2006

"Don't Read This If It's Not for You": The Legal Inadequacies of Modern Approaches to E-Mail Privacy

Joshua L. Colburn

Note

"Don't Read This If It's Not for You": The Legal Inadequacies of Modern Approaches to E-mail Privacy

Joshua L. Colburn∗

For many, electronic mail (e-mail) has become an integrated component of daily life. With no postage and the promise of a virtually instant reply time, it is no wonder that e-mail volume has increased from 5.1 million messages in 2000 to 135.6 million messages in 2005.[1] Unfortunately, many users cling to a false sense of security associated with e-mail's widespread acceptance as a legitimate communication medium.[2] In an effort to limit liability and increase privacy, a growing number of e-mailers have incorporated disclaimers into their messages.[3]

∗ J.D. Candidate 2007, University of Minnesota Law School; B.S. 2003, University of Minnesota: Institute of Technology. The author thanks Dean Joan Howland for her advice and guidance, Lorre and Vicki Colburn for their loving support, and the outstanding editors and staff of the *Minnesota Law Review*.

1. Lizzette Alvarez, *Got 2 Extra Hours for Your E-mail?*, N.Y. TIMES, Nov. 10, 2005, at G1.

2. CHRISTINA CAVANAGH, MANAGING YOUR E-MAIL: THINKING OUTSIDE THE BOX 46 (2003) ("We have fooled ourselves into regarding our e-mail correspondence as we would a conversation—a surrogate for a more personal exchange like the telephone or face-to-face.").

3. *See* CATHERINE SANDERS REACH ET AL., A.B.A. LEGAL TECH. RES. CTR., 2006 AMERICAN BAR ASSOCIATION LEGAL TECHNOLOGY RESOURCE CENTER SURVEY REPORT: WEB AND COMMUNICATION TECHNOLOGY TREND REPORT 13 (2006) (reporting that seventy-six percent of firms surveyed "use confidentiality statements as a security precaution").

For an example of a typical disclaimer, examine the following suggested e-mail footer:

> This e-mail and any files transmitted with it are confidential and are intended solely for the use of the individual or entity to whom they are addressed. This communication may contain material protected by the attorney-client privilege. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended re-

A possible explanation for the increasing popularity of e-mail disclaimers may be the recent adoption of e-mail in the legal community.[4] As the new millennium approached, lawyers were still debating the prudence of practicing law over the Internet.[5] When lawyers finally started to use e-mail,[6] many practitioners copied the privilege and confidentiality disclaimers from their letters and faxes into their e-mail messages.[7] Because these adapted e-mail disclaimers derive from legal obligations unique to the legal profession,[8] the effectiveness of disclaimers outside the legal profession dissipates.[9] Therefore, contrary to popular belief,[10] adding privacy disclaimers to business and personal e-mail messages has no legal effect.[11]

This Note takes a practical look at the legal foundations of e-mail disclaimers and argues that, outside the attorney-client relationship, disclaimers are generally unenforceable and,

---

> cipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please immediately notify _____ by telephone at _____. You will be reimbursed for reasonable costs incurred in notifying us.

MICHAEL R. OVERLY, E-POLICY: HOW TO DEVELOP COMPUTER, E-MAIL, AND INTERNET GUIDELINES TO PROTECT YOUR COMPANY AND ITS ASSETS 68–69 (1999).

4. *See* John Christopher Anderson, *Transmitting Legal Documents over the Internet: How to Protect Your Client and Yourself*, 27 RUTGERS COMPUTER & TECH. L.J. 1, 2 (2001) ("The use of e-mail and Internet technology in law firms has exploded over the last ten years."); Sherry L. Talton, *Mapping the Information Superhighway: Electronic Mail and the Inadvertent Disclosure of Confidential Information*, 20 REV. LITIG. 271, 272 (2000) ("E-mail will replace paper correspondence and radically alter the practice of law.").

5. Jason Krause, *Guarding the Cyberfort: Careless Internet Habits Can Open Your Firm to Malpractice*, ARK. LAW., Spring 2004, at 25, 25 (noting that some firms were known to block e-mail usage among their attorneys out of concern for disclosure of client information).

6. A.B.A. LEGAL TECH. RES. CTR., JUNE 2000 TELEPHONE SURVEY: HOW ATTORNEYS USE E-MAIL, http://www.abanet.org/tech/ltrc/surveys/june2000.html (last visited Oct. 19, 2006) (finding that ninety-four percent of attorneys participating in a random phone survey use e-mail in their practices).

7. Krause, *supra* note 5, at 29.

8. *See, e.g.*, MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2006) ("A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.").

9. *See* CAVANAGH, *supra* note 2, at 47 ("You have no control over your recipients' decisions to forward your messages to others without your knowledge or consent.").

10. *See* MATT HAIG, E-MAIL ESSENTIALS 76 (2001).

11. *See* CAVANAGH, *supra* note 2, at 47.

therefore, ineffective. Part I of this Note presents a brief background of similar disclaimers in other forms of communication, including traditional mail and facsimiles. Part II provides a summary of existing privacy law and explains the limits of its applicability to e-mail, including the unique role of e-mail privacy disclaimers in the legal profession. Part III examines the possible extra-legal benefits of including a disclaimer and suggests a few best practices for maximizing effect and enforceability. Part IV describes a proposal to modify current practices and update existing law in an effort to achieve increased e-mail privacy. This Note concludes that a majority of the common provisions of e-mail disclaimers are unenforceable and that e-mail encryption is a viable and substantially more secure alternative.

I. THE DISCLAIMER AS A PRIVACY TOOL

The risks associated with communicating confidential information are apparent in various contexts. An attorney is subject to reprimand or even malpractice liability by exposing confidential or privileged information.[12] An employee disclosing sensitive material may face dismissal or legal action.[13] There is no telling how much embarrassment or scrutiny an individual might encounter when private communications become public.[14]

Because communications privacy had been a general concern well before the proliferation of e-mail, e-mailers understandably look to older forms of communication for effective security solutions. With e-mail, however, "it is very easy to click on the wrong name and send the message to an unintended

12. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a). *See generally* Daniel L. Draisen, The Model Rules of Professional Conduct *and Their Relationship to Legal Malpractice Actions: A Practical Approach to the Use of the Rules*, 21 J. LEGAL PROF. 67, 67 (1997) (explaining that punishments for attorneys range from private reprimands to complete disbarment).

