Discoverability of "Deleted" E-Mail: Time For a Closer Examination

*Michael Marron**

I. INTRODUCTION

In the past ten years, electronic mail (e-mail) has significantly altered how we communicate with each other in the industrialized world.[1] Attracted by its relatively low cost, speed, and ease of use, individuals and businesses have turned to e-mail to replace or supplement traditional communication tools such as the written letter or the telephone.[2] As a result, legislatures and courts have been forced to examine whether existing legal structures are sufficiently flexible to resolve issues that are either not present in other communications tools or present but to a different degree.[3]

---

* J.D., 2002, Seattle University School of Law; LL.B. (1994) and B.A. (1992) National University of Ireland, Galway. I would like to express my thanks to my Law Review colleagues for their invaluable contributions to this Comment and to my parents Carole and Eamon Marron for decades of patience and support. I would also like to thank my wife, Kristin, and daughter, Sorcha, for their love and encouragement. This Comment is dedicated to my grandparents, Thomas and Eithne Egan.

1. A Senate report for the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.* (Supp. 1999)), defines e-mail as "a form of communication by which private correspondence is transmitted over public and private telephone lines. In its most common form, messages are typed into a computer terminal, and then transmitted over telephone lines." S. REP. NO. 99-541, at 8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3562. This description, although capturing the essential qualities of e-mail communication, is itself somewhat outdated in light of the technologies available in the year 2002. In addition to telephone lines, e-mail is now transmitted via cable and wireless satellite systems.

2. *See* Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327 (2000) ("E-mail and the Internet have begun to replace the telephone as the way people conduct daily personal and business communications."); Timothy Coughlan, Comment, *Applying the U.S. Postal Service Statutes to E-Mail Transmissions*, 25 RUTGERS COMPUTER & TECH. L.J. 375 (1999) (noting that by 1998 the number of e-mails transmitted far outnumbered the number of pieces of ordinary mail, so-called "snail mail," delivered by the United States Postal Service).

3. *See* Richard L. Marcus, *Confronting The Future: Coping with Discovery of Electronic Material*, 64 LAW & CONTEMP. PROBS. 253, 259 (2000) (noting the difficulty in separating advances in society that require changes to the existing legal structure, such as the introduction of

Because e-mail rapidly became a means of transporting large amounts of information, it was not surprising that privacy was one of the first issues to be raised. The legal community was faced with difficult questions such as whether employers should be allowed to monitor employee e-mails[4] and how to deal with the possibility that e-mails could be intercepted without authorization.[5] Other novel legal issues are related to e-mail's unique characteristics. For example, mass marketers were attracted to e-mail because they could transmit thousands of unsolicited messages (or "spam") with very little effort and very little cost. To counteract mass marketer's abuse of e-mail's efficiencies, many states quickly enacted anti-spam laws that placed restrictions on unsolicited e-mail messages.[6]

The e-mail revolution also had a profound effect in the area of civil discovery. As e-mail use became more commonplace, litigators quickly recognized the wealth of potential evidence that could be found in an opponent's e-mail archives. Many litigators were also pleased or shocked (depending on whether they were the requestor or requestee) to learn that it was also possible to recover e-mail messages that had apparently been discarded through the delete function found in all e-mail programs. In fact, it quickly became apparent that it is very difficult for a person to simply discard an unwanted or improper e-mail message. As a result of this technical quirk, many millions of new e-mail messages are created every day, and despite their author's best efforts to delete them, it remains technically possible to locate and produce these messages during pre-trial discovery.

The legal question of whether these "deleted"[7] messages should be produced is governed by the Federal Rules of Civil Procedure. The current Federal Rules apply the same criteria to the discovery of e-mails that have been applied to paper-based discovery for decades.

---

the motorcar, from developments, such as the use of the horse for transportation, that do not require a drastic change in the existing legal rules).

4. *See, e.g.*, Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that employees harbor no reasonable expectation of privacy concerning their use of workplace computers despite the employer's assurances that employee e-mails would remain privileged). *But see Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987 and H.R. 4908 Before the House Subcomm. on the Const. of the Comm. on the Judiciary*, 106th Cong. (2000) (documenting a failed attempt to require that employers give notice to employees before monitoring their e-mail correspondence).

5. *See* 18 U.S.C §§ 2511, 2701 (2000) (making it a federal crime to intercept or disclose e-mails during either transmission or storage).

6. *See* David E. Sorkin, *Spam Laws*, *available at* http://www.spamlaws.com/state/index.html (visited May 23, 2002) (listing anti-spam laws from 22 different states).

7. Throughout this Comment, "deleted" e-mails refer to those e-mails where both the sender and recipient have taken steps to destroy the correspondence. Technically, of course, these e-mails are not deleted and may still be recovered.

As a result, during the discovery phase of litigation, it has become increasingly common for a party to request that the opposing party recover and produce large numbers, often hundreds of thousands, of deleted e-mail messages through use of special "forensic" computer techniques.

This Comment will argue that the current discovery rules allow for the over-disclosure of deleted e-mail messages when considering public policy concerns such as communications efficiency, individual privacy, and free speech. However, before this argument can be made, it is necessary to define what should be the proper scope of civil discovery: how much production of information is too much? In a recent article discussing modern discovery reform, Professor Jeffrey Stempel offered a succinct and workable test for analyzing whether a suggested restriction on the scope of discovery is justified.[8] According to Professor Stempel, any arguments for restricting or, for that matter, expanding discovery should be made with reference to the central inquiry of whether "disclosure and discovery [are] providing the information to which litigants are rightfully entitled without requiring the production of an unacceptable amount of information that is too extraneous, disproportionately expensive to produce, private or privileged, or otherwise deserving of protection on public policy grounds."[9] Professor Stempel's formula suggests that the appropriate level of discovery can be found by balancing the litigants' right to access to information against a number of other concerns including cost, privacy, and other public policies.

In the case of deleted e-mails, this Comment will argue that the discovery rules presently require disclosure of an unacceptable amount of information. In particular, public policy concerns such as communication efficiency, individual privacy, and free speech should outweigh the rights of a litigant to access deleted e-mail correspondence without some showing of particular relevance or need. Perhaps the easiest way to expose the public policy issues involved in the production of deleted e-mails is to analogize it to a more familiar context such as discarded paper-based correspondence. As applied to deleted e-mails, the current rules are the equivalent of requiring a litigant to first dig through their garbage for huge amounts of shredded and discarded paper correspondence and then expend considerable resources to repair the letters and documents found. These documents are then

8. Jeffrey W. Stempel, *Ulysses Tied to the Generic Whipping Post: The Continuing Odyssey of Discovery "Reform"*, 64 LAW & CONTEMP. PROBS. 197, 221 (2001).

9. *Id.* at 221.

handed over to a litigation opponent and may appear as evidence in a civil case.

Although this analogy is useful to expose some of the potential issues, to fully comprehend the nuances involved with discovery of deleted e-mails, it is first necessary to understand the unique nature of e-mail. For this reason, Part II of this Comment will outline some of e-mail's advantages over other communications media to help explain the rapid rise in e-mail use. Part III will then explain, in layman's terms, how e-mail actually works and discuss some of the reasons why e-mail archives are often considered as likely to contain "smoking gun"[10] messages—the kind of evidence that can drastically affect the outcome of a case.[11] But what is it about e-mail that can make it such a potent evidentiary weapon? The answer lies in the combination of three factors discussed in more detail later in this Comment. First, a vast number of e-mails can be stored at a relatively low cost. Second, contrary to popular belief, an e-mail is extremely difficult to delete and often lingers in a later discoverable form. Finally, e-mail users tend to adopt a casual tone, using e-mail more like the telephone than a letter.

Due to this unique combination of factors, it is likely that the widespread discovery of e-mails is here to stay and will play an increasingly important role in litigation. What remains uncertain is whether the existing discovery rules are sufficiently flexible to incorporate such a significant change. To provide a background for answering this question, Part IV will discuss the existing discovery rules, the fundamental principles on which the rules are based, the existing limitations on the permissible range of discovery, and the extent to which the existing rules allow for extensive discovery of "deleted" e-mails. After examining the existing framework, Part V will assess the current rules' impact on e-mail usage, focusing on the fact that there is

---

10. "Smoking gun" is a term of art used by the litigation community to describe a document that constitutes strong evidence in favor of the claim being made. For an illustration of a "smoking gun" e-mail, *see generally* Siemens Solar Indus. v. Atlantic Richfield Co., No. 93 CIV. 1126, 1994 WL 86368 (S.D.N.Y. Mar. 16, 1994). Siemens filed a lawsuit against Atlantic Richfield (ARCO) claiming, among other things, securities fraud. *Id.* at *1. Siemens alleged that it had relied on representations that ARCO had developed commercially viable photovoltaic products that were of value to Siemens. *Id.* During discovery Siemens located an internal ARCO e-mail, which included the statement: "[A]s it appears that [the technology] is a pipe dream, let Siemens have the pipe." Leslie Helm, *The Digital Smoking Gun: Mismanaged E-Mail Poses Serious Risks, Experts Warn*, L.A. TIMES, June 16, 1994, at D1. This *Los Angeles Times* article offers the following example of "smoking gun" e-mails used in litigation: "Dear David, Please destroy the evidence," to which the recipient replied, "Acknowledging your request. Evidence destroyed. Aloha, David." *Id.*

11. *See* Marnie H. Pulver, Note, *Electronic Media Discovery: The Economic Benefit of Pay-Per-View*, 21 CARDOZO L. REV. 1379, 1380 (2000) (describing e-mail and other forms of electronic data as the "darling of discovery").

already evidence to suggest that the current framework has had a chilling effect on the type of information communicated.

In Part VI, this Comment will argue that the application of the current rules has failed to take into account important public policy considerations. The discussion will center on two policy concerns. First, the current rules might have a profound, negative effect on the efficiency of communication in our modern, wired world. Second, the rules neglect the privacy concerns of individuals who are subject to discovery of their deleted e-mails, causing negative effects on the individuals in deciding what information they should include in their e-mail correspondence. Given these concerns, a question is raised as to whether the mere fact that e-mails may be restored and recovered long after their deletion should automatically require them to be accessible in litigation. Perhaps technological ability should not necessarily set the standards of the law.[12] This Comment will propose a solution in Part VII—deleted e-mails should be presumptively undiscoverable unless a requesting party can make a particular showing of relevance.

If, as this Comment will argue, the current discovery rules may seriously inhibit the use of e-mail to communicate, it is important to understand what may be lost. For this reason, it will be useful to briefly analyze the general benefits that e-mail has to offer.

II. SOCIETAL BENEFITS OF E-MAIL

If e-mail is indeed, as it has been described, a revolutionary communications tool, regulations having a detrimental effect on its use should be carefully considered. Once an attempt has been made to describe and quantify the general societal benefits of e-mail, the question of whether the current rules of civil discovery have had, or are likely to have, a chilling effect on its everyday use can then be examined. Using Professor Stempel's test for whether a restriction on discovery is justified, the negative effects on communications efficiency, privacy, and speech can be weighed against the primary reason for allowing a requestor access to information: facilitation of the search for the truth of the matter in dispute.[13]

---

12. *See* Laurence H. Tribe, *The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*, THE HUMANIST, Sept.–Oct. 1991, at 15–16 ("New technologies should lead us to look more closely at just what values the constitution seeks to preserve.").

