SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Law Review

Volume 48 | Issue 2 Article 5

1998

Electronic Mail and Confidential Client-Attorney Communications: Risk Management

Colleen L. Rest

NOTES

ELECTRONIC MAIL AND CONFIDENTIAL CLIENT-ATTORNEY COMMUNICATIONS: RISK MANAGEMENT

INTRODUCTION

Automation of communication in the legal community has generally been met with resistance.[1] The legal community, like society as a whole, is uncomfortable with change.[2] Moreover, attorneys are resistant to automation of communication because of their duties to maintain the confidentiality of client-attorney communications. These duties require the placement of strong controls over communications. When automation occurs, a sense that control cannot be maintained provides a basis for heightened resistance.[3]

New communication technologies that provide sufficient benefits to the profession must be, and eventually are, accepted by the legal community even though confidentiality concerns exist. The entrance of the telegraph into the profession provides an example.[4]

---

[1] *See* JAMES MILLES, INTERNET HANDBOOK FOR LAW LIBRARIANS 1 (1993) (quoting Paul Bernstein, *Bulletin-Board Systems Hold Accessible Pools of Information*, NAT'L L.J., Apr. 7, 1986, at 15). Milles wrote:

> The history of electronic communication in the legal . . . profession[] has not always been one of enthusiastic embrace of innovation. The story is told that "many years ago, one of the largest New York law firms would not allow a new invention, the telephone, to be anywhere in its office except in the reception area, where it was kept to show clients how advanced and up-to-date the firm was."

Id.

[2] "Attorneys are most comfortable when conservative. Either they want to do it the old way, or they want to see a herd doing it the new way." BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE 36 (1991).

[3] *See* David Andrews, *The Legal Challenge Posed by the New Technologies*, 24 JURIMETRICS J. 43, 43 (1983).

[4] *See* MORRIS GRAY, A TREATISE ON COMMUNICATION BY TELEGRAPH 1 (1885)

When faced with the introduction of the telegraph, attorneys were concerned about confidentiality: How could confidentiality be protected when interception of telegraphic messages was possible?[5] Attorneys were also concerned about the applicability of the attorney-client privilege to telegraphic messages: Could the privilege apply when the nature of the telegraph required that a third party be exposed to the contents of the confidential communication?[6] Lawyers pondered these questions but were simultaneously aware that rejecting the use of the telegraph outright, because of a failure to understand how to control it, would not be efficient or profitable. The United States Supreme Court recognized that the telegraph was an "indispensable means of communication."[7] Lawyers responded by using the technology cautiously. The profession assessed the telegraph's capability to carry confidential information and established controls. One author created a substantial legal telegraphic code that "enable[d] lawyers to transmit telegraphic messages in their own legal phraseology, secretly. . . ."[8]

The legal community no longer uses the telegraph, but must never discontinue its assessment of new communication technologies for their ability to carry confidential information. The legal community must continue to develop controls over beneficial technologies to enable their use in spite of their weaknesses.

This Note performs such an assessment, and suggests a control with respect to another technology that is becoming an indispensable means of communication: electronic mail (e-mail).[9] The concern of this Note is whether e-mail should be used by the legal profession to carry confidential[10] communications.

A three inquiry risk management approach is adopted to guide

(defining the telegraph as "an apparatus, or a machine, used to transmit intelligence to a distance with the aid of electricity").

5. *See* NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE, COMMISSION STUDIES 2 (1976) [hereinafter NATIONAL COMMISSION]. "Wiretapping as a technological improvement on simple eavesdropping by the unaided ear came into being soon after the invention of the telegraph. Opposing forces in the Civil War tapped telegraph lines for military intelligence." *Id.*

6. *See* GRAY, *supra* note 4, at 206-17.

7. *Id.* at 210; *see* Pensacola Tel. Co. v. Western Union Tel. Co., 96 U.S. 1 (1877). "The electric telegraph marks an epoch in the progress of time. . . . It is indispensable as a means of inter-communication." *Id.* at 9.

8. Legal Code Corp., *Preface* to FRANK W. HELLER, LEGAL TELEGRAPHIC CODE v (1925).

9. For a definition of electronic mail, see *infra* note 25 and accompanying text.

10. The definition of confidential, as used in this Note, depends upon whether the reader's state is a jurisdiction that has adopted the Model Rules of Professional Conduct or a jurisdiction that has adopted the Model Code of Professional Responsibility. For a definition based upon the Model Rules, see *infra* note 87 and accompanying text. For a definition in a Model Code jurisdiction, see *infra* note 88 and accompanying text.

the analysis.[11] The first inquiry is whether e-mail is a risk management category.[12] This examination looks at the technology of electronic mailing, the limitations of the technology, and the relationship of the technological limitations to attorneys' current and potential use of e-mail. This section concludes that although beneficial to the attorney, the use of electronic mail to carry confidential client-attorney communications is risky.

The second inquiry is whether systems and procedures exist that reduce or attempt to reduce the risks associated with electronic mail.[13] This inquiry examines technological and legal systems and procedures that are available to the legal community to control the risks identified in the first inquiry.[14]

The third inquiry asks what strategy should be developed to control the risks that fall outside the protections identified in the second inquiry.[15] Some members of the legal community suggest that whether or not a duty exists, the e-mail using attorney should secure communications with technology. Another member of the legal community suggests that the legal systems in place provide sufficient protection for the attorney. To him, the use of security technology is solely a matter of business judgment. This Note concludes that an affirmative duty be placed on the attorney, but not an affirmative duty specifically to use security technology. Bar association ethics panels should recognize in their formal opinions a general duty of the attorney to take reasonable steps to protect client confidences in e-mail messages. Such a control will inevitably force the legal community to develop a professional standard of using security technology, without discouraging the use of electronic mail. The approach is also adaptable to the changing telecommunications frontier.

I. IDENTIFYING E-MAIL AS A RISK MANAGEMENT CATEGORY

The first step in assessing whether e-mail should be used by the legal community to carry confidential communications is examining whether the use of e-mail is a risk management category.[16] Identification of an element of legal practice as a risk management category denotes that the element has some risky characteristics. In other words, associated with the element there are "danger[s] that, if not controlled, may lead to . . . consequence[s] unintended by

---

[11] *See* ANTHONY E. DAVIS, RISK MANAGEMENT (1995) (suggesting law firms adopt risk management procedures).

[12] *See infra* Part II.

[13] *See* DAVIS, *supra* note 11, at 22.

[14] *See infra* Part III.

[15] *See* DAVIS, *supra* note 11, at 22; *infra* Part IV.

[16] *See* DAVIS, *supra* note 11, at 22.

and actually or potentially harmful to a law firm or practitioner."[17]

One element of practice readily defined as a risk management category is client intake.[18] A danger associated with this element of practice is failing to discover a conflict of interest before accepting a client. If the danger materializes and a conflict of interest is not discovered, disqualification from representation[19] or disciplinary sanctions[20] may ensue. These consequences are harmful to the law firm or practitioner and therefore risk management categorization is appropriate. A second example is docket and calendar management.[21] The danger associated with this element of practice is missing a statute of limitations. Failure to observe a statute of limitations is potentially harmful to the practitioner or law firm as it may lead to an attorney malpractice claim.[22] Docket and calendar management is therefore also appropriately recognized as a risk management category.

Is communicating confidential information via e-mail likewise deserving of risk management categorization? Lost confidentiality is a danger associated with using e-mail.[23] If the danger materializes and confidentiality is lost, disciplinary sanctions, a legal malpractice suit, and waiver of the attorney-client privilege may ensue.[24] Thus, risk management categorization of e-mail usage is appropriate. The danger of e-mail, if not controlled, may lead to consequences that are unintended by, and potentially harmful to the legal community.

A. How Confidentiality is Lost: E-Mail Technology

E-mail is a method of message exchange that enables users to communicate with one another noninteractively when their computers are connected.[25] E-mail capabilities depend not only on users,

---

17. *Id.* at 15.

18. *See id.* at 25-28.

19. *See* Cannon v. United States Acoustics Corp., 398 F. Supp. 209 (N.D. Ill. 1975) (disqualifying an attorney, due to potential conflict of interest, from representing a corporation as well as its shareholders in a derivative suit), *aff'd in part and rev'd in part on other grounds*, 532 F.2d 1118 (7th Cir. 1976).

20. *See* Columbus Bar Ass'n v. Grelle, 237 N.E.2d 298 (Ohio 1968) (upholding an attorney reprimand for representation of clients with conflicting interests).

21. *See* DAVIS, *supra* note 11, at 32.

22. *See id.* at 117.

23. To demonstrate, this Note discusses e-mail technology and the technology's limitations. *See infra* Part II.A.

24. The ethical and legal principles that guide the client-attorney relationship establish these consequences. *See infra* Part II.C.

25. *See* James R. Neill, *Electronic Mail, in* 1 MACMILLAN ENCYCLOPEDIA OF COMPUTERS 353 (Gary G. Bitter ed., 1992). Other definitions of electronic mail include "[c]orrespondence that is transmitted from one computer terminal to another through data communications lines," LINDA GAIL CHRISTIE & JOHN CHRISTIE, THE ENCYCLOPEDIA OF MICROCOMPUTER TERMINOLOGY (1984), and "a way for computer users to exchange mes-

but on two different technologies: networks, the means by which computers are connected,[26] and store-and-forward technology, facilitating the noninteractive nature of e-mail.[27]

1. Networks

Initially it is important to understand that although one has electronic mailing capabilities, he or she cannot by default reach any individual with an electronic mail address.[28] Internal electronic mail systems exist which allow individuals in an enterprise to e-mail only one another.[29] An internal system typically relies on a local area network (LAN)[30] and has no connection to networks outside of the enterprise. The result is one type of *closed* network; connections are limited to a predefined population,[31] such as all lawyers in one law firm. Security problems exist under this type of system[32] but security concerns such as third party eavesdropping, hacking,[33] or mistakenly sending documents to parties with adverse interests are not as acute, absent insider espionage. Internal e-mail systems are therefore not the focus of this Note.