13. AM. MGMT. ASS'N & EPOLICY INST., 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY SUMMARY 6–7 (2004), *available at* http://www.epolicyinstitute.com/survey/survey04.pdf (finding that twenty-five percent of employers surveyed had terminated "an employee for violating e-mail policy").

14. *See* Ann Carrns, *Those Bawdy E-mails Were Good for a Laugh—Until the Ax Fell*, WALL ST. J., Feb. 4, 2000, at A1 (reporting that improper contents of e-mail messages resulted in the firing of nearly two dozen *New York Times* employees).

person." Thus, e-mail garners more disclosure anxiety than traditional forms of communication.[15]

A. THE FACSIMILE: E-MAIL'S OLDER SIBLING?

With the introduction of the facsimile, the ease of sending information to the wrong recipient changed from a matter of writing the wrong address to mistyping a single digit. Because a cover sheet disclaimer is "virtually all you can do to ensure that a recipient who gets it incorrectly knows not to read the fax,"[16] lawyers have included disclaimers on facsimiles for quite some time.[17] The insecure practice of receiving faxes in a common area prompted the Minnesota State Lawyers Professional Responsibility Board to issue an opinion in 1999, distinguishing facsimiles from other, more acceptable, means of communicating confidential client information.[18]

In order to maximize enforceability, facsimile confidentiality disclaimers generally appear at the beginning of the message.[19] In fact, one commentator advises attorneys to "make it a practice to use a coversheet containing these confidential legends every time they send a fax containing privileged information."[20] While such a coversheet provides notice to all readers, lawyers are under an additional ethical obligation to return a missent communication to opposing counsel without examining it.[21] Though this obligation is most commonly associated with faxes, the American Bar Association Model Rules of Professional Conduct extend this duty to the receipt of *any* missent

15. OVERLY, *supra* note 3, at 13.

16. Abdon M. Pallasch, *Fax Cover Sheets Carry Dire Warnings for Law and Lasagna*, CHI. LAW., Feb. 1995, at 14, 15.

17. *See* Tracy Thompson et al., *Ethical Issues for Employment Lawyers*, *in* 664 PRACTISING LAW INSTITUTE LITIGATION COURSE HANDBOOK 859, 876 (2001) (noting the popularity of confidentiality disclaimers on legal fax cover sheets).

18. *See* Minn. State Lawyers Prof'l Responsibility Bd., Op. 19 cmt. (1999) [hereinafter Minn. Ethics Op. 19] ("With facsimile machines, the concerns are less with interception than with unintended dissemination of the communication at its destination, where the communication may be received in a common area of the workplace or home and may be read by persons other than the intended recipient.").

19. *See* Krause, *supra* note 5, at 29.

20. Anne G. Bruckner-Harvey, *Inadvertent Disclosure in the Age of Fax Machines: Is the Cat Really out of the Bag?*, 46 BAYLOR L. REV. 385, 397 (1994).

21. *See* Pallasch, *supra* note 16, at 15, 73.

"document."[22] However, it is important to recall that confidentiality concerns extend well beyond the limited realm of lawyer-lawyer and lawyer-client communication.[23]

B. THE ARGUMENT FOR DISCLAIMERS ON E-MAIL MESSAGES

If one considers e-mail just another form of written communication, many of the justifications for fax disclaimers are readily applicable. In fact, the State Bar of Michigan's Committee on Professional and Judicial Ethics equated e-mail communication to postcards or facsimile transmissions as early as 1996.[24] Much like a fax or postcard, "simple e-mail generally is not 'sealed' or secure."[25] Difficulties similar to those posed by receiving faxes in a common area[26] can also arise in a business environment when curious or disgruntled employees intercept an e-mail communication discussing sensitive matters such as a "proposed sale of the business or employee termination issues."[27] With e-mail, this threat also exists outside the office, where messages may be readily "accessed or viewed on intermediate computers between the sender and recipient."[28] Because of this vulnerability, "[e]-mail not only can be, but *is* intercepted with surprising frequency."[29] By contrast, facsimiles travel directly over the telephone line from sender to recipient and leave no intermediate copies behind. Moreover, a fax's readability quickly deteriorates across multiple transmissions, while an e-mail remains clear and legible after retransmission to an unlimited number of recipients.[30] Due to e-mail's digital

22. *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2006) ("A lawyer who receives a document relating to the representation of a lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.").

23. *See* NANCY FLYNN, THE EPOLICY HANDBOOK 3–9 (2001) (arguing that every organization should have e-mail, Internet, and software policies).

24. *See* Mich. Comm. on Prof'l Responsibility & Judicial Ethics, Op. RI-276 (1996), *available at* http://www.michbar.org/opinions/ethics/numbered_opinions/ri-276.htm.

25. Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

26. *See* Minn. Ethics Op. 19, *supra* note 18.

27. *See* Brett R. Harris, *Counseling Clients over the Internet*, COMPUTER & INTERNET LAW., Aug. 2001, at 4, 5.

28. *Reno*, 929 F. Supp. at 834; *accord* Anderson, *supra* note 4, at 4 ("Because e-mail is transmitted over an 'open network,' electronic documents travel through countless interconnected computers on their Internet voyage.").

29. Anderson, *supra* note 4, at 7.

30. *See* OVERLY, *supra* note 3, at 11–12.

format, degradation of quality over an enormous number of forwards is not an issue.[31]

In addition, the unique properties of e-mail introduce several new concerns, including fresh ways to dispatch a message to an unintended third party. For example, the relative ease of "spoofing," or making a message appear to be from someone else, creates the possibility that replying to an existing e-mail can result in disclosure of private information to an unintended recipient.[32] Hitting the reply button is considerably simpler than typing an incorrect seven- or ten-digit number into a fax machine. Therefore, a truly effective e-mail disclaimer should protect against more than the accidental misaddress of a message.

The various practical differences between faxes and e-mail messages are substantial enough to challenge the sufficiency of copying a fax disclaimer into an e-mail verbatim.[33] Furthermore, while facsimile disclaimers have yet to work their way into non-legal faxes, business and personal e-mail disclaimers appear to be quite popular.[34] This growth is overzealous, however, as the legal foundation for e-mail privacy disclaimers is difficult to identify.[35]

II. SEARCHING FOR A FOUNDATION

Most e-mail disclaimers suggest a level of legal support, but do not specifically reference any statutes or specific legal principles.[36] In fact, despite the common disclaimer language

31. *Id*.

32. Harris, *supra* note 27, at 6–7 (describing the potential for "spoofing"); *see also* Anderson, *supra* note 4, at 14 ("E-mail with a falsified return address may be used to trick an e-mail recipient into releasing confidential information.").