13. Other commentators have utilized a similar initial analysis when discussing proposed regulatory changes where privacy interests are at issue. For example, in the context of proposed regulation of internet-based businesses using personal information, one commentator has recommended that "[t]he first step in analyzing the trade-offs involved in enacting new regulations is identifying the benefits of new technologies or ways of doing business in order to weight them in the balance with the benefits of privacy and the costs of regulation." Kent Walker, *Where*

E-mail benefits may be divided into two separate, although related, categories: efficiency and social benefits. Efficiency benefits concern the potential savings in time and resources that e-mail offers compared to the other available methods of information transfer such as the telephone and postal mail.[14] Social benefits, on the other hand, involve the ability to enhance the feeling of community in our society. Obviously, the more efficient the communications method, the more likely people are to use it, and the more effective it will be for building and maintaining relationships.

A. Efficiency of E-Mail as a Means of Communication

E-mail is "arguably the most efficient means of communication yet devised by humans, with the possible exception of gestures."[15] Whether this statement is accurate or is a reflection of the hysteria that is often associated with new technologies, it nevertheless raises an intriguing question: What is it about e-mail that could inspire such a strong claim?

Compared to traditional instruments of communication, e-mail offers many significant advantages. An e-mail message may be thought out, written, and sent in less than a minute. Once sent, it can reach its destination, however distant, in a matter of seconds. Letters, on the other hand, take considerably longer to write because they require a more formal structure and subsequently take days rather than seconds to reach their destination. Although the telephone has the advantage of extremely fast transmission, it also requires that both parties be available to communicate simultaneously, a significant barrier to long distance conversations, where time differences can be substantial. E-mail is asynchronous, it requires only that one party be available at a particular time for the communication to take place; aggravating games of "phone tag" are avoided, and information moves more efficiently.

E-mail also allows the user to send large caches of data to a large number of recipients with little or no added time or effort. The sender avoids the costs of copying, printing, and delivering a large number of identical messages in hardcopy format. Moreover, e-mail not only

---

Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange, 2000 STAN. TECH. L. REV. 2, ¶ 186 (2000).

14. *See* Janet Mann & Melanie Freely, *LAN-Based E-mail Takes Off*, DATAMATION, Nov. 15, 1990, at 105.

15. Amy M. Fulmer Stevenson, Comment, *Making a Wrong Turn on the Information Superhighway: Electronic Mail, The Attorney-Client Privilege and Inadvertent Disclosure*, 26 CAP. U. L. REV. 347, 349 (1997) (citing Martin E. Hellman, *Implications of Encryption Policy on the National Information Infrastructure*, 11 NO. 2 COMPUTER L. WKLY. 28 (1994)).

eases the transportation of information, but it also provides both parties with a cheap and easy storage method.[16] Furthermore, e-mail is relatively cheap. Once the initial costs of the hardware are paid, the per-communication cost of e-mail is virtually zero.[17] In comparison, sending a letter costs at least as much as a stamp, and the cost increases with the size of the document. A telephone call may be free locally but quite expensive over longer distances. Sending a message by fax costs approximately one hundred times more than the equivalent e-mail.

In theory, therefore, e-mail represents an extremely efficient and inexpensive way to communicate. In practice, this potential is borne out by statistics showing that e-mail use is increasing dramatically and that U.S. businesses are quickly embracing e-mail for their day-to-day operations.[18]

B. E-Mail's Community-Building Role

E-mail may revolutionize communication in the same way that the telephone did at the start of the twentieth century. In the early 1900s, the telephone was partly responsible for an expansion in the scope of the possible communities because it broke down geographical boundaries that had previously hindered effective communications. After the telephone became more commonplace in households, relationships could be maintained over long distances with relative ease.[19]

---

16. E-mail is different from telephone communication, where fallible human memory is the only easily available recording method or written correspondence that requires someone to physically place a letter in a file. *See* Jerry Kang, *Cyber-Race*, 113 HARV. L. REV. 1130, 1154 (2000); Murphy Oil USA, Inc. v. Fluor Daniel, Inc., No. Civ. A. 99-3564, 2002 WL 246439 (E.D. La. Feb. 19, 2002) ("With electronic media . . . the costs of storage are virtually nil.").

17. Looking to cut costs in light of a downturn in automobile sales, executives at General Motors issued a directive to all employees that states that e-mail should be used instead of long distance telephone calls whenever possible. Keith Naughton, *Motown Slowdown*, NEWSWEEK, Nov. 27, 2000, at 60.

18. For example, at Microsoft Corporation, e-mail has replaced the telephone as the most frequently used instrument of communication. *See* Steve Lohr, *Antitrust Case Is Highlighting Role of E-Mail*, N.Y. TIMES, Nov. 2, 1998, at C1; *see also* Betty Ann Olmstead, *Electronic Media: Management and Litigation Issues When "Delete" Doesn't Mean Delete*, 63 DEF. COUNS. J. 523, 525 (1996) ("It is the versatility and simplicity of e-mail and voicemail that account for their phenomenal growth as a communication media of choice in the business world."); Timothy Q. Delaney, *E-Mail Discovery: The Duties, Danger and Expense*, 46 FED. LAW. 42, 43 (1999) ("In the last few years, corporate America has wholeheartedly embraced e-mail. At many corporations, e-mail has become the preferred form of communication.").

19. For a more complete description of the effects of the invention of the telephone on society, see generally IRWIN LEBOW, INFORMATION HIGHWAYS AND BYWAYS: FROM THE TELEGRAPH TO THE 21ST CENTURY (1995); DAN LACY, FROM GRUNTS TO GIGABYTES: COMMUNICATIONS AND SOCIETY (1996).

E-mail is a further advance in this revolution because it allows for cheaper, faster, and easier communication.[20]

In our increasingly industrial, high density, and urbanized society, communities tend to be more difficult to maintain, and individuals can feel increasingly isolated.[21] In addition to facilitating online communication, e-mail may also promote communication beyond the Internet. What starts as e-mail messaging can spill over into offline interaction such as visiting relatives in other cities or meeting old college friends.[22] Although inherently difficult to quantify, e-mail benefits society insofar as it allows for increased interaction among individuals. The extent to which the current discovery rules interfere with these benefits should at least be considered in determining the proper scope of discovery.

It would be premature, however, to discuss reform of the discovery rules before describing e-mail discovery practice as it exists today. E-mail discovery has been the focus of a great deal of attention because of e-mail's unique technological infrastructure and unusual human usage patterns.

III. E-MAIL AND ITS USE IN DISCOVERY PRACTICE

Increased use of e-mail for business and personal purposes has resulted in a corresponding rise in the frequency of production requests for e-mails in the discovery phase of litigation.[23] The rush to delve into an adversary's e-mail archives has been further fueled by a torrent of scholarly articles and newspaper stories expounding on the potential bounty to be found.[24] Perhaps, the most effective advertisement for increased discovery of e-mails has come in the form of media reports documenting the use of e-mail in an amazing diversity of high

---

20. *See* Charles Bermant, *The E-Mail Phenomenon: It's Showing Signs of Growing Up and Is Starting to Have (Gulp) Rules*, SEATTLE TIMES, June 13, 1999, at C1 (describing e-mail as a "further wrinkle" in the revolution that started with the telephone).

21. *See* Walker, *supra* note 13, ¶ 52 ("[T]he sense of community is in increasingly short supply in contemporary society.") (citing ROBERT N. BELLAH ET AL., HABITS OF THE HEART: INDIVIDUALISM AND COMMITMENT IN AMERICAN LIFE (1985); ROBERT D. PUTNAM, BOWLING ALONE: THE COLLAPSE AND REVIVAL OF AMERICAN COMMUNITY (2000)).

22. *See id.* (giving the example of getting back in touch with an old school or college friend).

23. The use of e-mail as evidence has become particularly common in employment discrimination, sexual harassment, and anti trust cases. For a detailed account of the rise in use of e-mail in litigation, *see* Samuel A. Thumma & Darrel S. Jackson, *The History of Electronic Mail in Litigation*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 1 (1999).

24. *See, e.g.*, Amy Harmon, *Corporate Delete Keys Busy as E-Mail Turns up in Court*, N.Y. TIMES, Nov. 11, 1998, at C1; Doug Bedell, *Erased and Found: Click on 'Delete' and Email Vanishes, But Don't Assume It's Gone for Good*, NEWARK STAR LEDGER, July 19, 1999, at 61.

profile cases such as the Iran-Contra affair,[25] the bribery scandal surrounding Salt Lake City's bid for the 2002 Winter Olympic games,[26] the Microsoft antitrust case,[27] the impeachment of President William Clinton,[28] and more recently the widespread reports of key e-mail correspondence that are expected to play a major role in the inevitable litigation arising out of the collapse of the Enron Corporation.[29] In recent years, a mini industry has sprung up to render technical assistance to attorneys regarding electronic discovery.[30] The leaders in this relatively new field, sometimes referred to as computer forensics, are also doing an effective job of increasing the profile of electronic discovery.[31]

---

25. During the Iran-Contra investigation, Oliver North and John Poindexter communicated via e-mail. Although they had deleted their e-mail messages, the messages were eventually retrieved from a backup tape and used as evidence in the investigation. *See* Geanne Rosenberg, *Electronic Discovery Proves an Effective Legal Weapon*, N.Y. TIMES, Mar. 31, 1997, at D5.

26. *See* Pulver, *supra* note 11, at 1412 (discussing a newspaper article that described how the ethics panel investigating alleged improprieties in the Salt Lake City's bid for the 2002 Winter Olympics based its conclusions, in part, on an e-mail written by a high ranking U.S. Olympic official stating that "[a] lot of promises were made to secure votes").

27. United States v. Microsoft Corp., 147 F.3d 935 (D.C. Cir. 1998). The *Microsoft* case was perhaps the most noteworthy example of high profile use of e-mail in litigation. Despite Microsoft CEO Bill Gates' denials of discussions of a cooperative agreement between Microsoft executives and Netscape officials, e-mail from one Microsoft executive summarized the meeting with Netscape stating that Microsoft needs to "understand if you [Netscape] will adopt our platform and build on top of it or if you are going to compete with us on the platform level." James V. Grimaldi, *The Gates Deposition: 684 Pages of Conflict*, SEATTLE TIMES, Mar. 16, 1999, at A1.

28. In February 2000, a *Washington Times* article revealed that the White House had not produced up to 100,000 e-mail messages sought through several subpoenas by investigators looking into "Filegate," "Chinagate," the Monica Lewinsky affair, and other matters. *See Legacy of Lawlessness*, WASH. TIMES, Feb. 18, 2000, at A20. These e-mails were allegedly inadvertently misplaced. *See* George Lardner, Jr., *E-Mail Probe Was Expected; White House Recovery Plan Awaited Inquiries From Hill*, WASH. POST, May 2, 2000, at A21. The White House was expected to produce the misplaced e-mails within six months. *See* Don Van Natta, Jr., *Former Counsel Takes Responsibility for Missing E-mails*, N.Y. TIMES NEWS SERV., May 5, 2000. The price tag on the White House's restoration of the missing e-mails from backup tapes is $3 million. *Id.*

29. *See* Julia Brunts, *For Litigators, Discovery Now Often Focusing on Data Files*, DAILY LAW BULLETIN, Jan. 18, 2002 (quoting an electronic litigation specialist, who stated on the likelihood that e-mail will play a role in future litigation, "What did [the Enron] CEO know and when is not going to be in any document, but it is going to be in his e-mail, and somebody's going to find it.").