Internal e-mail systems are to be compared with external e-mail systems, which allow the sending and receiving of e-mail outside the enterprise.[34] External electronic messaging allows the attorney to send e-mail to clients, to peers in other law firms, or to anyone connected to the lawyer's network. Increasingly, external e-mail is accomplished through connection of the office LAN to the Internet.[35]

"The Internet is an international network of computers and

---

sages," DANIEL P. DERN, THE INTERNET GUIDE FOR NEW USERS 130 (1994).

[26] "Networks connect computers to each other." HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY 4 (1996) (emphasis omitted).

[27] *See infra* note 51 and accompanying text.

[28] *See* Charles R. Merrill, *E-Mail for Attorneys from A to Z*, N.Y. ST. B.J., May-June 1996, at 20, 20.

[29] *See id.*

[30] *See* PERRITT, *supra* note 26, at 4 (noting that LAN's electrically connect from two to hundreds of computers within geographical proximity of one another).

[31] *See id.* at 5.

[32] Insider fraud, insider misuse of databases, and evidence tampering are three examples of misuse by authorized personnel. *See* PETER G. NEUMANN, COMPUTER-RELATED RISKS 142 (1995).

[33] "Hacking as a methodology to achieve some particular goal implies working at something by experimentation or empirical means, learning about the process under review or development by ad hoc mechanisms." J.A.N. Lee, *Hacking*, *in* 1 MACMILLAN ENCYCLOPEDIA OF COMPUTERS 425, 425 (Gary G. Bitter ed., 1992). One author suggested categorizing hackers by their activities, defining the novice, student, and tourist as those users who visit sites and learn about hacking. The crasher and thief are intruders interested in bringing harm to the systems they hack. *See id.* at 430.

[34] *See* Merrill, *supra* note 28, at 21.

[35] *See* DERN, *supra* note 25.

computer networks,"[36] and the user will notice little difference between internal and Internet based external e-mailing.[37] There are greater security concerns with external message exchange, though, because the Internet is an *open* network;[38] there is no predefined class of potential users.[39] The open nature of the Internet creates security risks because of system interconnectivity.[40] The Internet works because many different networks agreed to tie themselves together and share data.[41] An e-mail message may travel through computers in several states or several countries before arriving at its intended recipient's computer.[42] However, "[i]nterconnection results in the vulnerability of weak links endangering other parts of an interconnected system. This phenomenon is particularly insidious when different parts of a system fall under different managements with different assessments of risk."[43] The Internet's use of many different systems and many different computers limits the user's level of security to the level of security used by the networks with which it communicates.[44] Community vulnerability is thus a security issue inherent in networks.

Packet switching, the technology that enables the transfer of data from one computer to another, does provide some security.[45] All data transmitted across networks is broken into chunks, called

---

[36] PERRITT, *supra* note 26, at 5 (emphasis omitted).

[37] One difference users will typically encounter is the addressing format of messages. There are three pieces of an electronic mail address: the user name, the system, and the domain. Users of an internal network need only the user name when addressing messages to one another. Once e-mail extends outside the enterprise and across networks, though, the system and domain of the recipient's network need to be included. For example, an individual named Sue E. Smith attending Case Western Reserve University can be contacted by e-mail by other Case students at an address such as SES. If Sue was being e-mailed by an individual without an e-mail account at Case, the sender would have to address the message to SES@po.CWRU.edu. *See* Jim Burton, *How to E-Mail Anyone From Anywhere*, THE NET, Sept. 1995, at 73, 73.

[38] *See* PERRITT, *supra* note 26, at 5. "The Internet is the archetypal open network." *Id.*

[39] *See id.*

[40] *See* NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK 63 (1991). The Internet was not developed with security in mind. The precursor to the Internet was developed by the Department of Defense (DOD) in 1969, and a key basis for the network's development was national security. The DOD was attempting to develop a system of communication that would withstand enemy attack, able to automatically reroute communications if the route the communication was taking was disturbed by enemy attack. *See* JOHN R. LEVINE & CAROL BAROUDI, THE INTERNET FOR DUMMIES 11-12 (1993).

[41] *See* Jon Phillips, *How Your Data Snakes Across the Internet*, THE NET, Sept. 1996, at 45.

[42] *See id.* at 45-47.

[43] NATIONAL RESEARCH COUNCIL, *supra* note 40, at 63.

[44] *See* DERN, *supra* note 25, at 380.

[45] Packet switching is usually achieved in an external e-mail system with a set of two protocols, TCP/IP (Transmission Control Protocol/Internet Protocol). *See* Phillips, *supra* note 41, at 44.

packets, by the protocols in the sender's e-mail software. The packets are then reassembled by the receiver's e-mail software.[46]

The process of packet switching offers security because it is very difficult for a snoop to track each specific piece (packet) of the e-mail while it is in transmission, intercept it, and reassemble the message.[47] However, packet switching is not the complete solution to network insecurity because although a difficult process, packet interception is possible. One estimate indicates that 100,000 system passwords were stolen in 1994 through listening to network packets, leaving many password protected systems vulnerable to attack by unauthorized individuals.[48]

2. Store-and-Forward Technology

Electronic mail transmission also depends on store-and-forward technology.[49] Because electronic mail must travel through several computers to reach its intended recipient, store-and-forward technology is used to ensure message arrival. "[W]hen a mail server receives a[n electronic] message, it makes a copy (stores it) and then does its best to pass it along (forward it). (The stored copy is deleted after the receiving computer confirms receipt.)"[50]

Store-and-forward technology enables electronic mail to be considered a "non-real-time" or "noninteractive" application.[51] Unlike a telephone conversation, which relies on "real-time" response and interaction, store-and-forward technology allows electronic mail to wait for the intended recipient to retrieve it (similar to voice mail).

---

[46] *See id.* The internet protocol inserts into each data packet the address to the intended recipient's computer. Transfer control protocol then marks each packet with a sequence number and "[w]hen the packets reach their destination . . . reassembles them according to their sequence numbers. . . . If a specific packet is missing or corrupted, TCP will request that it be resent." *Id.* The following excerpt, analogizing a packet switched network to the United States Postal System, clarifies this point:

> Let's say that you have a close friend in the island nation of Papua New Guinea, to whom you want to send a copy of the manuscript for your new and very long book. . . . Unfortunately, the manuscript weighs 15 pounds, and the limit on packages to Papua New Guinea, is 1 pound. So you divide the manuscript into 15 pieces and on each package you write something like *PART 3 OF 15* and send them off. When the packages eventually arrive, probably not in the right order, your friend takes all the pieces, puts them back in order, and reads them. [N]etworks . . . work pretty much the same way.

LEVINE & BAROUDI, *supra* note 40, at 56-57.

[47] *See* G. Burgess Allison, *Technology Update* (visited Oct. 21, 1996) <http://www.abanet.org/lpm/magazine/tu963.html#tag0>.

[48] *See* FREDERICK B. COHEN, PROTECTION AND SECURITY ON THE INFORMATION SUPERHIGHWAY 75 (1995).

[49] *See* DERN, *supra* note 25, at 136.

[50] *Id.*

[51] *See id.*

Although store-and-forward technology provides benefits to the user,[52] there are security concerns raised by the technology. Because electronic messages are stored for some period of time before the intended recipient actually reads them, messages are susceptible to being read by system administrators or by hackers who unlawfully access the storage facility:[53] "The greatest risk for most email is at the two endpoints of the conversation. At both locations, most email is stored on computers in a form that's open and easily read by whoever operates the endpoint computer system . . . or . . . by hackers."[54]

3. Users

E-mail also depends on users, and human error is another basis of security risk:

> Unlike paper correspondence, it is extremely easy to misaddress an e-mail. Computer users typically address e-mail from an online directory. It is simple to click on the wrong recipient's address or, worse, accidentally select the option to send the e-mail to a large group of users when the communication was intended to be confidential.[55]

Electronic mail is an insecure medium. Human users are fallible; they may misdirect their communications. In addition, network technology and store-and-forward technology are susceptible to breach: "[D]isclosure of data while in electronic transit between computer systems"[56] is possible, and "data files stored on disks or other electronic media . . . [are susceptible to] tampering . . . or unauthorized examination."[57] Although computer crime may seem to be an unrealistic concern, "if NASA, federal agencies of all kinds, and financial institutions have security breaches, law firms cannot assume it cannot or will not happen to them."[58]

Presently, the predominant usage of electronic mail in the legal profession is reliance on internal systems,[59] suggesting that these

---

[52] *See infra* Part II.B.

[53] *See* Allison, *supra* note 47.

[54] *Id.*

[55] Michael Overly, *Avoid the Legal Pitfall of E-Mail*, LAN MAG., Jan. 1, 1997, at 75, 75.

[56] Cipher A. Deavours, *Cryptography, in* 1 MACMILLAN ENCYCLOPEDIA OF COMPUTERS 211, 212 (Gary G. Bitter ed., 1992).

[57] *Id.*

[58] Paul Berstein, *Encryption is Imperative For Lawyers Using The Internet: It's Not Safe Out There*, ILL. LEGAL TIMES, Aug. 1996, at 9; *see also* NEUMANN, *supra* note 32, at 132-42 (briefing numerous examples of computer security breaches in both the public and private sectors); Gary H. Anthes, *Few Gains Made Against Hackers*, COMPUTERWORLD, Sept. 16, 1996, at 20, 20 (discussing repeated hacker activity at the Pentagon).