33. *Compare* OVERLY, *supra* note 3, at 10–12 (describing the characteristics of e-mail), *with* Pallasch, *supra* note 16, at 14–15 (discussing facsimile cover sheet warnings).

34. REACH, *supra* note 3, at 13 (reporting that seventy-six percent of firms surveyed "use confidentiality statements as a security precaution").

35. Claire Smith, *Confusion Rules on Disclaimers*, FIN. TIMES, Dec. 21, 2005, 2005 WLNR 20764252 ("The validity of disclaimers is as yet largely untested.").

36. Consider, for example, this disclaimer suggested to academic advisors by the University of Maryland Campus Legal Office:

> This message and any included attachments are property of the University of Maryland, College Park, and are intended only for the addressee(s). The information contained herein may include trade secrets or privileged or otherwise confidential information.

that certain actions are "strictly prohibited"[37] or "may be unlawful,"[38] courts have yet to address the enforceability of a privacy disclaimer in the context of electronic mail. Therefore, this Note addresses the likely legal arguments favoring the most common provisions of e-mail disclaimers.

A. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986

The Electronic Communications Privacy Act of 1986 (ECPA),[39] an extension of the Federal Wiretap Statute of 1968,[40] provides the best foundation for a claim to e-mail privacy. Congress passed the ECPA in response to a study showing the potential threats that new technologies posed to the civil liberties of the citizenry.[41] The Senate Judiciary Committee reported that while a first class letter was "afforded a high level of protection against unauthorized opening," there were "no comparable . . . statutory standards to protect the privacy and security of communications transmitted by . . . new forms of telecommunications and computer technology."[42] Therefore, the ECPA makes unauthorized interception of e-mail subject to a $500 fine, not more than five years in prison, or both.[43] The concept of the ECPA was apparently persuasive, as many states have independently adopted most if not all of its provisions.[44]

> Unauthorized review, forwarding, printing, copying, distributing, or using such information is strictly prohibited and *may be unlawful*. If you received this message in error, or have reason to believe you are not authorized to receive it, please promptly delete this message and notify the sender by e-mail. Thank you.

Univ. of Md. Coll. of Agric. & Natural Res., *Email Disclaimers*, ADVISOR'S ADVISOR, Jan. 2005, http://www.agnr.umd.edu/AGNRnews/Article.cfm?&ID=4368&NL=87 [hereinafter Univ. of Md. Coll. of Agric. & Natural Res., *Email Disclaimers*] (emphasis added).

37. *See*, *e.g.*, OVERLY, *supra* note 3, at 69.

38. *See*, *e.g.*, Traversio, *Email Disclaimer*, http://www.traversio.com/traversio/corporate_legal_disclaimer.htm (last visited Oct. 19, 2006); Univ. of Md. Coll. of Agric. & Natural Res., *Email Disclaimers*, *supra* note 36.

39. Pub. L. No. 99-508, 100 Stat. 1848 (1986).

40. Pub. L. No. 90-351, tit. III, 82 Stat. 211–25 (codified as amended at 18 U.S.C. §§ 2510–22 (2000)); *see* Harris, *supra* note 27, at 5.

41. 132 CONG. REC. H4045 (daily ed. Jun. 23, 1986) (statement of Rep. Kastenmeier) (acknowledging that the ECPA "grew out of extensive hearings and an Office of Technology Assessment study"); OVERLY, *supra* note 3, at 25.

42. S. REP. NO. 99-541, at 5 (1986).

43. 18 U.S.C. § 2511(4)(a)–5(b) (2000); OVERLY, *supra* note 3, at 26.

44. *See*, *e.g.*, Privacy of Communications Act, MINN. STAT. §§ 626A.01–.41 (2004).

An important limitation of the ECPA, however, is that it only applies to the "interception" of electronic communication.[45] The statute itself defines "intercept" to be "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[46] Nonetheless, courts have thoroughly discussed the meaning of interception under the ECPA.

For example, the Eighth Circuit restricted the definition of interception under the earlier Federal Wiretap Statute to action taken with "bad purpose . . . , without justifiable excuse . . . , stubbornly, obstinately or perversely."[47] Under this definition, accidental e-mail recipients, who likely possess none of these attributes, would not qualify as interceptors under the ECPA. Because the ECPA restricts only the interception of electronic communications, accidental recipients would be free to do what they please with the contents of the message without fear of violating the statute.[48]

Courts have limited the applicability of the ECPA by finding that electronic communications that have reached their destination are ineligible for interception and, therefore, are outside the protections of the ECPA.[49] In 1998, the Third Circuit affirmed the determination that a person "can disclose or use with impunity the contents of an electronic communication unlawfully obtained from electronic storage."[50] The Eleventh Circuit followed suit in 2003 by agreeing that interception under the ECPA only occurs when a communication is in transit.[51] Due to this "contemporaneous interception"[52] requirement, the ECPA apparently does not protect electronic communications that have reached *any* destination, let alone those that have reached the incorrect destination. Because an e-mail must

45. *See* 18 U.S.C. § 2511(1)(a) (limiting applicability to "any person who . . . intentionally *intercepts*, endeavors to *intercept*, or procures any other person to *intercept* or endeavor to *intercept*, any . . . electronic communication" (emphasis added)).

46. 18 U.S.C. § 2510(4) (2000).

47. *See* United States v. Ross, 713 F.2d 389, 391 (8th Cir. 1983) (quoting United States v. Murdock, 290 U.S. 389, 394 (1933)).

48. *See* CAVANAGH, *supra* note 2, at 47 (describing an e-mail recipient's ability to do various things with received e-mail messages).

49. *See* Wesley Coll. v. Pitts, 974 F. Supp. 375, 389 (Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998).

50. *Id.*

51. *See* United States v. Steiger, 318 F.3d 1039, 1040 (11th Cir. 2003).

52. *Id*. at 1039.

reach a destination before a human recipient will read any disclaimer attached to it, the ECPA likely lends no authority to disclaimers that claim legal power over the actions of a recipient. Furthermore, the ECPA does not protect the copies an e-mail leaves on servers as it travels to its destination,[53] copies which are not themselves traveling.[54]

In addition to its failings in the realm of delivered e-mail, the ECPA contains an exception that significantly weakens the level of protection that it provides to e-mail messages that actually are in transit. Commonly referred to as the "provider exemption,"[55] it allows electronic communication service providers to "intercept, disclose, or use" communications sent through their facilities.[56] Therefore, the ECPA explicitly permits Internet service providers, employers, and various other e-mail providers to monitor any e-mail that travels on or through their internal network systems, notwithstanding any attached privacy disclaimers. Because of the open-network nature of the Internet, e-mail messages commonly travel on a provider's network without either originating from or terminating at an address on that same network.[57] Consequently, the ECPA permits providers to peer into mere pass-through e-mail traffic. Thus, the ECPA, through its limited scope and provider exemption, provides little protection to standard e-mail traffic.