30. The following is a non-exclusive list of companies specializing in the area of electronic discovery: Computer Forensics Inc., *see* information available at http://www.forensics.com/; Computer Discovery Labs, Inc., *see* information available at http://www.computerdiscoverylabs.com/; Data Discovery, Inc., *see* information available at http://www.teleport.com/~peterc/; Rehman Technology Services, Inc., *see* information available at http://www.surveil.com/index/html; and Applied Discovery, Inc., *see* information available at http://www.applieddiscovery.com/default.htm.

31. One such specialist, Joan Feldman of Computer Forensics Inc., based in Seattle, Washington, has contributed a number of articles. *See* Joan E. Feldman & Rodger I. Kohn, *The Essentials of Computer Discovery*, 564 PLI/PAT 51 (1999) [hereinafter Feldman & Kohn, *Essentials*];

But media exposure alone cannot explain why e-mail is now so widely accepted as a key component of effective discovery. A more complete explanation requires an examination of how e-mail works and how people are using it.

A. E-Mail's Technological Infrastructure

Although e-mail has become a very important component of the contemporary communications landscape, it is not perfect. One imperfection—the fact that it is very difficult to successfully delete an e-mail message—is at the root of the problem that this Comment addresses. Other characteristics, such as the ease with which large numbers of e-mails can be stored at very little cost, are potentially beneficial but nevertheless magnify the deletion problem in the litigation discovery context because they ensure that deleted e-mails remain available for discovery for longer periods of time. Because e-mail's technological infrastructure is at the root of both the communication benefits previously discussed and the increased use of e-mail in discovery to be described later, it is necessary to explain the basic technical elements that constitute e-mail.

The general public has become quite familiar with the look and feel of the various software programs that serves as the public face of e-mail. For many, however, this is the limit of their technical knowledge. These e-mail programs vary in visual appearance and complexity, but almost all allow the user to compose new messages and attach other electronic files, sort incoming messages using a number of different criteria, store incoming messages in individual files, delete messages, reply to messages without having to input target address, and search the mailbox using particular keywords.[32] Whatever the functions offered, the main role of these programs is to provide the user with an easy-to-use interface with the technological infrastructure representing the e-mail network.

The core concept of e-mail communication is that each mailbox has a unique identifier. In the same way that a letter requires a particular address, an e-mail can only reach its intended destination if the address is constructed correctly. In an attempt to make e-mail user-friendly, e-mail pioneers decided to use a form of identifier that would be familiar; thus, an e-mail address is similar to an address used for a

---

Joan Feldman & Rodger I. Kohn, *Collecting Computer Based Evidence*, N.Y. L.J., Jan. 26, 1998, at S5; Joan E. Feldman, *Electronic Risk Control: Effectively Managing Computer Files*, 42 PRAC. LAW. 41 (1996).

32. *See* LEE SPROULL & SARA KIELSER, CONNECTIONS: NEW WAYS OF WORKING IN THE NETWORKED ORGANIZATION (1991).

letter: an identifying name, followed by an "at" sign (@), followed by the name of the network where the particular mailbox is located.

Once an e-mail has been composed and addressed correctly, it can be sent to the desired recipient over two types of networks: a local area network (or LAN as it is commonly referred) or a wide area network (WAN). A local area network, as its name suggests, consists of a single computer or group of computers that are directly connected, usually in a single building or group of buildings.[33] When a person sends a message to another person within the group, the message is copied and posted to the target mailbox. A wide area network, on the other hand, involves the use of external networks, or the Internet. A message is sent either over a single network of related computers or between networks of related computer to the recipient computer.

A common computer language, or protocol,[34] allows e-mail messages to easily pass through the "gateways" between different networks. A protocol converts the e-mail message into a common "language" understood by all networks using that protocol. Typically, an e-mail message will pass through a number of computers as it closes in on the recipient computer before it is finally copied to the recipient mailbox. During the early days of e-mail networks, users were often restricted to communicating within a small network directly connected to them, but as technology developed, it became more commonplace for both local and wide-area systems to operate together, allowing access to all parties with e-mail addresses, regardless of the type of system on which they operate.[35]

B. The Role of E-Mail in Modern Discovery Practice

Recent commentary on the role of e-mail in modern discovery practice suggests that a request for production of e-mails may represent either a gold mine or a minefield, depending on whether you are the requestor or requestee.[36] Almost uniformly, contemporary commentators focus on three idiosyncratic characteristics of e-mail when attempting to explain why e-mail archives are likely to contain valu-

33. A Local Area Network (LAN) is a computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. *Id.* at 68.

34. A protocol is a set of rules that defines a format by which devices may transfer data to each other. TCP/IP, or Transmission Control Protocol/Internet Protocol, is the de facto standard used to connect local area networks to the Internet. *Id* at 233.

35. *Id.* at 50.

36. *See generally* James A. Snyder & Angela Morelock, *Electronic Data Discovery: Litigation Gold Mine or Nightmare?*, 58 J. MO. B. 18 (2002); James H.A. Pooley & David A. Shaw, *Finding out What's There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57, 59 (1995) (noting that electronically stored evidence could be considered a "potential gold mine" or "genuine mine field" depending on which party has control of the information).

able evidence: (1) e-mail users generally produce a large quantity of messages, thereby increasing the chance that one will contain evidence regarding a matter in dispute; (2) the content of e-mail messages tends to be less formal and more likely to contain sentiments unavailable from other sources; and (3) an e-mail is extremely difficult to permanently destroy.[37]

Millions of new e-mails are created everyday and the sheer volume of messages created tends to increase the likelihood that at least some may be relevant to future legal claims or defenses. In one sense, therefore, the importance of e-mail discovery is a product of simple mathematics. For example, a company with one hundred employees creating an average of fourteen e-mail messages per day will produce a total of roughly 100,000 messages per week.[38] When you consider that larger companies may have a workforces numbering in the thousands or hundreds of thousands, the numbers of messages produced increases exponentially. One electronic discovery professional recently calculated that a real-world company with a workforce of 100,000 was creating 22 million new e-mail messages per week – a figure that shocked the company's CEO.[39] But the number of sent e-mail messages represents only a part of the overall e-mails that may be accessible during discovery. The average U.S. worker with an e-mail account also receives roughly thirty messages per day.[40] These incoming messages are also potentially discoverable during discovery.

The large number of messages created might not be particularly significant in the litigation context if the content of these messages was essentially benign. There is reason to believe, however, that e-mail messages tend to contain information that a user might not reveal in other, more formal, modes of communication.

E-mail messages frequently contain the type of communication most beloved of litigators—spontaneous, open, candid, and sometimes even salacious.[41] Based on the anecdotal evidence, the tone of e-mail

---

37. *See, e.g.*, Marcus, *supra* note 3, at 181; Thumma & Jackson, *supra* note 23, at 1–4.

38. An average of fourteen sent e-mail messages per day is probably a conservative figure. There is evidence to suggest that the e-mail users may actually send considerable more. *See, e.g.*, Jon G. Auerbach, *Getting the Message*, WALL ST. J., June 16, 1997, at R22 (citing an estimate that by 2005, the average user will send 29.4 e-mail messages per day).

39. John Jessen, *Special Issues Involving Electronic Discovery*, 9 KAN. J. L. & PUB. POL'Y 425, 428 (2000).

40. Stephanie Armour, *E-Mail Delivers Legal, Privacy Issues*, USA TODAY, Nov. 12, 1998, at 3B.

41. Essentially, this is the type of communication that might have earlier taken place in whispers over cup of coffee or a meal. *See* Wendy J. Rose, *The Revolution of Electronic Mail*, THE LEGAL INTELLIGENCER, Jan. 21, 1997, at 7–14 ("Descriptions of e-mail communication styles include freewheeling, candid, unfiltered, not modulated, raw and off the cuff. . . . [T]hese very attributes, which lend themselves to easy, casual and seemingly efficient communications

correspondence appears to have evolved into a hybrid of oral and written communications. Struggling to describe this unorthodox message content, one writer stated that it is "like a phone call, only written. It's like a paperless letter, but faster. It's like a casual conversation, or a postcard, or a scribbled note to a classmate in the middle of class. It's all of the above, and . . . none of them."[42] Perhaps, this casual style is due to the lack of formal conventions and punctuation that tend to subdue spontaneous expression when one composes a letter. Also, it is possible that e-mail users may tend to be more open in their correspondence because they are under the mistaken impression that they can simply delete a message that might later seem to be inappropriate or an inaccurate portrayal of their true thoughts.

Whatever the causes might be, the result is that e-mails tend to contain information that is unlikely to be found in a letter or in other documents. If the delete button on e-mail computer programs performed the function its name suggests, it seems likely that many of these candid, conversation-like e-mails would be quickly discarded by both author and recipient and placed beyond the reach of even the most technologically proficient discovery expert. Reality, however, is not that simple.

Contrary to what most people believe, it is extremely difficult for the average, technologically unsophisticated, e-mail user to render an unwanted e-mail message unrecoverable. Encouraged by the common meaning of the word "delete," e-mail users cannot be faulted for thinking that a message is permanently destroyed when it is highlighted and the "delete" function is used.[43] In reality, the delete function does not immediately make a message irretrievable. Instead, the computer merely marks the message as available to be overwritten by newer information. The length of time that passes before a message is actually deleted from a hard drive depends almost entirely on two factors: the size of the storage space available on the computer (generally the more space available, the longer a message will remain retrievable) and the degree to which new data is inputted (the more new data input, the quicker the message is likely to be overwritten). Thus, if a computer has a large memory capacity and is used infrequently, a "de-

---

have stung many companies and individuals whose transmissions have returned to haunt them.").

42. Jacques Leslie, *Mail Bonding: E-Mail is Creating a New Oral Culture*, WIRED, Mar. 1994, at 42.

43. *See* Andrew Johnson-Laird, *Smoking Guns and Spinning Disks*, COMPUTER LAW, Aug. 1994, at 1 (noting the general public belief that computers can delete unwanted files); William Decoste, *Sender Beware, The Discoverability and Admissibility of E-Mail*, 2 VAND. J. ENT. L. & PRAC. 79, 81 (2000).

leted" e-mail message may remain available for a significant period of time.[44] Of course, these lingering, not overwritten, e-mails would still not be available for discovery if it were not for one final twist: modern software programs can access and recover documents that have not been completely overwritten. Because of its obstinate refusal to die, this not-quite-deleted information is commonly referred to as "shadow" or "ghost" data[45] and, when properly authenticated, it may be introduced as evidence in litigation.[46]

In the context of e-mail messages, therefore, delete does not mean delete. Indeed, U.S. District Court Judge James Rosenbaum has gone so far as to state that the inability to destroy electronic files may be the computer's ultimate flaw because the "inability to forget weakens and undermines the very ideas it permanently holds."[47] In the context of pre-trial discovery, this apparent weakness is exacerbated by the fact that this undeleted information may potentially be stored in multiple locations.

In addition to potentially recoverable deleted messages not fully overwritten, e-mails may be recovered from two other sources: (1) e-mails that have not been deleted, or "active" data, may be recovered from the hard drives of the computers where they are stored; and (2) e-mails that have been deleted and overwritten may still be available on backup tapes that are routinely used to avoid widespread loss of data in the case of system failure or other emergency situations.[48]

1. Active Data

In the simplest terms, active data is information that is currently being used. In the case of e-mail, the active data will consist of all e-mail in a user's inbox, any copies of sent e-mails that have not been deleted (unless the user has indicated that sent e-mails should not be saved), and any e-mails that have been saved to a file. Previously, e-mail messages remained active until the user decided to delete them, but more recently, often in reaction to the expanding use of e-mail in

---

44. *See* Johnson-Laird, *supra* note 43, at 8–9, 13.

