, by adopting the *Hasbro* position, the proposed addition to Rule 34 ameliorates the somewhat outdated statement in the Note to the 1970 amendment indicating that respondents may satisfy their obligation to respond to Rule 34 discovery by providing a printout of "data compilations." While this may have been so in 1970, producing hard copy versions of electronic evidence is not the practical equivalent of producing the same evidence electronically.

Additionally, requiring the production of electronic evidence in electronic form and creating a cost incentive not to request the same information in hard copy will also reduce the overall costs of Rule 34 discovery. As indicated earlier, massive quantities of electronic evidence may be duplicated and transmitted across long distances at very little cost. By comparison, the duplication, shipping and storage of paper documents requires litigants to incur high costs. Considering that one personal computer typically is capable of storing two million pages of information, the system-wide potential cost savings resulting from this addition to Rule 34 are significant.[181]

The proposed addition to Rule 34 also reduces the incentive for a requesting party to file a Rule 26(c) motion to shift the cost of producing duplicate hard copies of electronic evidence by creating a presumption that the requesting party must bear those costs. This presumption is not a departure from the majority position—namely, that parties presumptively bear the cost of preparing their cases.[182]

It could be argued that a more efficient method of reducing cost-shifting motions, and thus keeping judges out of the discovery process, would be to eliminate the possibility of doing so entirely. For example, Rule 34 could be amended to require, without exceptio, that a

---

[179] *See* 94 Civ. 2120, 1995 WL 649934, at *1–2 (S.D.N.Y. Nov. 3, 1995).

[180] *See* Williams v. Owens–Illinois, Inc., 665 F.2d 918, 932–33 (9th Cir. 1982).

[181] Requiring the production of discoverable electronic evidence in electronic form might also lessen, to some degree, the environmental impact of litigation by reducing unnecessary use of paper.

[182] This proposal rejects the position that the burden of persuasion rests on respondents seeking to shift costs under Rule 26(c). *See, e.g.*, Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985) (stating respondent must "shoulder the burden of showing 'undue' expense" under Rule 26 before courts shift the costs to the requesting party . . .").

requesting party seeking the production of electronic data in hard copy format must pay for the costs of producing a duplicate hard copy. This amendment would eliminate the possibility of shifting production costs by way of a Rule 26(c) motion. Such a departure from the existing cost-shifting rules, however, may be unwise. The Rules as a whole are designed to allow trial courts enough flexibility to take into consideration the circumstances of each case. Fixing the costs generated by Rule 34 requests on the discovering party in all cases would be a significant step away from this design.

Indeed, not everyone has a computer and one can imagine a case where a party does not have the capability to utilize electronic evidence. For this reason, the proposed amendment excludes litigants who represent themselves, as they typically have less access to and familiarity with computer technology. In such cases; fairness demands that Rules 26 and 34 should permit a party to request the production of electronic evidence in hard copy without necessarily incurring the cost of that production.

Consider the inequity of a rule that required prisoner litigants without access to computers and with no source of income to pay for the cost of a Rule 34 request propounded on a governmental defendant. The practical effect of such a rule would be to permit the changing tide of information technology to preclude such litigants from obtaining Rule 34 discovery. Leaving open the possibility of a Rule 26 cost-shifting motion permits courts to shift costs when doing so is necessary in the interests of justice and efficiency. For example, a party requesting a hard copy of information already produced in electronic format could avoid the cost of that production if it satisfied the four-prong test articulated by the *Bills* court.[183] In any event, the proposed Rule amendment would place the burden of shifting costs for duplicate hard copies of electronic evidence squarely on the discovering party.

Finally, the proposed addition to the Rule recognizes the inherently proprietary nature of electronic documents by providing that respondents may presumptively obtain a protective order under Rule 26(c) that bars the release of electronic evidence (produced pursuant to Rule 34) to third parties other than the requesting party's expert witnesses. This addition prevents the disclosure of proprietary or confidential information that might result from producing discover-

[183] *See supra* Part III.B.2.

able material responsive to a Rule 34 document-request in electronic form.