While analogies between postal mail and e-mail are accurate to a point, the ECPA is sorely ill-equipped to fulfill its purpose of placing e-mail on the same protective plane as postal mail. Unfortunately, the ECPA neglects the fact that the way modern e-mail systems work is rather similar to storing one's postal mail in a giant mailbox at the end of the driveway. The ECPA not only does not require disclaimers, but it also lends no substantive support to e-mail privacy disclaimers. Because the

53. *See* Anderson, *supra* note 4, at 5–6.

54. *See Steiger*, 318 F.3d at 1040; *Wesley Coll.*, 974 F. Supp. at 391.

55. *See* Thompson et al., *supra* note 17, at 874.

56. 18 U.S.C. § 2511(2)(a)(i) (2000) ("It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication."); *see also* Jon Swartz, *Boeing Scandal Highlights E-mail Checks*, USA TODAY, Mar. 11, 2005, at 5B ("Monitoring employee e-mail is becoming the norm in Corporate America."). *See generally* FLYNN, *supra* note 23, at 34 ("According to the [ECPA], an employer-provided computer system is the property of the employer.").

57. *See* Anderson, *supra* note 4, at 5–6.

ECPA neither mentions nor supports e-mail disclaimers, one must locate a more creative foundation for e-mail privacy.

B. COPYRIGHT

Federal copyright law provides another possible legal basis for e-mail privacy.[58] One commentator suggests that "[t]he instant you finish typing a message, the e-mail is protected under federal copyright law."[59] He further asserts that registration and copyright notice are "not necessary" to reserve one's copyright in a message.[60] Under this assessment, copyright appears to be an e-mail privacy panacea. However, the value of copyright as an e-mail privacy tool is overstated.[61]

Registration is not, in fact, required to invoke copyright protection, but it *is* required to file an infringement suit.[62] Therefore, to assert copyright protection as a basis for e-mail privacy without actually registering is, realistically, an idle threat. For most e-mailers, it is implausible to consider paying a thirty dollar copyright registration fee for each private communication.[63]

Even if a user manages to get past the registration hurdle, the nature of copyright law itself provides another bar to enforcement. A cause of action for copyright infringement also requires that the infringer actually violate the owner's copyright rights.[64] This action may include copying the work or distributing it, but simple disclosure of an e-mail's contents does not appear to qualify as infringement.[65] Though copyright appears to

58. *See* OVERLY, *supra* note 3, at 47.

59. *Id.*

60. *Id.*

61. Thomas G. Field, Jr., *Copyright in E-mail*, 5 J. ELEC. PUBL. (1999), http://www.press.umich.edu/jep/05-01/field.html ("Copyright should have no bearing on the use of messages never intended for public distribution.").

62. 17 U.S.C.A. § 411(a) (2005) ("No action for infringement of the copyright in any United States work shall be instituted until preregistration or registration of the copyright claim has been made in accordance with this title.").

63. *See* Marybeth Peters, *Analysis and Proposed Copyright Fee Schedule to Go into Effect July 1, 2002*, at 9–10 (2002), http://www.copyright.gov/reports/fees2002.pdf (noting that increasing copyright registration fees have been accompanied by diminishing numbers of copyright registrations).

64. *See* 17 U.S.C. § 501 (2000) ("Anyone who violates any of the exclusive rights of the copyright owner . . . is an infringer."); Field, *supra* note 61.

65. *See generally* 17 U.S.C. §§ 107–22 (enumerating the rights of a copyright owner).

be a creative way to fill in a few of the holes in the ECPA, it is by no means a complete patch.

C. FULFILLING A DUTY

Some e-mail disclaimers are nothing more than a response to a legal duty to identify certain communications as confidential.[66] Because "no cases directly address whether e-mail sent over the Internet is subject to a reasonable expectation of privacy,"[67] senders are arguably prudent to proceed as if there is no such expectation. Often, the inclusion of an appropriate e-mail disclaimer satisfies certain duties of nondisclosure. For example, the Internal Revenue Service's recent revisions to its Circular 230 require the inclusion of a disclaimer with written statements about specific federal tax issues.[68] Under such circumstances, the inclusion of an e-mail privacy disclaimer is both necessary and appropriate.[69] Ordinary business and personal e-mail messages, however, do not have any such statutory requirements.

Considering the duties of confidentiality imposed on other industries, the legal community's concerns over e-mail communication are readily visible. These concerns are likely due to the legal community's direct involvement in the issue of confidentiality. The American Bar Association's *Model Rules of Professional Conduct* place a general burden of confidentiality on an attorney regarding "information relating to representation of a client,"[70] and disclosure may subject a lawyer to malpractice proceedings or sanctions.[71]

Much of the discussion of e-mail privacy has surrounded the maintenance of attorney-client privilege. Because the law governing waiver of privilege through inadvertent disclosure is in a "state of flux," the effectiveness of including a disclaimer

66. A.B.A. LEGAL TECH. RES. CTR., *supra* note 6.

67. Talton, *supra* note 4, at 271.

68. *See* Jane Pribek, *New Trend: Law Firms Have Their Own 'In-House' Counsel*, MINN. LAW., Sept. 26, 2005, at S-1, *available at* 2005 WLNR 15313245.

69. *Id.*; *see also* Letter from McNair Law Firm, P.A. to Its Clients, IRS Circular 230 and Its Impacts, http://www.mcnair.net/230.pdf (explaining its inclusion of a disclaimer confirming with the requirements of Circular 230) (last visited Oct. 19, 2006).

70. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2006) ("A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation.").