[59] In a survey of corporate legal departments, use of internal e-mail was reported by

security issues are not yet of concern to the majority of attorneys. But the following discussion shows there are great advantages to, and a trend toward, expanding usage outside the enterprise.

B. Electronic Mail and the Legal Profession

Lance Rose points out in his book *Netlaw*[60] that in the 1966 novel, *The Crying of Lot 49*, Thomas Pynchon "imagined an alternative postal system riding on the back of intracorporate mail operations, outside the monopoly reserved for the United States Post Office."[61] Electronic mail is becoming that alternative postal system and, according to one commentator, is "destined to become a universal communication tool. . . ."[62] An examination of existing statistics regarding worldwide use supports this proposition.[63]

Although the percentage of worldwide users that are members of the legal community is not yet determined, lawyers recognized the potential benefits of e-mail from a point early in the development of e-mail systems.[64] Lawyers continue to discover the advantages of electronic mail communications today, increasing e-mail usage in their personal and professional capacities,[65] and recognizing that the worst mistake a computerizing attorney can make is "[b]uying a computer without a modem."[66]

68% of respondents while only 20% reported use of external e-mail. *See* AMERICAN BAR ASS'N, SURVEY OF AUTOMATION IN CORPORATE LEGAL DEPARTMENTS 35 (1993). In a survey of mid-size law firms, 44% of responding firms indicated that internal e-mail was available, and 9.8% of responding firm members indicated that they had external e-mail capabilities. *See* AMERICAN BAR ASS'N, AUTOMATION IN MIDSIZE LAW FIRMS 9 (1992). In a survey of smaller law firms, 50% of respondents with LAN's indicated that their LAN's provided internal e-mail, and 16% indicated that their LAN's were used for external e-mail. *See* AMERICAN BAR ASS'N, SURVEY OF AUTOMATION IN SMALLER LAW FIRMS 61 (1995).

60. LANCE ROSE, NETLAW (1995).

61. *Id.* at 169.

62. Merrill, *supra* note 28, at 20.

63. In 1993 it was estimated that the world e-mail community included 20 to 30 million users spanning 130 countries and 7 continents. *See* DERN, *supra* note 25, at 130. A 1996 article cited a figure of a worldwide userbase of 47 million. *See* Stevan Alburty, *E-Mail, E-Mail Everywhere*, THE NET, Aug. 1996, at 22, 22. This suggests a growth of between 17 and 27 million users in two years, and the userbase is using the technology: "Approximately 3 billion electronic mail messages were exchanged in 1988, and the volume is expected to grow to . . . 60 billion by the year 2000." Neill, *supra* note 25, at 353.

64. The American Bar Association created an electronic communications network, ABA/net, in 1984 to provide e-mail services. *See American Bar Association Uses E-Mail To Access Additional Services*, ELECTRONIC MESSAGING NEWS (Phillips Publishing, Inc.), Mar. 4, 1993.

65. A recent bar survey in Florida indicated that e-mail usage among its membership increased 52% between 1994 and 1996. *See* John F. Harkness, Jr., *Website Adds Value To Bar Membership*, FLA. B.J., July-Aug. 1996, at 10.

66. Daniel E. Harmon, *The Big "I"—Hottest Topic At the ABA Techshow '95*, THE LAWYER'S PC (Shepard's McGraw Hill, Inc., Colorado Springs, Colo.), May 1, 1995, at

What are the benefits that attract users, specifically attorneys? E-mail not only allows one-to-one communications,[67] (for which one could engage the services of the United States Postal Service) but also enables efficient one-to-many communications (otherwise achievable through a conference call or a mass mailing). In addition, features such as carbon copy and blind carbon copy permit users to send one message to multiple addresses at once.[68]

Electronic mail also has advantages over the fax machine. Although fax retains its position in the legal community as a favored means of communicating hard copies of documents,[69] electronic mail of documents still on a computer is more practical. "[I]f the sender and recipient both have external e-mail, it makes the most sense to skip the fax entirely and send the document from the sender's PC to recipient's PC and use recipient's printer if a hardcopy is needed."[70]

The non-intrusive nature of electronic mail is also a benefit to the attorney because "the e-mail message does not imply that an immediate reading is required."[71] It allows attorneys to handle messages at their leisure, enabling productivity. In addition, e-mail allows ease of document manipulation. A redlined draft of a document may be sent to opposing counsel via e-mail and edited without re-keying.[72] Other advantages include the speed of document delivery,[73] and the speed of response achievable through electronic mail.[74]

The reason that the use of electronic mail will continue to explode in the legal profession is not just because of the efficiency it provides within the firm or office. Client demand will force lawyers to either begin to use, or expand their use of this technolo-

---

1, 1.

67. *See* ALAN J. ROSS, THE LAW COMES TO TERMS WITH THE NET app. at 2 (1996).

68. *See* Bill Weinman, *NetFAQ*, THE NET, Dec. 1996, at 100, 100. Carbon copy is similar to a cc: line on a paper letter, indicating other recipients of the e-mail. *See* DERN, *supra* note 25, at 148. Blind carbon copy, "[a]gain mimicking hardcopy letter conventions, . . . lets [the user] include names of people [to receive] . . . a copy of the message . . . without letting any of the To: or Cc: names . . . [gain awareness] of it." DERN, *supra* note 25, at 149.

69. *See* HENRY H. PERRITT, JR., HOW TO PRACTICE LAW WITH COMPUTERS 274-76 (2d ed. 1992).

70. Merrill, *supra* note 28, at 22.

71. *Id.* at 21.

72. *See id.*

73. *See* Steven E. Ekeberg, *Building a Healthier Relationship with Technology*, 68 CLEVELAND B.J. 14, 14 (1996) ("[C]ommunicating through e-mail . . . ha[s] . . . increased the speed at which information can be created, revised, packaged, and delivered.").

74. *See* Cleveland Thornton, *Message dated Tuesday, 21 July 1992 15:32, in* THE EFFECTS OF ELECTRONIC MAIL ON LAW PRACTICE AND LAW TEACHING 4, 5 (I. Trotter Hardy ed., 1994) (stating that immediate response to electronic messages is possible by simply hitting the reply key and typing comments).

gy. Technology savvy clients will look upon those lawyers with electronic mailing capabilities favorably when shopping for an attorney.[75] The president of a law office consulting firm, for example, noted recently that "clients are instructing their law firms that they no longer wish to be billed for delivery services or fax charges and that all communications with the firm should be via . . . e-mail. . . ."[76] Meanwhile, one New Jersey attorney has "watched e-mail steadily mature from a gossip novelty into a serious practice tool"[77] in his law firm. The firm "now routinely use[s] e-mail in preference to both letters and telephone for a few . . . clients. In addition to questions and advice, [the firm] attach[es] . . . documents, spreadsheets, and even electronic bills . . . "[78] to the communications.

However, with increased usage there has not been an increased understanding of the technology involved. For the ordinary user, an understanding of the technology may not be critical. The technical limitations of the medium are particularly insidious to the legal community due to the strict requirement of confidentiality in the client-attorney relationship.

C. Confidentiality in the Client-Attorney Relationship

"A fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation."[79] This principle of confidentiality inheres in both legal and ethical duties imposed upon the lawyer. Whenever the attorney and client communicate confidential information, by any medium, there are two sets of considerations before the attorney: how to uphold his or her ethical duty of confidentiality, and how to uphold his or her legal duties of confidentiality.

1. Ethical Duty

The ethical duty of the attorney to maintain his or her client's confidences is found in the lawyer codes. Model Rule 1.6 of the Model Rules of Professional Conduct[80] (Model Rules) acts as the

---

[75] *See* Merrill, *supra* note 28, at 21; *see also* Daniel E. Harmon, *High Tech & Happy Clients*, THE LAWYER'S PC (Shepard's McGraw Hill, Inc., Colorado Springs, Colo.), Oct. 1, 1994, at 1 (noting that clients can be served "much faster and more efficiently through technology").

[76] Michael J. DiCorpo, *Technology—What Clients Demand*, 68 CLEVELAND B.J. 8, 8 (1996).

[77] Charles Merrill, *Message dated Monday, 20 July 1992 23:58, in* THE EFFECTS OF ELECTRONIC MAIL ON LAW PRACTICE AND LAW TEACHING 2, 2 (I. Trotter Hardy ed., 1994).

[78] *Id.*

[79] MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 cmt. (1995).

[80] MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1995). The Model Rule

confidentiality provision drafting guide for those states whose ethical codes resemble the Model Rules. For those states[81] whose codes continue to stem from the Model Code of Professional Responsibility (Model Code), Canon 4,[82] its accompanying Ethical Considerations, and Disciplinary Rule 4-101[83] provide guidance.

Whether the Model Rules or Model Code govern the jurisdiction, the ethical duty is quite broad. Under both regimes, disclosure of the protected information is prohibited in all circumstances, unless specifically allowed. An attorney is allowed to reveal client confidences when the client has been consulted and consents,[84]

---

provides that:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraph (b).
> (b) A lawyer may reveal such information to the extent the lawyer reasonably believes necessary:
> (1) to prevent the client from committing a criminal act that the lawyer believes is likely to result in imminent death or substantial bodily harm; or
> (2) to establish a claim or defense on behalf of the lawyer. . . .

Id.

[81] The only states that continue to utilize the Model Code of Professional Responsibility are Georgia, Iowa, Nebraska, New York, North Carolina, Ohio, Oregon, Tennessee, Vermont, and Virginia.

[82] MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1983) ("A Lawyer Should Preserve the Confidences and Secrets of a Client.").