45. *See* Matthew Goldstein, *Electronic Mail, Computer Messages Present Knotty Issues of Discovery*, N.Y. L.J., Feb. 8, 1994, at 1 ("Like ghosts from the past . . . forgotten electronic blips can come back to haunt a litigant, since computer data bases are subject to a civil discovery request.").

46. For a discussion of some of the obstacles to be overcome before an e-mail may be introduced as evidence, *see* Decoste, *supra* note 43, at 85–89 (2000); Christine Sgarlata Chung & David J. Byer, *The Electronic Paper Trail: Evidentiary Obstacles to the Discovery and Admission of Electronic Evidence*, 4 B. U. J. SCI. & TECH. L. 5, 35–42 (1998).

47. James M. Rosenbaum, *In Defense of the Delete Key*, 3 GREEN BAG 2d 393, 396 (2000), *available at* http://www.greenbag.org/rosenbaum_deletekey.pdf.

48. *See* Feldman & Kohn, *Essentials*, *supra* note 31, at 54.

litigation, companies have instigated procedures whereby all active e-mail messages are automatically deleted at regular intervals.[49] The producing party can recover active e-mails simply by opening the files and printing out the messages. However, as computer hardware technology advances, the number of locations in which active data is stored is likely to increase. In the last ten years for example, it has become increasingly common for active data to be stored on employee laptop as well as desktop computers.[50]

2. Backup Data

The vast majority of organizations utilizing computer technology wisely take the precaution of copying electronic files and storing them in a safe location as a form of disaster protection.[51] At regular intervals, a "snapshot" is taken of the entire computer system; the data is then transferred to portable media that are stored for a period of time that can range from a few days to many years.[52] Any e-mails existing on the system at the time of the snapshot will be stored and can be retrieved in future litigation for as long as the tape is kept.

By now it should be apparent that an e-mail user who wishes to truly delete an e-mail needs either a lot of technical assistance or luck. The situation that results is one where large numbers of candid e-mails are created, are not completely deleted, and remain available during discovery. With this in mind, it is not surprising that competent attorneys are likely to pursue e-mail discovery to the maximum extent allowed by the rules of civil procedure and the court's interpretations of those rules.[53]

IV. RULES OF CIVIL PROCEDURE: DISCOVERY OF E-MAIL

The Federal Rules of Civil Procedure reflect the basic philosophy that free access to relevant information is necessary to determine

---

49. For most systems, a received message is automatically saved, usually to the inbox. Unix systems, however, require a user to save a message, the default being deletion. *See* Ian C. Ballon, *How Companies Can Reduce the Costs and Risks of Associated with Electronic Discovery*, COMPUTER LAWYER, July 1998, at 10.

50. *See, e.g.*, Superior Consultant Co. v. Bailey, No. 00-CV-73439, 2000 WL 1279161, at *13 (E.D. Mich. Aug. 22, 2000) (ordering defendant corporation to produce a backup file of employee's laptop computer).

51. *See, e.g.*, McPeek v. Ashcroft, 202 F.R.D. 31, 32 (D.D.C. 2001) ("The purpose of having a backup system and retaining the tapes was to permit recovery from disaster.").

52. *Id.*; *see also* Linnen v. A.H. Robbins Co. Inc., No. 97-2307, 1999 WL 462015, at *1 (Mass. Super. Ct. June 16, 1999) (defendants keeping backup tapes for three months before recycling).

53. *See* Thumma & Jackson, *supra* note 23, at 33 (predicting that a rise in e-mail use in litigation will be restrained only by the creative vision of attorneys and the receptiveness of the courts).

the truth.[54] When originally enacted in 1938, the Rules introduced the then-revolutionary concept of expansive discovery during the pretrial stage of litigation.[55] Ten years later, the Supreme Court wholeheartedly embraced the policy of full disclosure, agreeing that "[m]utual knowledge of all the relevant facts is essential to proper litigation."[56] By the late 1970's, however, there was a growing perception that the discovery rules were being abused. These concerns went all the way to the Supreme Court where Justice White, acknowledging the growing disquiet, was moved to note that "there have been repeated expressions of concern about undue and uncontrolled discovery, and voices from this Court have joined the chorus."[57] Thus, the pendulum had begun to swing back towards restricting, rather than expanding, discovery: a trend that would continue in the following decades.

In 1983, the Rules were amended to introduce, among other changes, the concept of proportionality.[58] For the first time, judges were given the discretion to limit discovery when, in their opinion, the burden or cost of complying with a request for discovery outweighed the potential importance of the information in light of the importance of the issues in the case and the parties' ability to absorb the costs of production. This amendment clearly announced that there should be limits to the amount of discovery allowed even if potentially relevant information is thereby excluded. The trend continued in 1993, when the Rules were again amended to set presumptive limits on the number of interrogatories and depositions allowed for each party.[59] Despite this slight shift towards more limited discovery, the current rules still reflect the original framer's philosophy of broad access to relevant

---

54. *See, e.g.*, Tiedman v. American Pigment Corp. 253 F.2d 803, 808 (4th Cir. 1958) ("[D]iscovery is founded upon the policy that the search for the truth should be aided.").

55. *See* Stempel, *supra* note 8, at 202.

56. Hickman v. Taylor, 329 U.S. 495, 507 (1947).

57. Herbert v. Lando, 441 U.S. 153, 157 (1979).

58. The 1983 amendment added the following language to Rule 26(b)(1):

> The frequency or extent of use of the discovery methods set forth in subdivision (a) 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 discovery is unduly burdensome or expensive, taking into account the needs of the case, the amount in controversy, limitations on the parties' resources, and the importance of the issues at stake in the litigation. The court may act upon its own initiative after reasonable notice of a motion under subdivision (c).

6 JAMES WM. MOORE ET AL., MOORE'S FEDERAL PRACTICE ¶ 26.07[1] (3d ed. 1997) (reprinting 1983 amendment to Rule 26(b)(1), now Rule 26(b)(2)).

59. *See* FED. R. CIV. P. 26(b)(2). These presumptive limits can be increased if the court is satisfied that the added discovery would satisfy the proportionality test of Rule 26(b)(2).

information. In the context of e-mail discovery, two rules generally define the universe of information that may be requested: Rule 26 outlines the general rule of broad discovery and then gives certain exceptions to the general rule, including the proportionality principle, while Rule 34 describes the types of documentary evidence that may be requested.

A. Framework for Discovery of Documents: Rules 26 and 34

Rule 26, the core provision of the rules of discovery, clearly reflects a policy of allowing expansive disclosure. Adopting extremely broad language, the rule states:

> *In general.* 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 to the claim or defense of any party . . . . It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.[60]

In addition to the broad wording of Rule 26, the Supreme Court has further emphasized the expansive nature of the universe of information that can be discovered by stating that the courts should interpret the rules "broadly and liberally" in order to promote the policy of full disclosure.[61] When considering the appropriate boundaries of discovery, the courts have generally followed the Supreme Court's instruction and ensured that access to relevant information is as broad as the rules can possibly allow.[62] As noted above, however, the extent of disclosure may also be limited by Rule 26(b)(2), which grants a judge the discretion to limit full disclosure when the burden on the producing party would outweigh the benefits to the truth finding function of the court.

Pursuant to the general scope of discovery outlined in Rule 26(b), Rule 34 defines the categories of documents or tangible evidence that a party may request.[63] Prior to 1970, Rule 34 made no mention of electronically stored evidence. The modern era of electronic discovery was launched in 1970, when the Advisory Commit-

60. *Id.*

61. *Hickman*, 329 U.S. at 506.

62. *See* Cox v. E.I. DuPont de Nemours & Co., 38 F.R.D. 396, 398 (D.S.C. 1965) ("[I]n the search for the ultimate, TRUTH, the Federal Courts, blessed with the rules of discovery, are not shackled with strict interpretations of relevancy.").

63. FED. R. CIV. P. 34(c).

tee, reacting to the increasing use of computers,[64] revised the description of a "document" in Rule 34 to include "data compilations from which information can be obtained, [and] translated, if necessary, by the respondent."[65] To further clarify its intentions, the Advisory Committee included a comment stating that "electronic data compilations" were now to be included in the category of documents that were subject to discovery under the rule.[66] Subsequent judicial interpretation of the change has left no doubt as to whether electronic evidence is now discoverable. By 1985, a judge could comfortably declare that "it is black letter law that computerized data is discoverable if relevant."[67] Consequently, any relevant electronic documents, including active or deleted e-mails, are discoverable unless a recognized limitation applies.

B. Limitations on Discovery

Although the present discovery rules envision broad access to relevant information, they also recognize that there should be limits to how far discovery should reach. For example, privileged matters protected by the attorney-client privilege and the work-product doctrine are expressly excluded from the scope of discovery.[68] Additionally, the 1983 amendments to the Rules introduced the flexible proportionality limitation that allows judicial intervention when the "burden or expense of the proposed discovery outweighs its likely benefit."[69]

---

64. 8A CHARLES A. WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE: CIVIL § 2218 (2d ed. 1994).

65. The accompanying note states:

> The inclusive description of "documents" is revised to accord with changing technology. It makes clear that Rule 34 applies to electronics 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 his devices to translate the data into usable form.

FED. R. CIV. P. 34 advisory committee's note (1970). In addition to allowing discovery of electronic materials, the rule requires that the party in possession of the electronic information cooperate with the requesting party to make the information readable. Some courts have interpreted this to require the producing party to develop software programs to extract the electronic information and to educate the receiving party in how to review the data. *See* Nat'l Union Elec. Corp. v. Masushita Elec. Indus. Co., 494 F. Supp. 1257 (E.D. Pa. 1980).

66. FED. R. CIV. P. 34 advisory committee's note.

67. Anti-Monopoly, Inc. v. Hasbro, Inc., No. 94CIV. 2120 LMM AJP, 1995 WL 649934, at *2 (S.D.N.Y. Nov. 3, 1995); *see also* Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985) ("It is now axiomatic that electronically stored information is discoverable under Rule 34 of the Federal Rules of Civil procedure if it otherwise meets the relevancy standard prescribed by the rules.").

68. *See* FED. R. CIV. P. 26(b)(1) ("[P]arties may obtain discovery regarding any matter, not privileged."); FED. R. CIV. P. 26(b), (d) (codifying the work-product doctrine originally).

69. FED. R. CIV. P. 26(b)(2).

1. Privileges

Electronic data is subject to the same traditional privileges that apply to paper-based discovery. The significance of a privilege is that it allows a party to resist discovery of an otherwise discoverable document.[70] The traditional justification for privileges focuses on the fact that there are specific relationships, such as the husband-wife or lawyer-client relationships, that society should protect. Privileges reflect an implicit assumption that the benefit of protecting specific relationships is greater than the potentially negative effects of such protection on the truth-finding function of the judicial process.[71]

An alternative, although related, justification for privileges concentrates on actual communication and the effect that a privilege will have on individual privacy.[72] Thus, communications between the lawyer and client, in which the client seeks legal advice, are protected to allow for more open communication.[73] For purposes of this Comment, however, it is sufficient to note that the judicial system recognizes that the negative external effects, be they to society at large or to the individual, have been, and should be, taken into account in deciding the outer limits of litigation discovery.[74] Indeed, Rule 26(c) explicitly empowers judges to perform a similar balancing test.