71. *See* Draisen, *supra* note 12, at 67.

very much depends on the law of the applicable jurisdiction.[72] For all jurisdictions, a communication must satisfy three criteria in order to be eligible for privilege protection: the client must have intended it to be confidential, the client's expectation of confidentiality must be reasonable under the circumstances, and the confidentiality must have been subsequently maintained.[73]

There are three categories of attorney-client privilege jurisdiction: strict responsibility, balancing, and no-waiver.[74] In a strict responsibility jurisdiction, the existence of a disclaimer will do nothing to maintain privilege because disclosure alone waives the privilege.[75] In a balancing jurisdiction, the inclusion of an attorney-client privilege disclaimer will weigh in favor of maintaining the privilege in the case of an inadvertent disclosure.[76] In a no-waiver jurisdiction, a disclaimer is superfluous as long as the sender did not intend to waive the privilege.[77] While failure to assert attorney-client privilege has resulted in waiver,[78] it is important to note that the inclusion of a disclaimer apparently does no harm in any of the three classes of jurisdiction.

In 1998, the American Bar Association adopted Resolution 98A119A, urging the courts to afford e-mail communication "the same expectations of privacy and confidentiality as those accorded traditional means of communication."[79] A strict interpretation of this classification suggests that the ABA considers e-mail to be as secure as sending a letter through the postal service, where disclaimers are rarely used. A year later, the ABA Standing Committee on Ethics and Professional Responsibility built upon Resolution 98A119A in Formal Opinion 99-413 by addressing the confidentiality of unencrypted e-mail.[80]

72. *See* Talton, *supra* note 4, at 274.

73. *Id*. at 288–89.

74. Bruckner-Harvey, *supra* note 20, at 393.

75. *Id*.

76. *Id*.

77. *Id.*

78. United States v. Neill, 952 F. Supp. 834, 842 (D.D.C. 1997) (finding that a lack of evidence that the defendants asserted a claim of attorney-client privilege with respect to computer material precluded a later assertion of privilege).

79. Harris, *supra* note 27, at 10; *see also* A.B.A., POLICY & PROCEDURES HANDBOOK 276 (2005–06).

80. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999) [hereinafter Formal Op. 99-413].

Formal Opinion 99-413 states that "[a] lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct . . . because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[81] However, the Committee on Ethics and Professional Responsibility bases much of its conclusion on the presumption that the "unauthorized interception *or* dissemination of the information is a violation of [the ECPA]."[82] As discussed above in Part II.A., courts have held the ECPA to restrict the dissemination of only *intercepted* information.[83] Nonetheless, the Committee asserts the contrary conclusion that the ECPA somehow bars the disclosure of stored information.[84]

Despite the Committee's questionable assumption regarding the scope of the ECPA, Formal Opinion 99-413 prescribes that "[p]articularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters."[85] A disclaimer apparently does not qualify as a "particularly strong" measure, as the Committee only lists the avoidance of e-mail altogether as an example.[86]

The Minnesota State Lawyers Professional Responsibility Board appears to agree with the ABA's optimistic conclusions about the security of e-mail communications.[87] In a comment to Opinion 19, the Board states that "[t]his opinion reflects the prevalent view of other states and technology experts, that communications by facsimile, e-mail, and digital cordless or cellular phones, like those by mail and conventional corded telephone, generally are considered secure."[88] In the same vein, one commentator suggests that attorneys "worry too much" about

81. *Id*.

82. *Id*. (emphasis added).

83. *See* United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003); United States v. Ross, 713 F.2d 389, 391 (8th Cir. 1983); Wesley Coll. v. Pitts, 974 F. Supp. 375, 389 (Del. 1997), *aff'd*, 172 F.3d 861 (3d Cir. 1998).

84. *Compare* Formal Op. 99-413, *supra* note 80 (applying the ECPA to "dissemination" independent of "interception"), *with* 18 U.S.C. § 2511(1)(c)–(e) (2000) (addressing "disclosure" of *intercepted* information).

85. Formal Op. 99-413, *supra* note 80.

86. *Id*. (noting that e-mail should be avoided in situations that similarly "warrant the avoidance of the telephone, fax, and mail").

87. Minn. Ethics Op. 19, *supra* note 18.

88. *Id*.

Internet security,[89] but, much like ABA Opinion 99-413,[90] these aging and naïve conclusions fail to consider the reality of e-mail insecurity.

Despite this insecurity, an e-mail disclaimer as a claim of privilege has merit on its own. For example, in *United States v. Neill*, the D.C. District Court found that a lack of evidence demonstrating that the defendant asserted a claim of privilege with respect to computer files precluded a later assertion of privilege.[91] Under this rule, a disclaimer referencing privilege may insulate e-mail files from a default waiver of privilege.

Among the various duty-based reasons for ensuring the privacy of an e-mail, maintaining attorney-client privilege is clearly of special importance to the legal community. Nonetheless, there is no explicit requirement or recognition of e-mail privacy disclaimers. In the face of a seemingly ethereal legal foundation, a prudent e-mail disclaimer user should take advantage of whatever means are available to strengthen the disclaimer's effect.

III. STRENGTHENING THE BARK

The "bark" of the disclaimer refers to its general effect independent of its legal underpinning. Even without a specific legal foundation,[92] disclaimers may arguably serve deterrent purposes through either the benevolence of others or fear of retribution.[93] As a tool to limit dissemination of private information, any warning should prove effective to a friendly recipient. However, some approaches to disclaimer usage are likely to be more effective than others.

A. PLACEMENT

The placement of a privacy disclaimer logically has an impact on whether it is read before the recipient can "violate" its provisions. Nonetheless, most users place disclaimers of all

89. Anderson, *supra* note 4, at 7.

90. Formal Op. 99-413, *supra* note 80.

91. United States v. Neill, 952 F. Supp. 834, 842 (D.D.C. 1997).

92. *See, e.g.*, STEVEN E. MILLER, CIVILIZING CYBERSPACE: POLICY, POWER, AND THE INFORMATION SUPERHIGHWAY 362 (1996) ("The status of email is still in a state of legal confusion.").

93. *See* BRUCE SCHNEIER, E-MAIL SECURITY: HOW TO KEEP YOUR ELECTRONIC MESSAGES PRIVATE 3 (1995) ("[T]he only security anyone has is based on the honesty, ignorance, and indifference of those at the intermediate points.").

kinds at the end of their messages.[94] This practice brings the effectiveness of such appended disclaimers into question. "One cannot unring a bell"; after the content of the e-mail is read, the damage is done.[95]

Sensible practice would place the disclaimer at the beginning of the document where readers are more likely to read it *before* they read the contents.[96] This practice would better conform with the use of similar disclaimers in other forms of communication. For asserting attorney-client privilege, an additional notice could be placed in the subject line indicating that the message is a privileged communication.[97]

For maximum effectiveness, a user should place private information into a separate e-mail attachment.[98] The body of the e-mail should contain only the disclaimer. The disclaimer should also appear at the top of the attached document. Users of this practice may encounter difficulties if different word-processor programs are incompatible. However, a user may easily alleviate this problem through the use of a format that has a universal reader available, such as the portable document file (PDF) or rich-text format.