[83] MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101 (1983). DR 4-101 states:

> (A) 'Confidence' refers to information protected by the attorney-client privilege under applicable law, and 'secret' refers to other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client.
> (B) Except when permitted under DR 4-101(C) a lawyer shall not knowingly:
> (1) Reveal a confidence or secret of his client.
> (2) Use a confidence or secret of his client to the disadvantage of the client.
> (3) Use a confidence or secret of his client for the advantage of himself or a third person, unless the client consents after full disclosure.
> (C) A lawyer may reveal:
> (1) Confidences or secrets with the consent of the client or clients affected, but only after a full disclosure to them. . . .
> . . . .
> (3) The intention of his client to commit a crime and the information necessary to prevent the crime.
> (4) Confidences or secrets necessary to establish or collect his fee or to defend himself . . . against an accusation of wrongful conduct. . . .

Id. (footnotes omitted).

[84] *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(C)(1) (1983); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(a) (1995).

and when the client impliedly authorizes the attorney to disclose the confidence.[85] In addition, the lawyer is permitted to reveal confidential information when the revelation may prevent the client from committing a future crime.[86]

The two codes differ in their classifications of what information is to be protected. Under the Model Rules, the attorney shall not reveal any "information relating to representation."[87] Under the Model Code, the preservation required is of confidences and secrets of the client. "'Confidence' refers to information protected by the attorney-client privilege . . . 'secret' refers to other information gained in the professional relationship that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client."[88] The Model Rules expanded the range of communications that fall under protection, "[a]n important contrast to the Code is that the Rule's proscription goes beyond 'confidences and secrets' and extends to 'information',"[89] but under both regimes the duty is great.

A failure to fulfill the duty of maintaining client confidences may lead to imposition of disciplinary sanctions under the Model Rules or the Model Code. The ABA Standards for Imposing Lawyer Discipline (ABA Standards) "are a model for imposing sanctions on attorneys based on the ethical duty involved, the party to whom the duty is owed, the lawyer's motives and intentions, and the injury caused by the misconduct."[90] Penalties are provided in the ABA Standards, and range from an admonition to disbarment for disclosure of client confidences.[91] In particular, an admonition is appropriate when "a lawyer *negligently* reveals information relating to representation of a client . . . and this disclosure *causes little or no actual or potential injury* to a client."[92] A reprimand is appropriate when "a lawyer *negligently* reveals information relating to representation of a client . . . and this disclosure *causes injury or potential injury* to a client."[93] The majority of both Model Code and Model Rules jurisdictions look to the ABA Stan-

---

85. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(C)(4) (1983); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(a) (1995); *see also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 cmt. (1995).

86. *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(C)(3) (1983); MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(b) (1995).

87. MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(a) (1995).

88. MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(A) (1983).

89. RONALD E. MALLEN & JEFFREY M. SMITH, 1 LEGAL MALPRACTICE 643 (3d ed. 1989).

90. *In re* Pressly, 628 A.2d 927, 929 (Vt. 1993).

91. *See* STANDARDS FOR IMPOSING LAWYER DISCIPLINE 4.21-.24 (1996).

92. STANDARDS FOR IMPOSING LAWYER DISCIPLINE 4.24 (1996) (emphasis added).

93. STANDARDS FOR IMPOSING LAWYER DISCIPLINE 4.23 (1996) (emphasis added).

dards for guidance when determining what sanctions, if any, are appropriate.[94]

2. Legal Duties

There are also legal duties of the lawyer with respect to confidentiality; they are found in two bodies of law: the law of agency and the law of evidence.

a. The Law of Agency

The law of agency defines fiduciary relationships as those relationships that result "from the manifestation of consent by one person to another that the other shall act on his behalf and subject to his control, and consent by the other so to act."[95] Employment relationships are usually guided by the law of contracts, with a dereliction of the duties outlined giving rise to an action in contract. The fiduciary relationship is unique, though. The fiduciary is not merely employed, he or she is employed to act in the best interest of his or her employer.[96] Loyalty is thus a duty of the fiduciary, a violation of this duty giving the employer a cause of action outside of contract. Breach of a fiduciary duty gives rise to an additional cause of action in tort.[97]

It is easy to see that "[t]he attorney-client relationship is a fiduciary relationship as a matter of law."[98] The client-attorney relationship is more than just an employment contract; confidence and trust must be reposed in the attorney, and the attorney is required to remain loyal to his or her client. Thus, failing to maintain the confidences of a client is not only a breach of the attorney's ethical duty, but also a breach of the attorney's fiduciary duty of loyalty. It is generally agreed that a breach of this fiduciary duty may be the basis of an attorney malpractice claim.[99]

---

[94] For Model Rules states adopting the ABA Standards, see, for example, *People v. McCray*, 926 P.2d 578 (Colo. 1996); *Committee on Legal Ethics of W. Va. State Bar v. Boettner*, 422 S.E.2d 478 (W. Va. 1992); *Florida Bar v. Hosner*, 513 So.2d 1057 (Fla. 1987). For Model Code jurisdictions, see, for example, *In re Cutler*, 650 N.Y.S.2d 85 (N.Y. App. Div. 1996); *Dockery v. Board of Prof'l Responsibility of the Supreme Court of Tenn.*, 937 S.W.2d 863 (Tenn. 1996); *In re Haws*, 801 P.2d 818 (Or. 1990).

[95] RESTATEMENT (SECOND) OF AGENCY § 1(1) (1958).

[96] *See* ALFRED F. CONRAD ET AL., AGENCY ASSOCIATIONS, EMPLOYMENT & PARTNERSHIPS 328 (4th ed. 1987).

[97] *See* RESTATEMENT (SECOND) OF AGENCY introductory note (1958).

[98] Clement v. Prestwich, 448 N.E.2d 1039, 1041 (Ill. App. Ct. 1983); *see also* David Welch Co. v. Erskine & Tulley, 250 Cal. Rptr. 339, 341 (Cal. Ct. App. 1988) ("The relation between attorney and client is a fiduciary relation of the very highest character. . . ."); *In re* Wilson, 409 A.2d 1153, 1156 (N.J. 1979) ("Lawyers are more than fiduciaries. . . .").

[99] *See* Zeiden v. Oliphant, 54 N.Y.S.2d 27 (N.Y. Sup. Ct. 1945) (affirming a judgment for attorney malpractice in favor of a client after the attorney revealed client confi-

The elements of a malpractice claim include the existence of the lawyer-client relationship,[100] a duty owed,[101] such as the fiduciary duty of loyalty, and "departure or deviation from the usual and customary practice within th[e] . . . profession."[102] The issue is not whether the attorney acted negligently; instead, an examination into community standards of acceptable conduct is made: whether an average attorney "would have been as careless or imprudent as the defendant."[103] Finally, "but for" causation[104] and actual harm sustained must be proven.[105]

b. The Law of Evidence

The existence of the attorney-client privilege under the law of evidence furthers the unique status given to confidential communications between the attorney and client. The attorney-client privilege has been defined in the following way:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[106]

In a judicial proceeding the communications between an attorney and an actual or potential client made "without the presence of strangers . . . for the purpose of securing . . . legal services" are thus privileged.[107] Neither the client nor the attorney may be forced to testify as to the contents of such communications,[108] as long as the privilege is not waived.

The privilege is waived upon intentional communication of the privileged information to a third party. When the "client testifies to some of the [privileged] communications or permits the attorney to so testify,"[109] waiver ensues. In addition, "[t]he law will . . . im-

---

dences post discharge); MALLEN & SMITH, *supra* note 89, at 644 (stating that "[m]alpractice liability may be predicated upon a breach of confidence").

100. *See* DAVID J. MEISELMAN, ATTORNEY MALPRACTICE: LAW AND PROCEDURE 13 (1980).

101. *See id.*

102. *Id.* at 15-16.

103. Note, *Attorney Malpractice*, 63 COLUM. L. REV. 1292, 1300 (1963).

104. *See* MEISELMAN, *supra* note 100, at 40.

105. *See id.*

106. JOHN H. WIGMORE, 8 WIGMORE ON EVIDENCE § 2292 (John T. McNaughton ed., rev. ed. 1961).

107. United States v. United Shoe Mach. Corp., 89 F. Supp. 357, 358 (D. Mass. 1950).

108. *See* CENTER FOR PROFESSIONAL RESPONSIBILITY, ANNOTATED MODEL RULES OF PROFESSIONAL CONDUCT 73 (1996).

109. RICHARD O. LEMPERT & STEPHEN A. SALTZBURG, A MODERN APPROACH TO EVI-

ply a waiver whenever the holder of the privilege voluntarily discloses or allows to be disclosed any significant part of the privileged matter."[110]

An eavesdropper's acquisition of privileged information will not typically threaten the privilege. On one level, federal law is applicable. The Electronic Communications Privacy Act (ECPA),[111] discussed in more detail *infra*,[112] protects any otherwise privileged communication, intercepted under the ECPA, from losing its privileged character because of such interception.[113] The generally adopted common law rule is also important: "[I]f a client has a reasonable expectation of privacy in conversations with his attorney, then the privilege will not be jeopardized despite interception or overhearing by an eavesdropper."[114]

Whether waiver occurs after an inadvertent disclosure of client confidences is not clear. What is the result when the attorney mistakenly discloses a confidential memorandum during discovery, or when an attorney or client misaddresses an e-mail containing confidential information? Some jurisdictions maintain that for waiver to result, such revelation to a third party must be intentional.[115] Other jurisdictions hold, though, that disclosure always amounts to a waiver, even if the disclosure is unintentional.[116] A growing num-

---

DENCE 696 (2d ed. 1982).

[110] *Id.*

[111] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

[112] *See infra* Part III.B.1.

[113] *See* 18 U.S.C. § 2517(4) (1994) (providing that "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character").