2. Unduly Burdensome or Expensive: Proportionality Limitation Under Rule 26(c)

Where a court finds that the burden or expense of production is disproportionate to the value of the information to the particular case, the amount at stake, the parties' resources, and the importance of the

---

70. BLACK'S LAW DICTIONARY 831 (6th ed. 1991) ("That which releases one from the performance of a duty or obligation, or exempts one from liability which he would otherwise be required to perform, or sustain in common with all other persons."); FED. R. CIV. P. 26(b)(1) ("[P]arties may obtain discovery regarding any matter, not privileged.").

71. *See Developments in the Law—Privileged Communications: II. Modes of analysis: The Theories Justifications of Privileged Communications*, 98 HARV. L. REV. 1471, 1472 (1985).

72. *Id.* at 1484.

73. 8 J. WIGMORE, WIGMORE ON EVIDENCE § 2290, at 542 (McNaughton ed., rev. vol. 1961) (describing the attorney-client privilege as "the oldest of privileges for confidential communications.").

74. An excellent example of the judicial limitation on discovery based on negative external effects is the self-analysis privilege. The rationale behind this privilege is that an organization that conducts an internal, critical analysis of its own conduct should not be required to produce that analysis in later or related litigation unless the party seeking discovery can demonstrate substantial need, because discovery of such materials would have a chilling effect upon the company's motivation to self-analyze and improve its flaws and would therefore be against the public's interest. *See generally* John Louis Kellogg, *What's Good for the Goose . . . Differential Treatment of the Deliberative Process and Self-Critical Analysis Privileges*, 52 WASH. U. J. URB. & CONTEMP. L. 255 (1997); *see also* Flynn v. Goldman, Sachs & Co., 91CIV. 0035 KMW, 1993 WL 362380, at *1 (S.D.N.Y. Sept. 16, 1993).

issues raised in the case, the court may limit production of certain documents or shift the cost of production to the requesting party.[75] This proportionality principle is particularly relevant to the present discussion because it is the most commonly invoked legal mechanism to restrict the production of deleted e-mails.[76]

Production of "deleted" e-mails is generally more costly than that of active data. Deleted e-mails may be recovered either from the hard drive of a computer or from emergency backup tapes. But in either case, the recovery process is relatively expensive. The process of restoring deleted, but not overwritten, e-mails from a hard drive will usually require the assistance of a computer specialist because specialized computer programs are required to locate and recover deleted e-mails.[77] On the other hand, if the deleted e-mails is to be recovered from emergency backup tapes (so-called "ghost" data), the producing party will typically have to engage in a costly multi-stage process. [78] First, the available backup tapes must be searched to identify the tapes containing the mailbox files of the person whose e-mails are requested. Then the producing party must catalog the available backup tapes to locate those likely to contain responsive e-mails. This can prove difficult and costly because backup tapes are not organized in an easily searchable format: the purpose of having the tapes is not to archive documents for later retrieval, but rather to allow recovery in the case of disaster.[79] Having located the tapes containing potentially respon-

---

75. FED. R. CIV. P. 26(b)(1); *see also* FED. R. CIV. P. 34 advisory committee's note (1970), which states:

> [T]he courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay the costs. Similarly, if the discovering party needs to check the electronic source itself, the court may protect the respondent with respect to preservation of his records, confidentiality of non-discoverable matters and costs.

The normal presumption under the discovery rules is that the responding party must bear the expense of compliance. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 358 (1978).

76. *See* Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. Jan. 16, 2002) (the defendants seeking order to prevent discovery of e-mail correspondence due to excessive burden and expense involved); McPeek v. Ashcroft, 202 F.R.D. 31 (D.D.C. 2001) (Department of Justice claiming that the cost to restore e-mails from backup tapes was excessive); Playboy Enterprises, Inc. v. Welles, 60 F. Supp. 2d 1050 (S.D. Cal. 1999) (the defendant claiming that allowing discovery of "deleted" e-mails from her hard drive would cause undue burden because it would require shutting down her business for a time); Murphy Oil USA v. Fluor Daniel, Inc., No. CIV.A. 99-3564, 2002 WL246439 (E.D. La., Feb. 19, 2002) (the defendant claiming that expense and burden of restoring ninety-three e-mail backup tapes outweighed the likely benefits).

77. *See, e.g., Playboy Enterprises*, 60 F. Supp. 2d at 1052 (appointing the court's own electronic discovery specialist to perform the task of creating a "mirror image" of the defendant's hard drive).

78. *See Rowe*, 205 F.R.D. at 426–27 (describing the multi-stage process).

79. *See McPeek*, 202 F.R.D. at 33.

sive data, the producing party must then restore these tapes, save them to a master database, and remove any duplicate e-mails. If the producing party wishes to redact portions of e-mails in order to protect sensitive or privileged information, the party must also convert the files into a Tagged Image File Format (TIFF file). Finally, the producing party may wish to review all the files for privileged information before they are handed over to the requesting party. Due to the huge quantity of e-mails that may be produced in some cases, this privilege review can significantly add to the cost of production.[80]

Faced with the expense of restoring and producing deleted e-mails, many litigants request that the court either curtail the scope of a request for deleted e-mails or shift the cost to the requesting party. In theory, the difficulty and cost of producing "deleted" e-mails should limit the overall amount produced. If the courts are already limiting access to "deleted" e-mails or taking the privacy interests of the e-mail authors into account when applying the proportionality principle, the need for a modification of the discovery rules to protect privacy will be reduced.[81] It is therefore worthwhile to analyze how the courts have applied Rule 26(c)'s proportionality test in the context of electronic discovery in general and deleted e-mails in particular.[82]

a. Early Attempts to Shift the Cost of Producing E-mail

The courts got off to a bumpy start when attempting to apply the proportionality principle to discovery of deleted e-mails. In one of the first cases to address the issue, *In re Brand Name Prescription Drugs Antitrust Litigation*,[83] the U.S. District Court of Illinois denied a request to shift the cost of producing e-mails from backup tapes, because the court felt that the extra expense was a result of the producing

80. *See Rowe*, 205 F.R.D. at 426–27 (one of the four defendant companies estimating that it would cost approximately $247,000 to have a paralegal review responsive e-mails for privilege). Alternatively, a defendant could choose to perform privilege review by conducting a computer search of all responsive files. The danger with this review form is that it will not locate all privileged documents. For example, some attorney-client correspondence may not include the term "confidential" or "privileged" and therefore avoid detection.

81. It should be noted that many discovery disputes are resolved informally. Before hearing a discovery dispute, a court will require that the moving party at least attempt informal resolution. *See* FED. R. CIV. P. 26(c); FED. R. CIV. P. 37(a)(2)(A), (B); FED. R. CIV. P. 37(d). Also, anecdotal evidence suggests that some litigants have applied their own limitations on e-mail discovery by agreeing not to request each other's e-mails to avoid the huge costs involved. Kate Marquess, *In Re: Technology Discovery Grab Bag*, 36 ARK. LAW. 38, 39 (2001).

82. For a more comprehensive analysis of cost-shifting in the realm of electronic discovery, see Corinne L. Giacobbe, Note, *Allocating Discovery Costs in the Computer Age: Deciding Who Should Bear the Costs of Discovery of Electronically Stored Data*, 57 WASH. & LEE L. REV. 257 (2000).

83. C.A. No. 94C897, MDL No. 997, 1995 WL 360526 (N.D. Ill. June 15, 1995).

party's choice of technology, and therefore held that the producing party should bear these added costs.[84] In *Brand Name Prescription*, the class plaintiffs had requested production of a large number of e-mails from a defendant drug manufacturer. Estimating that it would cost between $50,000 and $70,000 to search, compile, and format responsive e-mails from backup tapes that contained roughly 30 million separate messages, the drug company sought an order shifting the costs to the plaintiffs. The court stated that a number of factors should be considered in addition to the cost of production. These factors included the benefit to be gained by production of the e-mails and the respective parties' ability to bear the cost of production and to reduce the costs of production.[85]

Having listed these additional factors, the court then essentially ignored them and focused on the drug manufacturer's decision to utilize a backup software system. The court stated that "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."[86] The court's reasoning has been criticized as displaying a fundamental ignorance of the reality of computer use in modern business.[87] The court seems to punish the defendant drug company for "choosing" to use an electronic storage system, and in doing so appears ignorant of the fact that by 1995 computers were such an invaluable tool that they were essentially replacing paper files in most businesses.[88] Furthermore, for many businesses, there was no realistic alternative to electronic storage because many documents existed only in electronic format and the cost of printing hardcopies would be prohibitive. The court does not appear to understand that the primary purpose of backup tapes is "to permit recovery from disaster, not archival preservation."[89] If it had really understood this important point, the court would undoubtedly have understood why it is unrealistic to require companies to maintain backup tapes containing a "snapshot" of the entire computer system in easily recoverable or searchable format.

---

84. *Id.* at *2.

85. *Id.* (citing Bills v. Kennecott Corp., 108 F.R.D. 459 (D. Utah 1985)).

86. *Id.*

87. *See* Pulver, *supra* note 11, at 1422 (criticizing the court for not recognizing that it is inevitable that businesses will use digital networks); *see also* Giacobbe, *supra* note 82, at 280–81 (stating that the court did not realize the extent to which computers have become a part of modern business).

88. *See* Bills v. Kennecott Corp., 108 F.R.D. 459, 462 (D. Utah 1985) ("Computers have become so commonplace that most court battles now involve discovery of some computer-stored information.").

89. McPeek v. Ashcroft, 202 F.R.D. 31, 31 (D.D.C. 2001).

The judicial confusion continued in *Linnen v. A.H. Robbins Co.*,[90] where the court again refused to shift the cost of producing deleted e-mails because the cost of producing e-mails from backup tapes was part of the risk inherent in choosing to use computer technology.[91] The plaintiff in *Linnen* was faced with a request to restore deleted e-mails from backup tapes at an estimated cost of up to $1.75 million.[92] The defendant had already produced a large number of active e-mails recovered from the employees' hard drives. Refusing to grant the plaintiff relief from the cost of production, the court repeated the *Brand Name* court's analysis:

> While [this] court certainly recognizes the significant cost associated with restoring and producing responsive communications from these tapes, it agrees . . . that this is one of the risks taken on by companies which have made the decision to avail themselves of the computer technology now available to the business world. To permit a corporation such as [the defendant] to reap the business benefits of such technology and simultaneously use that technology as a shield in litigation would lead to incongruous and unfair results.[93]

Like the *Brand Name* court, the *Linnen* court viewed use of computer technology as a matter of choice rather than a business necessity. The *Linnen* court's statement is even more surprising, however, because it was delivered in 1999, and by that time, even moderately computer savvy members of the general public were aware that the efficiency advantages of computers had made their use in many businesses virtually mandatory. Additionally (as later courts eventually recognized), requesting parties are likely to request as many backup e-mails as possible if there is a presumption that a party using computers should pay the costs of producing electronic data. Thus, the legal rules initially seemed to encourage litigants to seek maximum production of deleted e-mails.

b. The Emerging Test for Cost-Shifting

Perhaps in response to the widespread criticism of the *Brand Name* court's view of computer usage, or perhaps simply because judges have had more time to develop an understanding of computer technology, recent cases addressing the issue of proportional production of deleted e-mails have shown a more subtle analysis. In the first

90. No. 97-2307, 1999 WL 462015 (Mass. Super. Ct. June 16, 1999).
91. *Id.* at *6.
92. *Id.*
93. *Id.*

case to display this new attitude, *McPeek v. Ashcroft*,[94] an ex-employee of the Department of Justice (DOJ) sued the DOJ, claiming that he was retaliated against for having accused his supervisor of sexual harassment.[95] Although the DOJ had already searched its active e-mail files for responsive messages, the plaintiff further requested that the Department should be forced to search its backup computer tapes for e-mails from the computer of the plaintiff's former supervisor and others. In response, the DOJ claimed that the likelihood of locating relevant evidence on the tapes could not justify the great expense of restoration.[96]

The U.S. District Court of District of Columbia first acknowledged that the primary purpose of the backup system was not for preservation for later business use, but rather as an insurance against catastrophic failure of the computer systems.[97] Then, in a direct response to the *Brand Name* court's presumption that the cost of restoration was simply a cost of doing business, the court noted that it was almost impossible to walk into any business or government agency without encountering a computer system.[98] In light of this reality, the court asked, "What alternative [to using a computer] is there? Quill pens?"[99]

Preferring a conservative course of action, the court then ordered the DOJ to perform a "test run" restoration of the plaintiff's ex-supervisor's e-mails for a one-year period. The DOJ was also ordered to certify the cost of this test run, and the parties were to be given the opportunity to later argue that further discovery was justified.[100] In the wake of *McPeek*, it seemed that the courts might not automatically assume that the producing party should bear the cost of restoring e-mails simply because it chose to use computers to back up its files. Six months later, in *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*,[101] the U.S. District Court of New York affirmed this view.