Employing these practices would maximize the likelihood that the recipient notices and reads the disclaimer, regardless of whether the disclaimer is enforceable. Prominence and early placement create the greatest likelihood that an unintended recipient will comply with a disclaimer.

B. AUTOMATION

The practice of placing the disclaimer at the end of the message[99] is logically related to a tendency to simplify the disclaimer's inclusion. Some law firms even configure their computer systems to automatically place their own disclaimer at

94. Krause, *supra* note 5, at 28–29.

95. Talton, *supra* note 4, at 292.

96. *See* Thompson et al., *supra* note 17, at 877; Krause, *supra* note 5, at 28–29 (comparing e-mail disclaimers which typically appear at the end of the message to fax disclaimers that typically appear before the message).

97. JONATHAN BICK, 101 THINGS YOU NEED TO KNOW ABOUT INTERNET LAW 32 (2000).

98. *See* Talton, *supra* note 4, at 304.

99. *See, e.g.*, MONICA SEELEY & GERARD HARGREAVES, MANAGING IN THE EMAIL OFFICE 119 (2003) (advising organizations and individuals to "[s]et up your software's signature feature to add letterhead details and any disclaimer to your messages automatically").

the end of every outgoing e-mail message.[100] Though admittedly efficient, this approach may pose the greatest barrier to disclaimer effectiveness and enforceability.

For commercial e-mail clients[101] on the market today, the only way for an ordinary user to include text automatically in every message is to use a "signature." As the name suggests, e-mail clients provide an option to append a signature automatically to the end of a message.[102] This practice makes sense if one considers that software developers originally designed this feature to communicate a sender's contact information.[103] However, the automated signature feature is wholly inadequate for disclaimers. Until software designers create a plausible option to automatically insert text at the beginning of a message, tension will remain between the convenience of automation and the prudence of effective disclaimer placement.

Authors who are opposed to automation believe that these types of disclaimers are meaningless to a court if a user includes them on every communication,[104] including lunch appointments.[105] Over-inclusion, they argue, can only result in a dilution of the already questionable legal meaning of e-mail disclaimers.[106]

The possibility and potential consequences of forgetting a disclaimer on a single critical e-mail weighs heavily in favor of using automatic signatures to communicate disclaimers.[107] However, the possibility that overuse may indiscriminately invalidate the same disclaimer on *all* of a user's e-mail messages

100. Krause, *supra* note 5, at 29.

101. In this context a "client" is a software program used to interact with a server, such as an e-mail server. *See* JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH FEATURING THE INTERNET 10–11 (2d ed. 2003).

102. *See* Microsoft Office Assistance, About Signatures in Messages, http://office.microsoft.com/en-us/assistance/HP052427451033.aspx (last visited Oct. 19, 2006) (defining "e-mail signature" as "text and/or pictures that are automatically added to the end of an outgoing e-mail message").

103. Microsoft Office Online, Format E-mail Messages for Clarity, http://office.microsoft.com/en-us/FX011456181033.aspx (last visited Oct. 19, 2006) (suggesting that "the first place [e-mail recipients] look for your contact information is in the signature line at the end of your message" and that "[e]-mail message signatures should display complete contact data, including name, title, phone numbers, organization, and Web site address").

104. *See* Thompson et al., *supra* note 17, at 877.

105. *See* Krause, *supra* note 5, at 29.

106. Pallasch, *supra* note 16, at 15.

107. *Id.*

is far more devastating and should be sufficient to dissuade the average user from giving in to the simplistic appeal of automation.[108]

C. PLAUSIBLE COMPLIANCE

Two considerable issues arise when evaluating the plausibility of a recipient's compliance with the common provisions of an e-mail disclaimer. First, the recipient must determine the identity of the *intended* recipient.[109] Second, if a recipient resolves that he is not the intended recipient, he must delete the message from his system.[110] Because of the informal nature of e-mail,[111] ascertaining the true intention of the sender may be quite difficult. Clearly, a greeting containing a name other than the name of the recipient indicates that a message is intended for someone else. However, a brief message between two well-acquainted parties may not contain any information identifying the sender other than his e-mail address, let alone an indication of the intended recipient. In order to maximize the effect of a request to determine the intended recipient, senders should make the identity of their intended recipients unequivocally clear in the body of messages.

Realistically, senders have no control over the actions of e-mail recipients after receipt.[112] What is worse, even if recipients follow instructions to delete the e-mail, multiple copies of the e-mail's contents will likely remain elsewhere on the recipients' systems.[113] Therefore, the expectations associated with a disclaimer's request for deletion are also unrealistic in practice.

Through changes in placement and usage, users may be

108. *See* Thompson et al., *supra* note 17, at 877.

109. *See* Krause, *supra* note 5, at 28–29 (observing that the text of disclaimers typically claims that "[t]he above e-mail is for the intended recipient only").

110. *See, e.g.*, TD Bank Financial Group, Legal Notices and Disclaimers of Liability, http://www.td.com/legal/index.jsp (last visited Oct. 19, 2006) ("If you receive this communication in error . . . permanently delete the entire communication from any computer, disk drive, or other storage medium.").

111. OVERLY, *supra* note 3, at 11 (noting that the incorrectly perceived impermanence of e-mail is one reason people treat it so informally).

112. *See id.* at 12. ("[Y]ou have no control over whether that person keeps your message confidential or circulates it to any number of other people—or posts it on the Internet, where it may be viewed by thousands of people.").

113. *Id.* at 11 ("People wrongly believe that if they delete a piece of e-mail it is gone forever."); *see also* A.B.A. DIV. FOR MEDIA RELATIONS & COMMC'N. SERVS., FACTS ABOUT PRIVACY & CYBERSPACE 13 (1999) ("Deleted e-mail is often archived on tape and stored for years (deleting does not really delete).").

able to bolster the effect of e-mail disclaimers that contain reasonable provisions. However, without some legal support for e-mail privacy, a disclaimer is nothing more than a hollow threat. While changes to the law are the most straightforward means of increasing legal support, alternatives exist.

IV. STRENGTHENING THE BITE

The "bite" of an e-mail disclaimer refers to the actual legal impact of and obstacles to noncompliance. Two categories of e-mail disclaimer bites exist: prevention and punishment. Effective prevention measures are proactive and preclude the unintended recipient from disobeying the provisions of a disclaimer. In contrast, effective punishment measures are reactive and provide remedies or disincentives for the disobedient recipient.