[114] Dale W. Cottam, *Cellular Communications and Confidentiality: Can Waiver Occur On The Way To The Office?*, 25 CREIGHTON L. REV. 1185, 1203 (1992).

[115] *See* Georgetown Manor, Inc. v. Ethan Allen, Inc., 753 F. Supp. 936 (S.D. Fla. 1991) (holding that the inadvertent production during a discovery request of a privileged transcript of various tape recorded conversations did not waive the privilege), *aff'd in part*, 991 F.2d 1533 (11th Cir. 1993); Mendenhall v. Barber-Greene Co., 531 F. Supp. 951 (N.D. Ill. 1982) (holding that the inadvertent production during a discovery request to opposing counsel of privileged letters did not constitute waiver).

[116] *See In re* Sealed Case, 877 F.2d 976 (D.C. Cir. 1989) (holding that disclosure of a confidential memorandum to a government auditor waived the privilege); Golden Valley Microwave Foods, Inc. v. Weaver Popcorn Co., 132 F.R.D. 204 (N.D. Ind. 1990) (holding that the privilege that had attached to a confidential letter was waived when the letter was accidentally included in a discovery request; although the court did not explicitly adopt the strict responsibility approach, it held that under the strict approach waiver would result); Underwater Storage, Inc. v. United States Rubber Co., 314 F. Supp. 546 (D.C. Dist. 1970) (holding that the presentation of a letter by plaintiff to defendant placed the document in the public domain, breaching the confidentiality of the document, and thus destroying any attached privilege); United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461 (E.D. Mich. 1954) (stating that "where the policy underlying the rule can no longer be served, it would amount to no more than mechanical obedience to a formula to continue to recognize it").

ber of jurisdictions will not lay down a strict rule, but maintain that a number of factors must be examined before a determination as to waiver can be made.[117] The effect of an inadvertent disclosure of otherwise privileged information therefore varies by jurisdiction.[118]

Confidentiality is an important concern for lawyers. Professional ethics mandate its maintenance, and the laws of agency and evidence infuse its importance into the client-attorney relationship. A failure to maintain confidentiality may result in disciplinary sanctions against the lawyer, a claim of attorney malpractice if the breach leads to measurable damages to the client, or possibly in waiver of the attorney-client privilege that otherwise protected the communication. The weaknesses in electronic mail technology are thus appropriate concerns for attorneys.

The use of electronic mail in the conveyance of confidential information is a risk management category. There are limitations on electronic mail technology, creating a danger that confidentiality can be lost through its use. There are also potentially harmful consequences associated with failing to maintain client confidentiality. In other words, associated with the use of electronic mail, "danger[s exist] that, if not controlled, may lead to . . . consequence[s] unintended by and actually or potentially harmful to a law firm or practitioner."[119]

II. RISK LIMITING SYSTEMS CURRENTLY AVAILABLE OR IN PLACE

It is important to restate and clarify the terminology being used in this Note. The *danger* associated with using e-mail to convey confidential information is a failure to maintain confidentiality. The *consequences of the materialization of this danger* are disciplinary sanctions, attorney malpractice claims, and waiver of the attorney-client privilege. The danger, in association with the consequences, makes e-mail risky.

When looking to limit risk it is necessary to examine the means of decreasing the danger as well as means of decreasing the harm of the consequences. There are currently technological and legal systems available or in place that decrease the danger and

---

[117] *See* Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (upholding a decision to apply a factor test, stating that such a test serves the purpose of the privilege while not permitting the careless to enjoy its benefits); Monarch Cement Co. v. Lone Star Industries, Inc., 132 F.R.D. 560 (D. Kan. 1990) (applying five factor test in finding that due to reasonable efforts taken to prevent disclosure, the inadvertent production of eight confidential pages in a 9,000 page discovery request did not waive the privilege).

[118] *See* James C. Rinaman Jr., *What About Inadvertently Disclosed Documents or Information?*, 60 DEF. COUNSEL J. 613, 614 (1993) (discussing all three theories).

[119] *See supra* note 17 and accompanying text.

consequences of using electronic mail to convey confidential information.

A. Technological Systems

The communications security industry is constantly introducing products into the marketplace that attempt to alleviate the electronic mail user's security fears. These products can decrease the likelihood that the danger associated with electronic mail, loss of confidentiality, will be realized. The products offer technological fixes to the previously discussed weaknesses in e-mail technology.

Two products introduced into the market in the fall of 1996 provide examples. The first product is compatible with most existing LAN based electronic mail systems and facilitates "[e]-mail connections with partners, clients, and suppliers across a private network . . . avoid[ing] the security and reliability pitfalls of Internet E-mail."[120] A second product is a tool that "contains matrices, or tables, that allow organizations to match up applications, threats and defenses into a kind of three-dimensional security checklist. The matrices let . . . users determine when a particular type of security is inadequate or overkill."[121] Either of these systems may help to minimize the dangers associated with electronic mail usage. The first product would enable users to enlarge (or create) a closed network, limiting the need for external e-mail and thus avoiding its limitations. The second product allows a firm or practitioner to determine the types of security technologies available and appropriate for its proposed use of e-mail. These products are just two examples of the many available on the market today.

The most commonly cited technological solution to the confidentiality problem, though, is the use of cryptography.[122] "Cryptography is the study of methods for secret writing"[123] and the

---

[120] Tim Ouellette, *Internet Mail Service Links E-Mail Nets*, COMPUTERWORLD, Nov. 18, 1996, at 63, 68.

[121] Gary H. Anthes, *Tool May Allay 'Net Fears*, COMPUTERWORLD, Oct. 21, 1996, at 89, 89.

[122] *See generally* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 724 (1995) (suggesting that professionals with a duty of confidentiality use encryption to protect that confidentiality); Charles R. Merrill, *A Cryptography Primer, in* WHAT LAWYERS NEED TO KNOW ABOUT THE INTERNET (Henry H. Perritt, Jr. ed., 1996) (stating that the solution to the security problems of electronic commerce is encryption); *E-Mail and Privacy—Keeping Confidential E-Mail Confidential*, LAW OFF. TECH. REV., Mar. 24, 1994 (reviewing the use of cryptography as a method of ensuring confidentiality).

[123] Deavours, *supra* note 56, at 211 (emphasis removed from original). Cryptography works by applying an algorithm, called a key, to a plaintext message to encode it. A key is then applied by the recipient to decipher the message. *See* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 3-5 (2d ed. 1996). The following explanation of two basic types of key-based cryptosystems, symmetric key and public-key, clarifies this.

goal of cryptography is to "enable . . . people . . . to communicate over an insecure channel in such a way that an opponent . . . cannot understand what is being said."[124]

Cryptography is the favored e-mail protection because it is extremely difficult to subvert. One publicly available cryptographic software package, Pretty Good Privacy (PGP), allows implementations that provide security that range from "breakable, but with much effort . . . [to] possibly breakable by three letter organizations . . . [to] generally believed unbreakable."[125] The developers of the algorithm underlying PGP even issued a challenge to decrypt a message encrypted with the algorithm, estimating that it would take forty quadrillion years to accomplish the feat.[126] The developers overestimated the strength of their algorithm. Acceptors of the challenge decrypted the message after only eight months. This by no means invalidates the security of cryptography. To decrypt the message "a worldwide team cooperating over the Internet and using over 1600 computers"[127] was required.

The use of cryptography, or other technologies, is thus an effective means of protecting electronic mail communications from tampering. Technological systems decrease the possibility that confidentiality will be lost when e-mail is used.

B. Legal Systems

Legal systems are also in place that decrease the possibility that confidentiality will be lost when e-mail is used. Legal systems also decrease the effect and applicability of the consequences of lost confidentiality.

> Think of a symmetric algorithm as a safe. The key is the combination. Someone with the combination can open up the safe, put a document inside, and close it again. Someone else with the combination can open the safe and take the document out. Anyone without the combination is forced to learn safecracking. . . . [P]ublic-key cryptography . . . [on the other hand] use[s] two different keys—one public and one private. . . . Anyone with the public key can encrypt a message but . . . [o]nly the person with the private key can decrypt the message. It is as if someone turned the cryptographic safe into a mailbox. Putting mail into the mailbox is analogous to encrypting with the public key; anyone can do it. Just open the slot and drop it in. Getting mail out of a mailbox is analogous to decrypting with the private key. Generally it's hard; you need welding torches.

Id. at 61.

[124] DOUGLAS R. STINTON, CRYPTOGRAPHY: THEORY AND PRACTICE 1 (1995).

[125] WILLIAM STALLINGS, PROTECT YOUR PRIVACY: THE PGP USER'S GUIDE 63 (1995).

[126] *See id.* at 64.

[127] *Id.*

1. The Electronic Communications Privacy Act

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III)[128] "is the primary law protecting the security and privacy of business and personal communications in the United States today."[129] Congress enacted much of Title III to codify the principles of law established in the Fourth Amendment Supreme Court decision *Katz v. United States*,[130] a case that greatly altered Fourth Amendment interpretation.

Prior to *Katz*, *Olmstead v. United States*[131] outlined the fundamental legal rules of electronic eavesdropping in the United States. According to *Olmstead*, the Fourth Amendment protection against unreasonable searches and seizures applied only to the seizure of tangible items, and only to searches accomplished by a physical invasion. Wiretaps and other means of electronic eavesdropping did not violate the Fourth Amendment under *Olmstead* because they did not provide the requisite physical trespass.[132]

Katz v. United States overturned *Olmstead's* position in 1967,[133] and paved the road for communication privacy in the present age of telecommunications. In *Katz*, the Supreme Court held that protection offered by the Fourth Amendment was intended to benefit "people, not places."[134] The Court stated that "the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any 'technical trespass under . . . local property law.'"[135] Title III was subsequently enacted, adopting the principles established in *Katz*, recognizing that both wire and oral communications are protected from unlawful invasions of privacy.[136]

Unfortunately, Title III failed to keep pace with the changing

---

[128] Omnibus Crime Control and Safe Streets Act, Pub. L. No. 90-351, 82 Stat. 197, 213 (1968).