The proposed Rule provides only a presumptive protective order for several reasons. The most obvious is to allow for a situation where the production of electronic evidence implicates no proprietary or confidential information, in which case the respondent cannot claim to be entitled to a protective order. The Rule, however, must also allow for situations where the requesting party or third parties (such as law enforcement entities or the press) present an overriding interest (be it their own or that of the public) in gaining access to the electronically-stored information produced under Rule 34.[184]

C. *The Rate of Technological Change Favors Prophylactic Rule Changes*

Currently there is a real question as to whether the existing Rules do an adequate job of managing discovery, whether electronic or not. Discovery of electronic files is not yet such a widespread and intractable problem as to raise an immediate and dire threat to the continued viability of Rule 34. We are convinced, however, that the proliferation of computer technology throughout the nation[185] weighs strongly in favor of not waiting until the Rules become ineffective before beginning the process of affecting their change. Every available indication shows the nation is witnessing a period of tremendous development in the use of computer technology that will have a widespread impact on how we as a society create, use, communicate and store information. As stated at the beginning of this Article, our fundamental premise is the prediction that within just a few years, many facets of life throughout the developed world will be inextricably linked to computers and the Internet. This development inevitably will result in a surge in the centrality of electronic evidence in federal civil litigation.

The lengthy deliberative process by which the Rules are changed ensures that no revision can take effect quickly. The contrast in the

---

[184] *See, e.g.*, Martindell v. IT&T Corp., 594 F.2d 291, 295–96 (2d Cir. 1979) (establishing standard to be applied to a non-party government intervenor's petition for modification of a protective order); Crothers v. Pilgrim Mortgage Corp., No. 95 Civ. 4681, 1997 WL 570583, at *2–4 (S.D.N.Y. Sept. 11, 1997) (discussing circumstances under which private non-party asserting its own interests may obtain the modification of a sealing order issued pursuant to a settlement agreement of which it had no notice); *In re* "Agent Orange" Prod. Liab. Litig., 104 F.R.D. 559, 568 (E.D.N.Y. 1985), *aff'd on different grounds*, 821 F.2d 139, 147 (2d Cir. 1987) (establishing standard applied to petitions by private parties who assert a public interest to obtain modification of protective orders).

[185] *See supra* notes 1–8 and accompanying text.

rate at which society is changing and the speed with which procedural rules can conform to that change raises the specter of a system of justice rendered obsolete by lack of forethought. Therefore, the suggestion that the Rules should not be amended until they are proven to be problematic ignores the risk that such an approach will result only in procedural changes that are outdated before they are printed.

D. *Case Law Will Not Produce Consistent Procedural Rules Regarding Electronic Discovery*

It is certainly true that the same changes to Rule 34 proposed above could be, in theory, accomplished through the development of case law. For example, courts could rationally interpret the term "document" to include all forms of electronic evidence and also could effectively "read in" the suggested addition to Rule 34(b). Thus, it may be argued that it is better to allow the common law process to adapt the Rules to changing technology.

But such an approach would necessarily involve courts in the resolution of discovery disputes, cutting against the grain of the Rules' general goal of promoting extrajudicial discovery practice. Another flaw in this *laissez-faire* approach is that it ignores the interlocutory nature of discovery disputes. As discussed above, few trial court decisions regarding the scope and logistics of discovery wend their way to the appellate level. As a result, allowing trial courts to address the deficiencies of electronic discovery under Rule 34 could generate conflicting rules within the same district, between districts of the same circuit and, of course, between the circuits themselves. The resulting patchwork of varying discovery "rules" across the country is unlikely to enhance the efficiency of electronic discovery practice—or to provide the desired guidance or certainty.

V. Issues for Future Debate and Deliberation

These proposals raise a multitude of questions and new concerns that are beyond the scope of this Article. The paragraphs that follow flag the most pressing issues that the legal community will need to confront in the near future.

A. *Disputes Concerning Formatting and Licensing Agreements*

Requiring the production of electronic evidence in the form in which it is stored may lead to formatting and translation problems. For example, a discoverable data file created by Party A with one

brand of word processing software may not be accessible to Party B that owns another brand. A possible solution would be for Party A to allow Party B to use its word processor to examine the discoverable data files. If this is not permitted by the licensing agreement Party A entered when purchasing its word processor software, however, the Rules certainly cannot require it. Party B is therefore left with a data file that it cannot use without purchasing Party A's word processing software (assuming it is for sale) or the burden of paying for the costs associated with a hard copy production.

Assuming licensing issues do not prevent Party A from providing Party B with the software necessary to make use of discoverable electronic evidence, the problems associated with the generally-proprietary nature of software remain. Such concerns may be only partially resolved by the proposed Rule's presumptive protective order provision. The overarching question of how to allow electronic discovery while simultaneously providing adequate protection to the intellectual property of litigants and third parties, such as software vendors, raises complex questions.