A. PREVENTION

Two proactive privacy measures are presently available to users. First, recent advances in e-mail encryption software have made encryption a plausible way to maintain privacy at a reasonably high success rate.[114] A second and much less immediate option involves introducing better e-mail standards. If one of these options is adopted, it is likely that the other will be as well.

1. Encryption

Because of its effectiveness both in transit and after delivery, encryption is a powerful means of securing e-mail communications.[115] Moreover, an encrypted message maintains privacy while requiring compliance on the part of an unintended recipient.[116] Encryption involves scrambling a message before dispatch[117] and transmitting the scrambled message to recipients who have unique keys that allow them to unscramble the message. In fact, deciphering a message coded by modern encryption without a key can be so difficult that it takes a high-

114. *See* SEELEY & HARGREAVES, *supra* note 99, at 201 ("[Encryption software] is a relatively mature, albeit underused, form of email management.").

115. Talton, *supra* note 4, at 284.

116. *See* LILIAN EDWARDS & CHARLOTTE WAELDE, LAW & THE INTERNET: REGULATING CYBERSPACE 141–47 (1997).

117. BICK, *supra* note 97, at 32 (explaining that encryption effectively renders a message "unintelligible to all those but the intended recipient").

speed computer years of computing to solve.[118] In addition to the added security encryption provides, the extra steps of scrambling and unscrambling allow for a more formal system of providing proof of receipt.[119]

Today's encryption software employs "public key" cryptography to encode and decode messages.[120] To decrypt encrypted e-mail messages, a user must acquire two keys: a public key and a private key.[121] As the names suggest, users give their public keys to whomever they want to send encrypted messages and keep their private keys secret.[122] After the public key is distributed, senders use it to encrypt messages to users, who decrypt all of the messages with their private keys.[123]

A popular analogy explains encryption as a system of metal boxes and padlocks.[124] The user distributes metal boxes and open padlocks (the public keys).[125] The user has a special key (the private key) that opens all of the padlocks.[126] Only the user has the private key, so once the senders lock their padlocks, only the user can access the contents.[127]

Upon such a straightforward explanation, one begins to ponder how something as simple as acquiring a few keys and giving them to a user's contacts is an obstacle to the widespread adoption of something so secure. Consider, then, having to maintain a different key for every e-mail contact. For many users, that would be one very large, and very confusing, key

118. DOUGLAS E. COMER, THE INTERNET BOOK 290 (3d ed. 2000).

119. NANCY FLYNN & RANDOLPH KAHN, E-MAIL RULES 175 (2003).

120. *See* Tim Greene, *Sun, Lucent Tout Encrypted E-mail Service*, NETWORK WORLD, Nov. 21, 2005, at 40, 40; COMER, *supra* note 118, at 288–94 (providing a basic overview of the e-mail encryption process).

121. SCHNEIER, *supra* note 93, at 24 (explaining that typical encryption keys are between 40 and 128 bits long, or 13 to 40 decimal digits).

122. *Id.* at 42.

123. COMER, *supra* note 118, at 291.

124. *See, e.g.*, Cornell Univ., Primes, Modular Arithmetic, and Public Key Cryptography II (2004), http://www.math.cornell.edu/~mec/2003-2004/cryptography/RSA/RSA.html (last visited Oct. 19, 2006); Open2.net, Mathematical Thinking, http://www.open2.net/sciencetechnologynature/maths/primer.html (last visited Oct. 19, 2006); Univ. San Francisco Cal., Public Key Encryption, http://www.cs.usfca.edu/~parrt/course/601/lectures/public.keys.html (last visited Oct. 19, 2006).

125. *See* Cornell Univ., Primes, Modular Arithmetic, and Public Key Cryptography II, *supra* note 124.

126. *Id.*

127. *Id.*

ring.[128] Until recently, the costs of managing such key rings were prohibitive.[129]

A growing number of software developers have introduced encryption suites that dramatically reduce the cost and complexity of the encryption process.[130] Transparency is crucial, as even contemplating the actual processes behind encryption can unnerve a computer scientist, not to mention the average user.[131] With many current products, key management is completely automated and takes place behind the scenes.[132] Similarly, developers have also simplified the process of enabling encryption for a particular e-mail message. For one product, "[e]nd users wishing to encrypt a message type the trigger word 'secure' in the subject line before hitting the send button."[133] Another tool actually "scans the e-mail's text and attachments and looks for combinations of words and numbers that look like it's going to be [confidential] information."[134] In a 2005 evaluation of available e-mail encryption suites, the University of Kansas's manager of Local Area Network Support Services commented that "[a]ll the products proved to [the evaluators] that getting started with e-mail encryption is much easier than [one] might think."[135]

Despite these recent advances in the software industry, electronic communications experts suggest that "[f]ew organizations employ e-mail encryption technology broadly enough."[136] One commentator goes so far as to direct his read-

128. Rhonda M. Jenkins & Jack Seward, Protecting Your Digital Assets: Overcoming E-mail Insecurity, http://www.hp.com/sbso/solutions/legal/expert_insights_protecting_digital_assets.html (last visited Jan. 5, 2006) (commenting that it would be "difficult to keep track of the many digital keys necessary to lock and unlock the volumes of encrypted messages").

129. *See id.* (explaining that server-based e-mail solutions offering enterprise-level domain-to-domain encryption between attorney and client locations are costly and complex to implement).

130. *See* Travis Berkley, *CipherTrust Tops Encryption Field*, NETWORK WORLD, Aug. 15, 2005, at 39, 41. *See generally* Electronic Privacy Information Center, EPIC Online Guide to Practical Privacy Tools, http://www.epic.org/privacy/tools.html (last visited Oct. 19, 2006) (providing a non-exhaustive listing of available e-mail encryption programs).

131. Berkley, *supra* note 130.

132. *See, e.g.*, SCHNEIER, *supra* note 93, at 44, 208.