[129] S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 [hereinafter SENATE REPORT].

[130] 389 U.S. 347 (1967).

[131] 277 U.S. 438 (1928).

[132] *See id.* at 466.

[133] *See* 389 U.S. at 353.

[134] *Id.* at 351.

[135] *Id.* at 353 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[136] *See* NATIONAL COMMISSION, *supra* note 5, at 5. Title III was also enacted to codify procedures for obtaining court authority to electronically eavesdrop; this portion of Title III is based upon the Supreme Court case of *Berger v. New York*, 388 U.S. 41 (1967). Although *Berger* held unconstitutional a New York statute that authorized court approved eavesdropping, "[t]he inference drawn from this decision . . . was that electronic eavesdropping would be within accepted Fourth Amendment bounds when requirements of particularity were included within a scheme of statutory provisions which allowed an adequate degree of judicial approval and supervision." NATIONAL COMMISSION, *supra* note 5, at 5.

telecommunications landscape. The wire and oral communications protected by Title III encompassed only the contents of communications audible and comprehensible by the human ear[137] (e.g. telephone conversations, face to face discussions). Title III's failure to protect electronic communications, including electronic mail, prompted its amendment in 1986.[138]

The Electronic Communications Privacy Act of 1986[139] (ECPA) amended Title III, expanding its coverage to protect electronic communications. The legislative history of the ECPA stated its purpose as "updat[ing] and clarify[ing] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies."[140] The ECPA accomplished this purpose in three Titles, two of which are relevant to this Note.

a. Title I of the ECPA

Title I[141] of the ECPA "protects communication streams (communications while in transit),"[142] by punishing the *interception* of communications.[143] Interception is the key violative activity under Title I and is statutorily defined. An interception is any "aural or other acquisition of the contents of any wire, [or] electronic . . .

---

137. *See* SENATE REPORT, *supra* note 129, at 2.

138. *See id.* at 1-3.

139. *See supra* note 111.

140. SENATE REPORT, supra note 129, at 1.

141. Title I is codified at 18 U.S.C. §§ 2510-2522 (1994).

142. PERRITT, *supra* note 26, at 102.

143. *See* 18 U.S.C. § 2511(1)(a) (1994). The statute provides "(1) Except as otherwise specifically provided in this chapter any person who- (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; . . . shall be punished as provided . . . or shall be subject to suit as provided. . . ." *Id.* The Title also outlaws the *use* of information acquired by unlawful interception:

> (1) Except as otherwise specifically provided in this chapter any person who—
> (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception . . . in violation of this subsection; . . . shall be punished as provided . . . or shall be subject to suit as provided. . . .

18 U.S.C. § 2511(1)(d) (1994). The Title also outlaws the *disclosure* of information acquired by unlawful interception:

> (1) Except as otherwise specifically provided in this chapter any person who—
> (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception . . . in violation of this subsection; shall be punished as provided . . . or shall be subject to suit as provided. . . .

18 U.S.C. § 2511(1)(c) (1994).

communication through the use of any electronic, mechanical, or other device."[144] Knowledge of the definitions of wire communication and electronic communication facilitate understanding of what Title I actually outlaws.

Wire communication is defined in the ECPA as "any aural transfer made . . . by the aid of wire, cable, or other like connection. . . ."[145] An example of a wire communication is an ordinary telephone call.[146] The term wire communication also includes "any electronic storage of such communication;"[147] common examples of stored wire communications are voice mail messages and answering machine tapes.[148]

An electronic communication is "any transfer of signs, signals, writing, images, sounds, data, or intelligence . . . but does not include . . . any wire communications. . . ."[149] Electronic mail, while in transit from sender to receiver, is an example of an electronic communication.[150] The definition of electronic communication does not include "any electronic storage of such communication" as the definition of wire communication does.

By outlawing the acquisition of wire and electronic communication streams, Title I of the ECPA outlaws such activities as wiretapping a telephone conversation, acquiring the contents of a voice mail message, and acquiring an e-mail message as it streams from sender to receiver. The ECPA thus offers protection to the e-mail utilizing attorney and client. By outlawing interception of electronic communications, the ECPA deters individuals who would otherwise attempt to profit from electronic mail's technological limitations.[151] Accordingly, Title I decreases the potential for the realization of the danger associated with electronic mail.

Title I also limits the consequences associated with the realization of the dangers of e-mail. Any otherwise privileged communication intercepted under the ECPA, lawfully[152] or unlawfully,

---

144. 18 U.S.C. § 2510(4) (1994).

145. 18 U.S.C. § 2510(1) (1994).

146. *See* SENATE REPORT, *supra* note 129, at 12 (stating that "wire communication encompasses the whole of a voice-telephone transmission").

147. 18 U.S.C. § 2510(1) (1994).

148. *See* SENATE REPORT, *supra* note 129, at 12 (stating that "wire communications in storage like voice mail, remain wire communications" for the purposes of the Act).

149. 18 U.S.C. § 2510(12) (1994).

150. *See* SENATE REPORT, *supra* note 129, at 14.

151. Deterrence is achieved through the imposition on the violator of both civil and criminal penalties. Relief in a civil action may include actual damages, statutory damages, punitive damages, and reasonable attorney fees. *See* 18 U.S.C. §§ 2520(a), 2520(b) (1994). Criminal penalties include a minimum $500 fine for some second offenders, and imprisonment of up to five years is permitted in lieu of or in addition to the fine. *See* 18 U.S.C. §§ 2511(4), 2511(5) (1994).

152. A lawful interception would be an interception permitted by court order. *See* 18

does not lose its privileged character because of such interception.[153]

b. Title II of the ECPA

Title II[154] of the ECPA is also relevant to this Note. The key violative activity under Title II is *access*, as compared with interception in Title I. An individual who unlawfully accesses "a wire or electronic communication while it is in electronic storage" in a facility in which electronic communication services are provided violates Title II.[155] An example of such a violation is the accessing of an e-mail message in storage on a computer, awaiting forwarding to its recipient.[156]

Like Title I, Title II uses deterrence to offer protection to attorneys and clients who wish to communicate via electronic mail. Title II criminally punishes an unlawful access with various combinations of fines and imprisonment, depending upon the purpose of the access and the offender's history of Act violations.[157] Title II also permits civil actions, granting actual damages incurred because of the access, punitive damages for wilful violations, and reasonable attorney fees.[158] Through the imposition of these penalties, Title II decreases the probability that the danger associated with electronic mail will materialize.

There is no provision in Title II that protects otherwise privileged information from losing its privilege upon a violative or even lawful access. Only *intercepted* electronic communications are statutorily protected from losing their privilege under Title I.[159]

U.S.C. § 2518 (1994) (outlining the procedure through which a court may grant an order authorizing an interception).

153. *See* 18 U.S.C. § 2517(4) (1994).

154. Title II is codified at 18 U.S.C. §§ 2701-2711 (1994).

155. 18 U.S.C. § 2701(a) (1994). That section states:

> (a) Offense—Except as provided in subsection (c) of this section, whoever—
> (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or
> (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system
> shall be punished as provided in subsection (b) of this section.

Id.

156. *See* Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457 (5th Cir. 1994) (affirming a district court determination that the federal government violated Title II by confiscating, without the appropriate court approval, a computer that held unread e-mail messages stored in its memory).

157. *See* 18 U.S.C. § 2701(b) (1994).

158. *See* 18 U.S.C. § 2707(b) (1994).

159. *See supra* notes 113, 144-51 and accompanying text.

2. Inadvertent Disclosure

A second legal system that attempts to decrease the consequences of a realization of the dangers associated with electronic mail recognizes that imperfect users increase the risk that electronically mailed communications will lose their confidentiality. If an attorney wishes to send his or her client a confidential message electronically, and accidentally places an opposing counsel's address as a carbon copy recipient, the contents of that message are no longer secret. An important question is whether any attorney-client privilege otherwise attached to that communication is waived.

Within the discussion of the attorney-client privilege *supra*,[160] it was noted that some jurisdictions maintain that for waiver to result, communication of privileged information to a third party must be intentional.[161] This approach, called the "subjective intent approach," is the traditional rule in inadvertent disclosure cases. Generally, the subjective intent approach holds that no waiver of the attorney-client privilege results after an inadvertent disclosure. A court adopting this approach begins its analysis with a definition of waiver as "the intentional relinquishment or abandonment of a known right,"[162] and proceeds to a discussion of the beneficiary of the privilege. Because the privilege exists for the benefit of the client, the logical conclusion in a subjective intent jurisdiction is that without client intention to relinquish the privilege, there can be no waiver. The negligent acts of one's counsel may not be imputed to, and result in punishment of, the client.[163]

Those jurisdictions that adopt the subjective intent approach seemingly offer legal protection to the electronic mail using attorney and client. Because the requisite intent to abandon the privilege is absent, privileged status will not be lost if a message is inadvertently missent.

Not all jurisdictions adopt the subjective intent approach; the trend is toward adopting the "relative conduct approach" to determine whether an inadvertent disclosure amounts to waiver. The relative conduct approach examines various factors to determine whether the privilege has been lost. "The reasonableness of the precautions taken to prevent inadvertent disclosure; . . . [t]he time taken to rectify the error; . . . [t]he extent of disclosure; . . . [and t]he overriding issue of fairness"[164] are among the factors exam-

---

160. *See supra* notes 106-18 and accompanying text.