The *Rowe* plaintiff was a black concert promoter, who had accused the defendant booking agencies and concert promoters of attempting to freeze them out of the market for promoting concerts for white bands.[102] The plaintiff made thirty-five requests for documents including any e-mail communications relating to the selection of con-

94. 202 F.R.D. 31 (D.D.C. 2001).
95. *Id.* at 31–32.
96. *Id.* at 32.
97. *Id.*
98. *Id.*
99. *Id.* at 33.
100. *Id.* at 35.
101. 205 F.R.D. 421 (S.D.N.Y. 2002).
102. *Id.* at 423.

cert promoters.[103] Four of the defendants objected to the requests and sought a court order either limiting the production of e-mails or requiring the plaintiff to bear the costs of production.[104] The four defendants produced estimates ranging from $84,000 to $403,000 for compliance with the request, not including the cost of reviewing the e-mail messages for privileged information.[105]

Analyzing whether the costs of production should be shifted to the plaintiff, the district court first rejected the plaintiff's reliance on the *Brand Name* presumption that production costs were cost of using computers that should remain with the defendants. The court observed that the basic premise of the plaintiff's argument was flawed because it was based on the premise that e-mail messages are retained because they are useful and if a party is willing to pay the cost of retention, it should hence pay the cost of production.[106] Electronic data, however, was different; it could be retained simply because the cost of doing so is minimal or for the limited purpose of recovery in the case of disaster. The court thus soundly rejected the *Brand Name* court's reasoning and concluded that "it is not enough to say that because a party retained electronic information, it should necessarily bear the cost of producing it."[107]

Having rejected the *Brand Name* presumption, the court turned to a multi-factor analysis to determine whether the cost of producing e-mails should be shifted to the plaintiff. The relevant factors included (1) the specificity of the request, (2) the likelihood of finding relevant information, (3) the availability of such information from other sources, (4) the purposes for which the data was retained, (5) the possibility that the responding party might benefit from the production, (6) the total cost of production, (7) the relative ability of the parties to control costs and the incentives to do so, and (8) the resources of each party.[108] The court then analyzed the facts of the case and found that five of the factors favored a finding that the costs should be shifted, two favored a finding to the contrary, and one factor (the parties' resources) was neutral.[109] Thus, the court ordered the plaintiff to bear the cost of production.[110]

103. *Id.* at 424.
104. *Id.* at 424–26.
105. *Id.*
106. *Id.* at 429.
107. *Id.*
108. *Id.*
109. *Id.* at 429–32.
110. *Id.* at 433.

One month later, the U.S. District Court of Louisiana adopted the same multi-factor test to decide whether the costs of producing e-mails from backup tapes and again held that the cost should be shifted to the requesting party.[111] This new approach is likely to result in a shift of the cost of producing electronic evidence more often than under the *Brand Name* analysis. It is not completely clear, however, precisely what effect the new test will have on requests for deleted e-mails.

It appears that many of the factors listed by the *Rowe* court will usually favor shifting the cost of production where the requesting party seeks access to deleted e-mails. For example, the fourth factor listed in *Rowe*—the purposes for which the data is retained—will almost always favor cost shifting in such a situation because deleted e-mails are generally located on backup tapes and hard drives. As the *McPeek*, *Rowe*, and *Fluor* courts noted, backup tapes are not kept to ensure that the information can be accessed for regular business purposes, but to insure against a disaster that wipes out a company's electronically stored data. Likewise, deleted e-mail messages that remain on hard drives because they have not been overwritten are not intentionally kept for further use but remain solely due to a quirk in the technology.

The sixth *Rowe* factor—the total cost of production—will favor cost shifting when deleted e-mail messages are targeted because the restoration process is complicated, expensive, and time consuming. The *Rowe* court suggested that, based on precedent, costs as little as $1,680 could be considered sufficiently substantial to warrant cost shifting.[112] It is difficult to imagine that any request for production of deleted e-mails from backup tapes or hard drives would cost less than this amount, and in many of the reported cases, the costs can run into tens of thousands or possibly even millions of dollars.[113] The seventh factor—the parties' relative ability and incentive to control costs—will tend to favor cost shifting in most cases because, as the *Rowe* court stated, the requesting party controls how expansive discovery will be, and therefore "[t]hey are in the best position to decide whether further searches would be justified."[114]

On the other hand, at least one of the *Rowe* factors may favor the producing party retaining the burden of paying for discovery of de-

111. Murphy Oil USA, Inc. v. Fluor Daniel, No. Civ. A. 99-3564, 2002 WL 246439 (E.D. La. Feb. 19, 2002).

112. *Rowe*, 205 F.R.D. at 431.

113. *See, e.g.*, *Fluor*, 2002 WL 246439, at *6 (noting that the cost of producing e-mails in that case was $6,000,000).

114. *Rowe*, 205 F.R.D. at 432.

leted e-mails. This is because deleted e-mails, by their nature, are generally not available from other sources.

The picture emerging from these recent cases is that the courts are increasingly likely to shift the cost of producing deleted e-mails to a requesting party. However, it is worth noting that the number of e-mails produced is nevertheless likely to remain steady so long as the requesting party believes that the cost of production is worthwhile given the possible rewards. In this regard, the fact that e-mails are considered likely to contain "smoking gun" evidence will tend to encourage parties to request deleted e-mail documents even if they must pay to do so. In fact, in each of the cases where the cost of production was shifted to the requesting party, production of large quantities of e-mails proceeded nonetheless.

c. Attempts to Assert Privacy Concerns

In their attempts to limit the scope of discovery of e-mails under Rule 26(c), parties have claimed that the detrimental effect on their privacy also constitutes a "burden" that should be considered.

Although no court has actually precluded the production of deleted e-mails on privacy grounds, at least one court was willing to take privacy considerations into account when establishing the procedure by which e-mails were to be recovered. In *Playboy Enterprises Inc. v. Welles*,[115] the publisher of Playboy sued a former "Playmate of the Year," claiming that the use of its Playboy and Playmate trademarks on her personal website infringed its trademarks.[116] During the discovery phase of trial, the plaintiff became aware that the defendant had deleted e-mail messages on the personal computer that she used for both business and personal correspondence. Consequently, the plaintiff requested that they should be allowed to access the defendant's computer in order to restore any deleted e-mails that had not already been overwritten.[117] In response, the defendant claimed that the four-to-eight-hour shutdown needed to recover the deleted e-mails would cause her to suffer financial losses, would result in production of privileged attorney-client confidences, and would seriously infringe her privacy.[118]

The court held that the plaintiff should be allowed access to the computer, but in order to protect the defendant's privacy and attorney-client privilege, the court placed conditions upon the recovery

115. 60 F. Supp. 2d 1050 (S.D. Cal. 1999).
116. *Id.* at 1051.
117. *Id.* at 1052.
118. *Id.* at 1054.

process.[119] First, the plaintiff was required to produce statements from experts to the effect that there was a likelihood that the e-mails could be recovered, as well as the likelihood of damage to the defendant's computer system.[120] Furthermore, once a copy of the hard drive was made, it should be given to the defendant who could then withhold any unresponsive e-mails.[121] At first glance, this decision seems to indicate that courts may be willing to take procedural steps to protect the privacy interests of producing parties. However, the facts of the *Playboy* case are somewhat unusual in that the producing party was self-employed. In the more common setting where employers are asked to produce the e-mail messages of its employees, the courts have not been as sensitive to the privacy concerns of the individual authors.

For example, in the *Rowe* case, the defendant business attempted to assert the privacy concerns of its employees in addition to its request to shift the costs of production. In *Rowe*, as is likely the case in most businesses, the defendant's archived e-mail files contained the employee's personal as well as business communications. The court, however, refused to take into account the privacy concerns of the employees whose messages were to be produced because "an employee who uses his or her employer's computer for personal communications assumes some risk that they will be accessed by the employer or by others."[122]

Thus, it seems that any consideration of the e-mail author's privacy concerns, which may be allowed when the author himself is the producing party, simply disappears when it is his employer that produces the messages. The court's reasoning demonstrates that the privacy concerns of e-mail authors in the context of discovery are only one aspect of the overall picture. It will be of little comfort to employees that their deleted e-mails will not be produced during discovery if, as is currently the case, their employer can monitor their messages without notification.[123]

The *Rowe* court also suggested that the defendant in that case could have cured any privacy concerns of its employees by simply removing any personal correspondences before production. Again, this is not likely to provide any realistic protection for employees. It is unlikely that a business will go to the added expense of reviewing all e-mails and excluding any personal messages. Even if an employer took

119. *Id.*
120. *Id.*
121. *Id.*
122. *Rowe*, 205 F.R.D. at 428.
123. *See, e.g.*, Smyth v. Pillsbury, 914 F. Supp. 97 (E.D. Pa. 1996).

these steps, the process of reading and removing employee's e-mails is likely to be an intrusion in and of itself.

The preceding discussion of the application of the existing limits on discovery suggests that deleted e-mails will continue to be produced in large quantities and that employee's privacy concerns will not be taken into account. Before discussing whether privacy and other concerns should be considered in this context, it will be useful to consider the impact, if any, that the rules have had on e-mail usage.