B. *Altering the Rules of Inadvertent Production of Privileged Material to Enhance Electronic Discovery*

Another major issue is the current jurisprudence concerning the inadvertent production of privileged material. As discussed above, existing case law holds that a producing party may waive her right to assert a privilege if a document is produced by mistake during discovery. In some cases, such a mistake may result in a waiver as to the entire subject matter of the produced communication. It would therefore come as no surprise if litigants choosing to produce discoverable evidence in electronic form would still voluntarily incur high costs to hire attorneys to carefully review each page of every responsive document to determine whether it is privileged.[186] The attorneys' fees for a large document review usually dwarf the costs arising from copying, shipping and storing those documents. Thus, the proposed amendment to Rule 34(b) regarding the manner in which electronic evidence is produced is unlikely to reduce system-wide discovery costs where the produced documents must be reviewed for privileged communications or work product.

---

[186] Even in the absence of privilege concerns, litigants may elect to have their attorneys scrutinize all produced material to ascertain the strategic value of the production to their adversary.

One suggestion would be to amend the Rule to allow a party producing discoverable information in electronic format to reserve its privilege objections until trial. This amendment would allow the respondent to avoid the high cost of reviewing the produced documents for privilege as well as the cost of copying, shipping and storing the hard copy of the produced documents—combined, these cost savings would be substantial. The procedure might merely delay the cost of reviewing discovered documents until just before trial. But because over ninety-nine percent of civil cases in federal court settle before trial, this procedure would effectively reduce the total cost of litigation.

While attractive in theory, altering the rules regarding inadvertent waiver of privilege would not be a simple project. For example, how could one prevent a party to whom privileged communications were inadvertently produced from using the knowledge of those communications to seek additional discovery or from sharing that information with third parties? How could such a limitation be enforced? This topic surely requires close scrutiny and much deliberation.

C. *Defining When Residual Data Is Within "The Possession, Custody or Control" of a Respondent*

The terms "possession, custody or control" in Rule 34(a) are difficult to apply to residual data. Because the location of the residual data has been deleted from the computer's directory, a residual data file cannot be identified and located without use of special computer programs designed for such purposes.[187] For this reason, deleting an electronic document cannot be analogized to shredding or otherwise destroying a paper document.

The resolution of this tricky issue is of far-ranging consequence. First, residual data represents a possible source of valuable information for litigants. For example, discovery of residual data might allow a party to find and use all prior drafts of a disputed document in order to show the contracting parties' intent. Second, the universe of residual data is potentially enormous. Including such information within the scope of Rule 34 dramatically increases the total amount of

---

[187] *See supra* Part I.C.1. (discussing and explaining residual data). Portions of a deleted file lingering on as residual data may be overwritten with other information, because by deleting the file's address from the storage device's directory the user signals the computer that it may re-use the space it once allotted for the deleted file.

available information. Third, because most litigants and their attorneys are unaware of the existence of residual data, they may fail to look for it when responding to Rule 34 requests. Fourth, requiring a respondent to search for residual data imposes a potentially significant discovery burden because it requires technical expertise beyond that of the average computer user. Finally, permitting the discovery of residual data, especially that of third parties, in today's computerized world raises important privacy issues by essentially preventing the effective deletion of *any* thought product created and stored electronically.

One approach would be to define the terms "possession, custody or control" to exclude information intentionally discarded prior to the anticipation of litigation. Like all bright line rule-making, such a solution has the appeal of clarity. Also, Rule 26(b)(3) already protects material "prepared in anticipation of litigation or for trial" from discovery. Courts could, therefore, apply cases construing Rule 26(b)(3) to define the limits of when residual data can be considered to be within the "possession, custody or control" of a respondent.

Conclusion

This Article's proposed revisions to Rule 34 permit courts to distinguish effectively between paper and electronic evidence, and thus allow for the development of decisional law addressing the special properties of the continuously-evolving information technology. The revisions would also clarify that all forms of electronic evidence are within the scope of Rule 34(a) and specify the method in which electronic evidence must be produced thereby reducing the need for judicial involvement. In addition, the proposed rule would create incentives for federal litigants to use the most efficient means possible to locate, duplicate, transmit and store discoverable electronic evidence.

The proposed modifications to Rule 34 may be less important than the questions they implicate. But given the centrality of discovery in modern civil litigation, the specter of immense confusion and costs generated by a surge in electronic discovery, as well as the relationship between the rules of discovery and some, if not all, areas of substantive law,[188] the time is right for the legal community to focus on the new media and how their nationwide use requires systemic

[188] *See, e.g.*, Marcus, *Discovery Containment Redux*, *supra* note 165, at 749–51 (discussing question of whether broad discovery rules have put pressure on areas of substantive law).

amendments to the existing Rules. If this Article serves to incite debate and deliberation on how the Rules should best be brought into the twenty-first century, we have achieved our goal.