161. *See supra* note 115 and accompanying text.

162. Mendenhall v. Barber Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1982).

163. *See id.*

164. Monarch Cement Co. v. Lone Star Industries, Inc., 132 F.R.D. 558, 560 (D. Kan. 1990). Most inadvertent disclosure cases arise after counsel inadvertently includes privileged documents in a discovery request. The fifth factor usually examined is the extent of

ined. The courts accepting this view "emphasize the relative inadvertence of the production versus [the] intentional relinquishment or abandonment of a known right. . . . [T]hey resist waiver of the privilege where there is unintentional production with reasonable precautions taken."[165] However, understanding that the consequences of carelessness should not go unaccounted for, middle ground jurisdictions will find implied waiver of the privilege when the facts surrounding the disclosure demonstrate continued protection is unwarranted.[166]

Under the proper circumstances, protection can be afforded to client-attorney e-mail communications in those jurisdictions adopting the relative conduct approach. No case has yet dealt with the issue of a mistakenly sent electronic mail message, but protection was granted in a recent case in which a privileged document was mistakenly *faxed* to an opposing counsel.[167] The court ultimately determined that fairness weighed in favor of maintaining privilege,[168] but found the sending party's precautions to be inadequate.[169] It is not clear what procedures will be adopted by the legal community that will amount to reasonable precautions with respect to sending electronic mail, but with reasonable precautions, the factor test jurisdictions can decrease the effects of lost confidentiality for the attorney and client.

There are technological and legal systems currently available or in place that reduce, or attempt to reduce, the risks associated with electronic mail. The technological solutions provide a means of preventing confidentiality from being lost, and legal systems are in place that both prevent and decrease the effects of lost confidentiality. Are the existing legal protections sufficient on their own, though? Is availing oneself of technological protection simply a matter of business judgment, or should there be a duty to use the technology? The third step in risk management, the development of a strategy to control the risks falling outside of the discussed protections, is now appropriate.

---

such discovery request. Because the inadvertent disclosure discussed in this Note is not based upon a document request, the fifth factor is not discussed.

165. Rinaman, *supra* note 118, at 614.

166. *See* Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (concluding that the proper analysis regarding inadvertent disclosures must take into account, on a case by case basis, the circumstances surrounding the disclosure).

167. *See* 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 (1994).

168. *See* James P. Ulwick, *Producing By Mistake*, LITIGATION, Spring 1992, at 20, 68 (discussing the ethical and legal consequences of a case in which a legal secretary mistakenly faxed a document to opposing counsel).

169. *See id.* at 68. The sending attorney did not properly instruct his temporary secretary on the office policy regarding inadvertent facsimile transmissions. *See id.*

III. FORMULATION OF A STRATEGY TO CONTROL THE ASSOCIATED RISKS

A. Previously Proposed Strategies

Before discussing the proposed strategy, examining the strategies proposed by the legal community to date is helpful.

1. Proposed Strategy #1: Sole Reliance on Existing Legal Protections

As discussed *supra*, legal protections exist that reduce the risks associated with electronic mail usage. Thus, one strategy for the legal community to adopt in relation to electronic mail usage is sole reliance on existing legal protections.

A recently published article adopts such an approach. *Privilege and Confidentiality in Cyberspace*,[170] authored by Albert Gidari, addresses whether the attorney-client privilege can be maintained when attorney and client communicate over the Internet. The article discusses the ECPA's prohibition on the interception of electronic and wire communications[171] and the ECPA's maintenance of the attorney-client privilege on any otherwise privileged electronic or wire communication intercepted under the ECPA.[172] The article further explains that no ECPA provision statutorily protects the attorney-client privilege after an access of stored data. Congress failed to include such a provision, it argues, because "none is needed."[173] The common law rule holds that "there is no waiver of privilege when a thief steals a document out of a file cabinet, and likewise no waiver [will occur] when the file is in digital form and the break-in occurs through the phone line."[174] The article concludes that the ECPA sufficiently protects the attorney-client privilege; the level of communication security an enterprise chooses should be based on business judgment, not on fear of losing the attorney-client privilege.[175]

Mr. Gidari's interpretation of the law of electronic communications is not wholly unpersuasive. A key provision of the ECPA for the attorney and client is §2517(4).[176] This provision maintains the status of any otherwise privileged communication inter-

---

170. Albert Gidari, *Privilege and Confidentiality in Cyberspace*, COMPUTER LAW., Feb. 1996, at 1.

171. *See id.* at 1; *see also supra* notes 141-53 and accompanying text.

172. *See* Gidari, *supra* note 170, at 2; *see also supra* notes 113, 151-53 and accompanying text.

173. Gidari, *supra* note 170, at 2; *see also supra* note 159 and accompanying text.

174. Gidari, *supra* note 170, at 2.

175. *See id.* at 3.

176. 18 U.S.C. § 2517(4) (1994); *see also supra* notes 113, 153 and accompanying text.

cepted in accordance with, or in violation of, the ECPA. Mr. Gidari's conclusion that the ECPA protects against loss of privilege when communications are intercepted is accurate.

Note the language of §2517(4), though: "[n]o *otherwise privileged* . . . electronic communication . . . shall lose its privileged character"[177] due to an interception. The application of §2517(4) requires an initial showing that the communication was privileged. For a communication to obtain the protection of the attorney-client privilege it must be sheathed in a reasonable expectation of privacy.[178] A legitimate inquiry can thus be made into whether that sheathe is available to communications made via the breachable electronic mail format.[179]

Mr. Gidari suggests in his article that Congress directly provided the sheathe. Gidari states that the ECPA makes "clear that essentially any communication carried over a communication system provided by a telecommunications carrier is deemed to be not 'readily accessible to the general public' . . . [and thus sheathed in] a reasonable expectation of privacy."[180]

Mr. Gidari's analysis on this point is based upon ECPA §2510(16).[181] At the time Mr. Gidari's article was published, this subsection stated: "(16) 'readily accessible to the general public' means, with respect to a radio communication, that such communication is not— . . . (F) an electronic communication."[182] A plain reading of this does not suggest that §2510(16) reveals the nature of electronic communications; it seems to apply only to radio communications. The legislative history of the ECPA interprets this provision, though, as stating that radio communications are not deemed to be readily accessible to the general public when they

---

177. *Id.* (emphasis added).

178. *See supra* notes 106-08 and accompanying text.

179. *Cf. supra* notes 5-6 and accompanying text (discussing the applicability of this question to telegraphic messages).

180. Gidari, *supra* note 170, at 3.

181. 18 U.S.C. § 2510(16) (1994). The section currently reads:

> (16) "readily accessible to the general public" means, with respect to a radio communication, that such communication is not—
>
> (A) scrambled or encrypted;
>
> (B) transmitted using modulation techniques whose essential parameters have been withheld from the public . . . ;
>
> (C) carried on a subcarrier . . . ;
>
> (D) transmitted over a communication system provided by a common carrier . . . ; or
>
> (E) transmitted on frequencies allocated under . . . [various parts of the section].

Id.

182. 18 U.S.C. § 2510(16) (1994), *amended by* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 203, 108 Stat. 4279, 4291 (1996).

"fit into one of five specified categories. These excepted categories . . . *usually are not susceptible to interception by the general public.*"[183] Electronic communications were, at the time of publication of Mr. Gidari's article, one of the excepted categories. Thus, a fair interpretation of the ECPA at the time Mr. Gidari authored his article was that electronic communications in general were not readily susceptible to interception by the general public, and therefore able to be sheathed in a reasonable expectation of privacy.

However, Part (F) of Subsection 16 was recently repealed.[184] Electronic communications are no longer included among the list of communications that are deemed "usually . . . not susceptible to interception by the general public."[185] Mr. Gidari's reliance on the ECPA to sheathe electronic mail in a reasonable expectation of privacy is thus dated; the ECPA no longer provides the solution Mr. Gidari relied upon in his proposal.

Common law may provide the sheathe, though. A military court, whose rulings are only persuasive authority in civilian courts of law,[186] recently discussed the expectation of privacy in an electronic mail message. The court held that "appellant clearly had an . . . expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password. Similarly, he had an . . . expectation of privacy with regard to messages he transmitted electronically to other subscribers."[187] The court held that messages stored on network computers awaiting retrieval by the intended recipient, and messages in transmission, are reasonably expected to be private. The court admonished "[i]n the modern age of communications, society must recognize such expectations of privacy as reasonable."[188]

In addition, civilian courts asked to determine whether to permit the discovery of e-mail communications have denied production on the basis of privilege. In a recent case, thirty-two e-mail communications were held undiscoverable due to attorney-client privilege protection.[189] A second court granted a writ of prohibition to

---

183. H.R. REP. NO. 103-827(I), at 81 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511 (emphasis added).

184. *See* Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132, § 731(2)(C), 110 Stat. 1303, 1303 (striking subparagraph (F) of § 2510(16) and thereby excluding electronic communications from being statutorily "readily accessible to the general public").

185. H.R. REP. NO. 103-827(I).

186. *See* KENNETH R. REDDEN, FEDERAL SPECIAL COURT LITIGATION 221-23 (Evan G. Lewis et al. eds., 1982) (discussing the authority of military court decisions in civilian courts).

187. United States v. Maxwell, 42 M.J. 568, 576 (A.F. Crim. App. 1995) (upholding the court martial's dismissal of an Air Force Colonel for violations, through use of his personal computer, of federal pornography laws).