V. HOW THE PRESENT DISCOVERY RULES AFFECT E-MAIL USAGE

Anecdotal evidence suggests that the present discovery rules are changing the way we use e-mail. Commentators have increasingly recommended extreme caution to companies in the use of e-mail, often citing broad discovery of e-mails and the inability to control the destruction of e-mails as key factors.[124] Companies are being advised to set up e-mail retention policies that retain only the absolute minimum amount of electronic evidence for the absolute minimum time.[125] Many commentators recommend companies not to allow e-mail to be used for personal purposes, others place restrictions on the type of communications that e-mail may be used for, and some warn that "if you wouldn't want the message published in a newspaper, don't write it in an e-mail"[126] or encourage employers to "tell employees that if they are in doubt about whether to send an e-mail, they should ask themselves: 'How would I feel if this ended up in the hands of my worst enemy?'"[127] Businesses are encouraged to inform employees not to use humor or sarcasm[128] and to adopt document "retention" policies

124. *See* Carey S. Meyer & Kari L. Wraspir, *E-Discovery: Preparing Clients For (and Protecting Them Against) Discovery in the Electronic Age*, 26 WM. MITCHELL L. REV. 939 (2000); Henry S. Knight, Jr. et al., *Technology Issues in the Workplace*, 47 FEDERAL LAWYER, Oct. 2000, at 34; Grover J. Brittain, *Drafting an E-Mail and Internet Usage Policy for Your Firm*, 27 COLORADO LAWYER, Oct. 1998, at 17.

125. *See* Ballon *supra* note 49 ("[B]ackup tapes should regularly be overwritten so that at any given moment a company only has records of e-mail for the preceding week or two."); Meyer & Wraspir, *supra* note 124, at 959 ("[A]s part of their routine practice, companies should consider using computer programs that electronically remove deleted messages so that hey can no longer be retrieved.").

126. Meyer & Wraspir, *supra* note 124, at 957.

127. Brittain, *supra* note 124.

128. Knight, Jr. et al., *supra* note 124 ("[N]o employee should create an e-mail referring to age in a joking, sarcastic, or pejorative manner."); Sheila J. Carpenter & Shaunda A. Patterson, *Discovery of Electronic Documents*, *in* BRIEF, 29 A.B.A. TORT & INSURANCE PRACTICE SECTION 1, 64, 69 (2000) (recommending that employers should discourage employees from using humor and sarcasm in e-mail messages).

that employ special software to permanently delete e-mails as soon as they are read.[129]

At least on a corporate level, it seems likely that e-mail use will become increasingly limited to strictly innocuous information. Even where no official policy is in place, individuals who are aware of the indestructibility of e-mail communications are likely to resort to more traditional modes of communication, leaving e-mail to operate in a diminished capacity of transporting strictly sterile business information.

VI. PUBLIC POLICY AND PRIVACY ARGUMENTS IN FAVOR OF LIMITED PRODUCTION OF "DELETED" E-MAIL

In the realm of discovery practice, the Advisory Committee brought the Federal Rules of Civil Procedure into the modern computer age in 1970 by simply adding the words "data compilations" to the list of document types that could be produced. Because the first e-mail was not sent until one year after the committee made this change, the committee could not have contemplated the ramifications this addition would have for a society, which thirty years later, produces 500 billion e-mail messages annually.[130] These facts alone suggest, at the very least, that re-evaluation of the Rules is warranted. Indeed, the Advisory Committee on Civil Rules of the Judicial Conference has noted that "electronic storage and retrieval of information are changing the opportunities for discovery and the dangers of excessive discovery."[131]

The purpose of this Comment is to question whether the difficulty that e-mail users face in deleting their e-mail messages might also lead to excessive discovery. The question, therefore, is whether the benefits gained by complete disclosure of "deleted" e-mails justify the burdens placed on recognized societal interests. Discovery should be curtailed if the revelation of a category of information will result in a net detriment to recognized public concerns such as efficiency, pri-

129. Charles A. Lovell & Roger W. Holmes, *The Dangers of E-Mail: The Need for Electronic Data Retention Policies*, 44 R.I. B.J. 7, 9 (1995) ("In most cases, e-mail should be destroyed immediately after the recipient reads the message.").

130. Peter Lyman & Hal R. Varian, *How Much Information?*, *available at* http://www.sims.berkeley.edu/how-much-info/internet/emaildetails.html (showing a study produced by the faculty and students at the School of Information Management and Systems, University of California (Berkeley)) (original release Oct. 18, 2000) (last visited May 25, 2002).

131. Alfred W. Cortese Jr. & Edward C. Wolfe, *Electronic Discovery: Problems and Solutions*, *in* METROPOLITAN CORPORATE COUNSEL, Apr. 2000 (citing a Memorandum from Hon. Paul V. Niemeyer, Chair, Advisory Committee on Civil Rules, to Chief Justice, Re: Comment on Letters on Disclosure and Discovery Proposals, Sept. 1, 1999, at 3).

vacy, and free speech.[132] This is in line with commonly accepted rationales for the traditional privileges such as attorney-client privilege and work product, which reflect the recognized societal concern of allowing access to certain materials in the judicial system. What follows are discussions of some of the public policy concerns that are interrelated in many ways and that up until now have not received serious consideration in the context of the discovery of deleted e-mails.

A. Efficiency Costs

Under the present discovery rules, an e-mail user cannot easily prevent a discarded e-mail message from being produced in discovery and subsequently used at trial. On a corporate level, the threat of large-scale mining of the stored e-mail files has become a significant source of concern for commercial entities, particularly for those that rely heavily on e-mail for both internal and external communications and are regularly involved in litigation.[133] For both individuals and corporations, e-mail offers efficiency advantages unavailable in any other widely used form of communication. However, the ability to avail one's self of e-mail's unique efficiencies is likely to be restricted to the extent that e-mail has the potential to become a source of legal liability in future lawsuits.[134] A presumption that deleted e-mails are undiscoverable would greatly relieve, although not eliminate, some of the concerns faced by individuals and companies alike.

In the business setting, individuals are being discouraged from using e-mail and encouraged to use traditional forms of private communications, like the telephone, for correspondence that might subject the business to future legal liability. For example, it is likely that e-mail usage among the top-level management of many of the country's largest companies has changed considerably following the dramatic fashion in which Bill Gates of Microsoft was forced to defend potentially harmful e-mail messages that were sent internally. This is not to say that these corporate managers are not entertaining many of the same thoughts as before—undoubtedly, antitrust, sexual harassment, or discrimination issues will continue to exist—although it is likely

132. A similar analysis is used in those cases that have suggested that there should be a self-analysis privilege. *See* Flynn v. Goldman, Sachs & Co., 91CIV. 0035 KMW, 1993 WL 362380, at *1 (S.D.N.Y Sept. 16 1993).

133. *See* Scott Dean, *E-Mail Forces Companies to Grapple With Privacy Issues*, CORP. LEGAL TIMES, Sept. 1993, at 11; Marianne Lavelle, *Digital Information Boom Worries Corporate Counsel*, NAT'L L.J., May 30, 1994, at B.

134. *See* Goldstein, *supra* note 45, at 1 ("Like ghosts from the past, these forgotten electronic blips can come back to haunt a litigant, since computer data bases are subject to civil discovery requests.").

that the actors will seek out a more secure forum.[135] Arguably, less efficient means of communication might only be used in a relatively small number of cases where the parties think that their statements, ideas, or thoughts are likely to have negative legal consequences. However, given the variety of possible legal liability in modern businesses, the increase in the use of less efficient means of communication may nevertheless result in significant inefficiency.

In addition to the increased use of inefficient communication methods, there will likely be a decrease in the amount of information available during discovery as a result of two factors. First, as users become better educated regarding the possible use of e-mail against them in litigation, they will tend not to produce the "smoking gun" e-mails that have caused such alarm in some of the recent high profile cases. Furthermore, sophisticated e-mail users will become more likely to employ encryption software in an attempt to prevent access to their correspondence in future litigation. The process of diminishing returns of evidentiary quality e-mails may take time but is likely to occur.

Efficiency concerns involve questions of cost and time; a more serious issue is raised when an author thinks they have deleted an e-mail message yet later learns that the message may still be used as evidence in future litigation. It is the equivalent of a person shredding a letter and throwing it in the garbage, only to find it is legally permissible for another person to dig around in his garbage, take out the shredded message, and use it as evidence against him.

B. Privacy Concerns

Privacy concerns are implicated when the contents of millions of individual communications may legally be exposed to an audience wider than that expected or desired by the author. It must be noted at the outset that the following discussion will refer to general concepts of privacy rather than privacy rights. Although the two concepts are related, the general concept of privacy involves a broad spectrum of issues on how much we should protect individuals from intrusion by outside forces, whatever form the intrusion may take. Privacy rights, on the other hand, generally refer to a narrower set of constitutional restraints on strictly governmental intrusions, such as search and sei-

135. At least one district judge concluded that people's thoughts, if not their expression of those thoughts, will not be changed regardless of whether they refrain from communicating them. *See* Rosenbaum *supra* note 47, at 395 ("[D]oes anyone believe that people are 'thinking' more perfect thoughts simply because they are increasingly reluctant to express them? I seriously doubt it.").

zure restrictions, under the Fourth Amendment.[136] These constitutional restraints are relevant in this Comment insofar as they demonstrate that privacy, at least in some form, has always been seen as a right of all people. The alternative, of course, would be an Orwellian nightmare, where the state could freely intrude on the individual. However, this Comment addresses more limited question as to whether privacy concerns are implicated when deleted e-mails can be freely accessed during discovery, and if so, whether the intrusion is nevertheless justifiable by the ultimate truth finding goal in litigation. Before attempting to assess the degree to which individual privacy concerns are implicated, it is necessary to at least attempt to define privacy. The challenge of doing so, however, has proven difficult and has occupied some of the keenest legal minds of the past two centuries.[137]

In 1890, Samuel Warren and Louis Brandeis described privacy as "the right to be let alone,"[138] thus beginning an ongoing discussion regarding the core principles implicated by the concept of privacy. Later in his career, Justice Brandeis stated that privacy was "the most comprehensive of rights and the right most valued by civilized men."[139] Although the Justice's comment illustrates the importance that some noted jurists have placed on privacy, it does not help narrow the definition of privacy to concrete terms.

Nearly three-quarters of a century after the Warren and Brandeis article, Edward Bloustein attempted to provide a more unifying and useful description of the privacy interest.[140] He concluded that the core interest that privacy sought to protect was human dignity. Presciently, Bloustein also realized that technological advances posed a significant threat:

> [I]n our own day scientific and technological advances have raised the spectre of new and frightening invasions of privacy. Our capacity as a society to deal with the impact of this new technology depends, in part, on the degree to which we can assimilate the threat it poses to the settled ways of our legal insti-

136. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable search and seizures."). The Supreme Court has implied other privacy rights. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing a right to marital privacy).

137. *See* J.B. YOUNG, PRIVACY 2 (J.B. Young ed., 1978) ("[P]rivacy, like an elephant, is more easily recognized than described.").

138. Samuel Warren & Louis Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193, 195 (1890).

139. Olmstead v. United States, 277 U.S. 438, 478–79 (1928) (Brandeis, J., concurring).

140. *See* Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962 (1964).

> tutions have developed for dealing with similar threats in the past.[141]

Bloustein was concerned with the "spectre" of electronic surveillance.[142] However, his concerns apply equally to the more benign technology of e-mail. The "spectre" at issue in this context is the inability of persons to easily delete e-mail messages, or, put another way, technology's ability to limit ease of deletion.

Although the concepts of human dignity and personality may be useful in defining the broad sweep of the privacy concept, these concepts are extremely difficult to apply to real world situations. The concept of privacy as described by Professor Alan Westin, however, is easier to apply. Professor Westin agreed that privacy had the ability to protect human dignity[143] but went a step further and isolated four social goals that are furthered by protecting a citizen's right to control the release of personal information.[144]

First, Professor Westin stated that privacy has a role in the protection of personal autonomy and individuality. It affords an individual a zone of protection, where new ideas can be tested before being revealed to a wider audience.[145] Second, privacy provides a means for individuals to relax without having to worry about the pressure of playing societal roles. Thus, the individual is allowed to essentially "blow off steam" without worrying about being held responsible for his comments.[146] Third, privacy allows an individual to evaluate the increasing amount of information that surrounds him before choosing to make his reasoned thoughts public.[147] Finally, Professor Westin suggests that privacy also provides a means by which an individual can safely share his most personal feelings and secrets with those he trusts.[148] This concept is related to the community building function

141. *Id.* at 963.