133. Paul McNamara, *You've Got Mail*, NETWORK WORLD, Aug. 15, 2005, at 36, 38.

134. *Id.*

135. Berkley, *supra* note 130, at 45.

136. FLYNN & KAHN, *supra* note 119, at 174.

ers to "not use the Internet for communication of confidential information unless it is encrypted."[137] In his analysis, he states that "it is generally agreed that a lawyer's failure to use security technology could be construed as a failure to take reasonable precautions."[138]

As far as lawyers are concerned, however, the courts have yet to find that communication via unencrypted e-mail exhibits an intention to disclose information to a privilege-destroying third party.[139] In fact, Bar Association committees have found precisely the opposite. For example, the Illinois State Bar Association and the D.C. Bar Legal Ethics Committee explicitly decided to allow transmission of confidential information by unencrypted electronic mail in 1997 and 1998, respectively.[140]

Because of the widespread trend toward accepting unsecured e-mail as a secure method of communication, a change in the disposition of the various bar ethics committees will likely occur only after a vast majority of the legal community starts to employ encryption. This change may already be in progress, as almost one-third of large firms recently reported using encryption to secure client e-mail messages.[141] A cautious user, whether a lawyer or a private individual, should thoroughly consider using encryption, especially for particularly sensitive communications.

2. Introducing New E-mail Standards

The introduction of e-mail standards is a potential alternative to using encryption as a preventative measure. For example, many companies are adopting a "'bright-line' no-forwarding policy" in order to avoid the complications of dealing with unauthorized forwarding.[142] Such a policy reduces liability and provides a sense of security to those who send e-mail to persons

137. BICK, *supra* note 97, at 32.

138. *Id*. at 31.

139. Thompson et al., *supra* note 17, at 871–72 (citing Mitchell v. Towne, 87 P.2d 908 (1939)).

140. D.C. Bar Legal Ethics Comm., Op. 281 (1998), available at http://www.dcbar.org/attorney_resources/opinions (discussing ethical implications of using encryption and stating that encryption is not ethically mandated); Ill. State Bar Ass'n, Op. 96-10 (1997), *available at* http://www.illinoisbar.org/CourtsBull/EthicsOpinions (discussing electronic communication, the use of encryption, and ethical implications); *see also* Ohio Bd. of Comm'rs on Grievance & Discipline, Op. 99-2 (1999).

141. *See* REACH ET AL., *supra* note 3, at 13.

142. *See* OVERLY, *supra* note 3, at 17.

within the organization. Other e-policy experts advocate a sweeping requirement of obtaining the original sender's permission before forwarding an e-mail.[143] This approach holds the additional advantage of curbing unauthorized forwarding without eliminating forwards entirely. Alternatively, a universal shift from placing disclaimers at the end of a message to placing them at the top may improve efficacy.

B. PUNISHMENT

While the sender can easily apply most prevention measures himself or herself, punishment options are more cumbersome to implement. Unfortunately, Congress appears unlikely to implement most proposed Internet legislation.[144] Despite this record, claims that existing law is sufficient underestimate the limitations of the ECPA and other allegedly applicable statutes.

Much of the existing policy regarding e-mail security assumes that "intercepting an electronic mail message is illegal under the ECPA."[145] However, the threat of interception is much less troublesome compared to the threats of dissemination to unintended third parties through disclosure or unauthorized forwarding by a recipient.[146]

In enacting the ECPA, the Senate Judiciary committee exhibited intent to prevent unauthorized opening of e-mail analogous to the protections afforded to first class postal mail.[147] The law protects first class mail from unauthorized opening until it reaches the directed recipient, even while it sits in the mailbox after delivery.[148] Yet, through its express limited application to

143. FLYNN, *supra* note 23, at 92 ("A confidential email message intended for a single reader could have a negative impact on the original sender if forwarded to additional, unintended readers.").

144. BICK, *supra* note 97, at 101.

145. Ill. State Bar Ass'n, *supra* note 140.

146. Claire A. Simmers & Adam Bosnian, *Reducing Legal, Financial and Operational Risks: A Comparative Discussion of Aligning Internet Usage with Business Priorities Through Internet Policy Management*, *in* MANAGING WEB USAGE IN THE WORKPLACE 270, 279 (Murugan Anandarajan & Claire Simmers eds., 2002) (discussing Twentieth Century Fox's perception that "one keystroke could result in the loss of a confidential movie/TV script or contract detail").

147. S. REP. NO. 99-541, at 5 (1986).

148. United States v. Palmer, 864 F.2d 524 (7th Cir. 1988) (finding that the ECPA prohibits a person from taking a letter before it has been delivered to the person to whom it has been directed, even when the address may be outdated or incorrect).

communications interception, the ECPA does not afford this presumed protection to e-mail messages[149] and therefore fails to fulfill congressional intent to place e-mail on the same privacy footing as first class mail.

Though requiring the original sender's permission to disseminate an electronic message would eliminate the threat of unauthorized forwarding, such a provision would fall outside the original intent of the ECPA and would require new justification.[150] In fact, postal mail forwards are presently subject to the same laws as e-mail forwards. The only difference is that e-mail forwards are not subject to the physical limitations that accompany the copying of a letter, and therefore they require additional limitations to achieve the same effect. Though unlikely,[151] either a change in e-mail industry standards or a congressional amendment of the ECPA to ban unauthorized forwarding would achieve this effect.

In order to realistically extend to e-mail the same level of protection as first class mail regarding delivery to the correct recipient, e-mail addresses and recipient names would both need to be required separately, much like how both an address and the name of a recipient are required on an envelope. Such a separation would greatly clarify the intent of the sender[152] and would enable compliance with currently ineffective disclaimer provisions. When combined with a statutory extension of first-class mail protections to e-mail, the security of e-mail messages would be greatly increased.

CONCLUSION

The initial tepid response of the legal profession to client communication over e-mail is understandable. Despite a lack of advancements in the security of standard e-mail, the legal profession has nonetheless embraced e-mail as an acceptable means of communication. With the lawyers came the confidentiality disclaimers, which are presently toothless outside the attorney-client privilege context. A more personal "please don't copy or forward this" statement likely better serves most non-lawyers.

149. *See* S. REP. NO. 99-541, at 5 (1986).
150. *See id.*
151. BICK, *supra* note 97, at 101.
152. *See* Krause, *supra* note 5, at 28–29.

In addition, the means of use of e-mail disclaimers has been more a creature of convenience than of functionality. The limitations of existing technology have sacrificed effectiveness. Unless Congress takes new steps to increase the effectiveness and enforceability of modern e-mail disclaimers, encryption is a reasonable and substantially more effective alternative privacy tool.

The proposals outlined in this Note are sensible and practical extensions of existing law and policy that will better align practice with perception. Congress can additionally secure e-mail through just a few slight changes in policy, without substantial deviation from the spirit of the ECPA. Not only will the lessened threat of unauthorized e-mail dissemination expand the marketplace of ideas, but existing disclaimers will also become more effective as the intended recipient becomes more evident.