142. *Id.* at 963 n.7.

143. *See* ALAN WESTIN, PRIVACY AND FREEDOM 33 (1967) ("In democratic societies there is a fundamental belief in the uniqueness of the individual, in his basic dignity and worth as a creature of God and a human being, and in the need to maintain social processes that safeguard his sacred individuality.").

144. Professor Westin's definition has also been used in the debate over the appropriate degree of privacy to be given to personal information. *See* Walker, *supra* note 13, ¶ 6 ("For purposes of framing the contemporary debate about whether and how to regulate the exchange of personal information, the best definition of privacy arguably comes from the seminal modern work *Privacy and Freedom* by Alan Westin . . . .").

145. *Id.* at 34.

146. *Id.* at 35.

147. *Id.*

148. *Id.* at 39.

that e-mail may perform in a modern urban society where "reserved communication is the means for psychic self-preservation."[149]

To understand the role of e-mail in furthering the privacy goals outlined by Professor Westin, an analysis of how e-mail is used is in order. Empirical evidence suggests that many e-mail users expose their most candid thoughts in e-mails, which is one of the primary reasons why e-mails currently play such a prominent role in discovery. In the pre-computer world, these interactions would have been carried out via telephone or in person—in doorways or around the water cooler. These candid e-mail messages represent thoughts that an individual would usually commit to a more permanent written record only when they felt that the ideas were fully developed and refined.[150] Whether justified in doing so, a great many people seem to use e-mail as though it provides a secure zone in which they can further the goals outlined by Professor Westin. This situation alone indicates that the outlets for these types of personal interactions may severely be limited by the potential discoverability of these private messages.

A recent decision by the U.S. District Court of Maryland illustrates the limited availability of communication tools to serve individualistic and expressive goals of privacy.[151] Mr. Allan Lucas, a management-level employee at the United States Fidelity and Guaranty Company, sent an e-mail message to his fellow management-level employee that contained a numerical code corresponding to a list of seventy-five profane words and phrases.[152] Mr. Lucas then utilized the code to criticize his general manager, inserting the numerical equivalent for each profane word.[153] In a later e-mail, Mr. Lucas expressed his dissatisfaction with new salary provisions at the firm and again utilized the code to insert a number of profane phrases.[154] As a result of these e-mails, Mr. Lucas was fired.[155] What is particularly notable about this case is the apparent lack of outlets for secure communication available to Mr. Lucas. As a management-level employee, he likely had a range of possible ways to communicate at his disposal. Yet, apparently, none allowed him the ability to vent his personal views on issues that affected his work.

---

149. *Id.*

150. *See* Susan J. Silvernail, *Electronic Discovery in the Computer Age*, 58 ALA. LAWYER 176, May, 1997, at 181 (noting that e-mail has become a substitute for telephonic and printed communications, as well as a substitute for direct oral communications).

151. *See* Miller v. U.S.F. & G., No. 93-1968, 1994 WL 395718 (D. Md. May 13, 1994).

152. *Id.* at *2.

153. *Id.* When translated from the code, Mr. Lucas's message described his manager as a "Dick Head." *Id.*

154. *Id.*

155. *Id.*

Mr. Lucas attempted, in vain, to establish his own zone of privacy on an e-mail network. He did so precisely for the reasons that Professor Westin outlined. He was attempting to release his feelings to a trusted colleague, to "blow off steam" about various subjects such as his manager and his firm's policies. Undoubtedly, he was not ready to tell his manager how he felt about him, although, over time, he may have refined his thoughts enough to confront the manager regarding his concerns. However, Mr. Lucas did not get that chance, as his thoughts were revealed uncensored and unrefined, and not surprisingly, the consequences were serious.

In addition to providing individuals with a channel for releasing their emotions, e-mail also serves to convey the more relaxed communications that are a part of everyday life. Jeffrey Rosen, the author of a recent book addressing privacy concerns in the modern age, asserts that "[f]or more and more citizens the most important way of exchanging gossip is e-mail."[156] Although gossip is not the foundation on which civilizations are built, gossip and other related modes of expression such as humor, sarcasm, irony, and satire have been around for centuries and enrich the human experience. It is probably easiest to understand the degree to which they do so by imagining a society wherein these forms of expression are not allowed, a society more totalitarian than democratic.

C. Free Speech

Privacy also tends to encourage free expression. The goals advanced by affording privacy to the individual are similar to the goals achieved by protecting free speech.[157] Freedom of expression is central to a democratic society. As the privacy expectations of e-mail users diminish, the freedom of the thoughts expressed via this medium will likely tend to move towards only those ideas and thoughts considered acceptable for a wide audience.[158] There is a risk that organizational and individual censorship will result and much will be lost.

Of the billions of e-mail messages that are sent each year, there are undoubtedly a large number of messages that would not be consid-

---

156. Jeffrey Rosen, *The Eroded Self*, N.Y. TIMES MAGAZINE, Apr. 30, 2000, §6, at 51.

157. *See* THOMAS I. EMERSON, THE SYSTEM OF FREEDOM OF EXPRESSION 6 (1970). Emerson lists four essential values of free speech. First, it allows for individual self-fulfillment. Second, it allows for the advancement of knowledge and discovery of truth. Third, it allows participation in the decision making process by all members of society. Finally, it encourages a "more adaptable and hence stable community." *Id.* at 389.

158. Heather Brewer, *Snap Judgments*, BUSINESS LAW TODAY, July–Aug. 1999, at 4 ("The chill in cyberspace comes from the not-so-user-friendly impact that e-mail messages have had in Microsoft's run-in with the Justice Department.").

ered worthy of protection. However, the basic tenet of American free speech jurisprudence holds that all ideas and expressions should be encouraged as far as possible, until conflicting social concerns demand that speech be limited.[159] Where, as here, the effective curtailment occurs of an individual's ability to control when and how to reveal his speech, there is a danger that an author of ideas, both good and bad, will turn to other less efficient means or refrain from expressing ideas completely. Thus, the author, without ability to control his speech, will express opinions via e-mail that "tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited tend to lose their quality of unique personal warmth and to become the feelings of everyman. Such a being, although sentient, is fungible; he is not and individual."[160] Therefore, the cost to free speech must be considered in assessing the relevant costs and benefits of exposing "deleted" e-mails to the glare of judicial discovery.

VII. POTENTIAL SOLUTIONS

In light of the harmful effects on communication efficiency, privacy, and free speech that are likely to result from the present rules of free discovery of "deleted" e-mails, it will be worthwhile to at least consider alternative courses of action. If the "flaw" that needs to be addressed is the inability of an author to effectively destroy e-mails in the same manner as paper documents, the most obvious solution is to allow technology to provide a remedy. Indeed, software programs are now available to allow the sender of e-mails to destroy their messages upon receipt or upon the passage of a certain time period after receipt.[161]

The technological self-help solution has the obvious advantage of not requiring any judicial intervention. [162] Developing technology would be allowed to provide the necessary privacy for individuals and companies. There are, however, problems with relying on technology alone. First, requiring individuals to create their own "privacy-zones" is likely to lead to unequal protection. Whereas large firms may have

159. *See* JOHN STUART MILL, ON LIBERTY 19; *see also* Abrams v. United States 250 U.S. 616, 630 (1919) (Holmes, J., dissenting) (evoking the image of a "market place of ideas").

160. Bloustein, *supra* note 140, at 1123.

161. For detailed information regarding one such program, see OMNIVA POLICY SYSTEMS, TRANSPARENT AND EASY-TO-USE SECURE EMAIL, *available at* http://www.disappearinginc.com (last visited June 1, 2002).

162. *See* William J. McSherry, Jr., *"E-Discovery" and the Non-Party: Effective Use of Existing Protections Can Guard Against Unwarranted Expenses*, N.Y. L.J., June 26, 2000, at S3 ("One of the reasons for exercising great caution is that software and hardware continue to evolve at a pace that far outstrips the capacity of the rule-making process to generate court rules.").

the technical knowledge and deep pockets to pay for the cost of special encryption software, individuals and smaller firms may not have similar resources. Second, even if encryption software becomes widely available, we should question whether the legal rules should encourage the use of "deletion" software. Software products that permanently delete e-mail correspondence will greatly diminish the amount of evidence available in all cases. It is the equivalent of encouraging companies to shred all but the most vital documents. The pool of information to be discovered in each case may be limited to those documents created in the few days before the litigation became foreseeable. The likely result is to greatly hinder the central function of discovery: the search for the truth.

Third, it may not be desirable to force litigants to enter into an ever-escalating battle of encryption and decryption. It is not altogether impossible that another software program may rise to the challenge of recovering even "permanently" destroyed e-mail messages, although at even greater cost. Finally, given the choice, most observers would agree that it is better to avoid a situation where e-mail users are forced to encrypt their messages if another alternative is available because the very act of encryption can reinforce the feeling that the "spectre" of surveillance is omnipresent in modern society.

Given the difficulties with allowing technology to solve the problem of undeletable e-mails, it may be desirable to consider an alternative solution: a presumption of non-discoverability of "deleted" e-mails. In the normal case, a party's deleted e-mails would be off-limits during discovery. However, a party could overcome this presumption by showing a strong likelihood that the deleted e-mails contain relevant information. For example, a party could make this showing by demonstrating that another party had deliberately set about destroying relevant documents or by giving a detailed explanation as to why the party believes relevant e-mails were deleted and the potential importance of this evidence to the issues being litigated. The advantage of such a rule is that the law would comport with the expectations of the majority of e-mail users—"delete" would once again mean delete.

VIII. CONCLUSION

The present discovery rules, promulgated before the recent explosion of e-mail use, do not sufficiently reflect a number of important societal concerns. E-mail, as the most dynamic communication device of the present era, should be utilized to the maximum degree possible. The cost to the truth finding function of discovery must be balanced

against concerns about communication efficiency, privacy, and free speech. We should not blindly force companies to use inefficient communication tools or resort to encryption. Perhaps, more importantly, e-mail users should be afforded the luxury of a dress rehearsal before being threatened with making their discarded thoughts public.

With regard to the present discovery practice, distinct advantages are gained by enforcing a presumption against the discoverability of "deleted" e-mails. Because the present trend of e-mail use will tend to lessen the amount of available material for discovery over time, the cost of this presumption to the judicial process will not be profound. The Standing Committee on the Rules of Civil Procedure should consider an amendment to the civil rules.[163] Time is of the essence because once usage habits are formed, they may be extremely difficult to alter.

163. The Texas Rules of Civil Procedure have adopted a provision that limits access to residual or deleted data. *See* TEX. R. CIV. P. 196:

> The responding party must produce the electronic or magnetic data that is responsive to the request and is reasonably available to the responding party in its ordinary course of business. If the responding party cannot – through reasonable efforts – retrieve the data or information requested or produce it in the form requested, the responding party must state an objection complying with these rules. If the court orders the responding party to comply with the request, the court must also order that the requesting party pay the reasonable expenses of any extraordinary steps required to retrieve and produce the information.