188. *Id.*

189. *See* National Employment Serv. Corp. v. Liberty Mutual Ins. Co., 3 Mass. L. Rptr.

ensure nondisclosure of an e-mail communication, holding that the contents of the e-mail message were privileged.[190] It thus seems that electronic mail communications are increasingly considered sheathed in a reasonable expectation of privacy by the courts; the attorney-client privilege is available to the contents of e-mail. If the courts continue along this trend, the common law, in conjunction with the ECPA, will allow electronic mail messages to obtain the privilege and then maintain it after an interception.

The express language of §2517(4) of the ECPA applies its protections only to interceptions, though.[191] There is no mention in the Section, or in the ECPA, of the effect that an access of a stored communication has on the privilege. Can the interception sections of the ECPA be applied to activities that appear to be accesses? The quick answer to that question is no. The ECPA is quite distinct in its treatment of interceptions and accesses, each having its own Title.[192] Courts would be in complete derogation of principles of statutory construction if they were to hold that §2517(4) was really meant to apply to both accesses and interceptions.

The next question to ask is whether behaviors that appear to be accesses can be reclassified as interceptions. Of more specific concern to this Note, can the unlawful access of a stored electronic communication be classified as an interception of a stored electronic communication?

A 1994 case first raised the issue of whether an action that appeared classifiable as an unlawful access could be classified an unlawful interception. The case, *Steve Jackson Games, Inc. v. United States Secret Service*,[193] placed before the court the question "whether the seizure of a computer on which is stored private E-mail that has been sent . . . but not yet read (retrieved) by the recipients, constitutes an 'intercept'" within the meaning of Title I of the ECPA.[194] After examining the language of the ECPA, and its legislative history, the court determined that Congress intended

---

221 (1994) (holding that because e-mail messages between defendant's corporate counsel and defendant's outside counsel were made in the outside counsel's professional capacity, they were privileged and undiscoverable; notably, the court did not raise the issue of whether the electronic mail format affected the availability of the privilege).

190. *See* State v. Canady, 460 S.E.2d 677 (W. Va. 1995).

191. *See* 18 U.S.C. § 2517(4) (1994). For further discussion of this section, see *supra* note 113 and accompanying text.

192. *See supra* notes 143-59 and accompanying text.

193. 36 F.3d 457 (5th Cir. 1994) (holding that seizure of a computer containing private, unread e-mail did not constitute an intercept under the ECPA; the federal government argued for reclassification because as an intercept their activity was properly authorized, as an access, it was not).

194. *Id.* at 460.

to treat stored wire and stored electronic communications differently.[195] "Congress' . . . omission in [the] definition [of electronic communication] of the phrase 'any electronic storage of such communication' (part of the definition of 'wire communication') reflects that Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage'."[196] The court held that the access could not, therefore, be an intercept.[197]

Since the *Steve Jackson* decision, two additional cases reasoned that the language of the ECPA combats any attempt to reclassify accesses of stored electronic communications as interceptions.[198] Courts are repeatedly asserting that stored electronic communications cannot be intercepted.

Stored electronic communications accessed under the Act thus have no statutory privilege protection. Common law must prevent loss of the attorney-client privilege. Mr. Gidari asserts that the common law does prevent such a loss, and that, as a result, no statutory protection is needed.[199] Mr. Gidari is correct in his assertion that the common law protects the privilege from being waived upon a thief's or an eavesdropper's activity.[200] Additionally, "a party does not waive the attorney-client privilege for documents which he is compelled to produce."[201] Thus, whether stored e-mail communications are accessed in violation of, or in accordance with the Act, the common law will seemingly protect the attorney-client privilege.

Analysis beyond statutory interpretation of the ECPA was necessary to conclude that the attorney-client privilege is protected from lawful or unlawful accesses or interceptions of electronic communications, but legal principles alone protect the privilege. Perhaps Mr. Gidari's approach, strict reliance on legal protections and use of technology only if business judgment so suggests, is appropriate.

In reality, however, it is not. Mr. Gidari's analysis of the

---

[195] *See id.* at 461-63. Recall the difference in treatment between stored wire and stored electronic communications discussed *supra* at note 156 and accompanying text.

[196] *Steve Jackson Games, Inc.*, 36 F.3d at 461-62.

[197] *See id.* at 458.

[198] *See* Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (holding that no interception of electronic communications in the form of alphanumeric pages is possible when the electronic communications are in storage); United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996) (holding that seizure of pagers containing private, unread messages did not constitute an intercept under the ECPA).

[199] *See* Gidari, *supra* note 170, at 2.

[200] *See supra* notes 111-14 and accompanying text.

[201] Transamerica Computer, Inc. v. International Bus. Machines, Corp., 573 F.2d 646, 651 (9th Cir. 1978) (emphasis omitted). A lawful access under the ECPA of a stored electronic communication will not affect the privilege that attached to the communication.

ECPA's effect on the attorney-client privilege may be accurate, but his proposal is misleading and overbroad. There are issues beyond the scope of Mr. Gidari's article, yet the article's tenor suggests to the reader that the only issue that exists for the attorney and client when conveying confidential communications over the Internet is loss of privilege through interception or access. He states, for example, "there are . . . real *business* risks associated with the use of digital communications today . . . but privilege waiver probably is not one of them."[202] He also states "[i]n the end, the degree of privacy necessary for communications should be a *business* decision."[203] Certainly business decisions are going to be a piece of the attorney and client's determination of whether to use electronic mail to convey confidential information. Business decisions and the issue of waiver of the attorney-client privilege by interception or access are not the only elements of the decision, though.

As previously discussed,[204] waiver of the attorney-client privilege may occur inadvertently, without third party interception or access. The traditional, subjective intent approach to this scenario protects the electronic mail utilizing attorney and client.[205] Also, in the appropriate fact pattern, the factor test will provide protection.[206] But there is a third approach: some jurisdictions hold that unintentional disclosure *always* amounts to a waiver.[207] This "strict responsibility approach" to waiver of the attorney-client privilege places a great burden on the attorney and client, waiving the privilege after an inadvertent disclosure despite any reasonable care taken to prevent the disclosure.[208]

The jurisdictions that adopt the strict responsibility approach look to realism rather than theory. These jurisdictions reject the notion that only the client may waive the privilege,[209] and also question the relative conduct approach's examination into the precautions taken to protect the privileged document. Courts that adopt the strict responsibility approach state that such an examination is a fiction: the existence of the disclosure manifests the insufficiency of the precautions taken.[210] Under this theory, no party is granted the benefit of the privilege if they fail to treat their privileged

---

202. Gidari, *supra* note 170, at 1 (emphasis added).

203. *Id.* at 3 (emphasis added).

204. *See supra* notes 115-18, 161-69 and accompanying text.

205. *See supra* notes 115, 161-63 and accompanying text.

206. *See supra* notes 117, 164-69 and accompanying text.

207. *See supra* note 116 and accompanying text.

208. *See* Underwater Storage, Inc. v. United States Rubber Co., 314 F. Supp. 546, 549 (D.C. Dist. 1970).

209. *See id.*

210. *See, e.g.*, United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461, 465 (E.D. Mich. 1954).

communication "like jewels—if not crown jewels."[211]

There is no legal protection afforded the missent e-mail message in jurisdictions that follow the strict responsibility approach. The possibility that human error can cause waiver of the attorney-client privilege suggests that legal protections alone are not sufficient to decrease the dangers of lost confidentiality in those jurisdictions.

Legal protections alone are also insufficient to prevent disciplinary sanctions. Sanctions such as a reprimand and an admonishment may be imposed upon the attorney for negligently revealing client confidences.[212] Presently there is no established legal standard stating that using electronic mail to convey client confidences without security technology is reasonable. The ECPA's outlaw of an interception of electronic communications does not guarantee that a disciplinary proceeding would find an attorney not negligent for relying on e-mail.

Besides leaving open the effect of an inadvertent disclosure and failing to prevent disciplinary sanctions, the legal protections available do not prevent an attorney malpractice claim based on a failure to maintain confidentiality while using e-mail. Recall that unique to the claim of attorney malpractice is an inquiry into whether the attorney acted in accordance with the standard behavior of his or her professional community.[213] Presently there is no standard protocol within the legal community regarding the use of electronic mail. Encryption is not widely used, and there is evidence that even external e-mail is not yet widely used.[214] This does not imply that technological protection is not required, though. "[A] whole calling may have unduly lagged in the adoption of new and available devices. . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."[215]

Sole reliance on legal systems does not provide complete protection for the attorney and client. Existing legal protections mitigate the effects of lost confidentiality, but do not fully remove them. This suggests that to ensure the appropriate use of e-mail, the legal community should consider imposing upon itself a duty to use technological protections. Has such a duty developed?

---

[211] *In re* Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989).

[212] *See supra* notes 91-93 and accompanying text. Note that harm does not need to be established for an admonishment to be administered.

[213] *See supra* notes 102-03 and accompanying text.

[214] *See supra* note 59.

[215] The T.J. Hooper v. Northern Barge Corp., 60 F.2d 737, 740 (2d Cir. 1932) (holding a tug unseaworthy because of its unreasonable failure to have a weather radio aboard, even though the custom in the tug industry was to not carry a radio).

2. Proposed Strategy #2: The Duty to Use Technology

Articles currently being published advise lawyers that cryptography is the solution to Internet based confidentiality concerns.[216] The articles identify the benefits that technologies such as cryptography provide to the legal community, but the commentators have not suggested that there is, or should be, a duty to use such technology. Bar Associations, however, have.

a. Effect of Bar Association Ethics Opinions

Bar Association ethics opinions, promulgated by the ABA Committee on Ethics and Professional Responsibility (ABA Committee), and by committees in all but seven states, are "a means by which the bar establishment can affirm its conception of the appropriate . . . attitudes of lawyers."[217] Advisory opinions are promulgated under different systems depending on the lawyer's home state. Many bar committees follow the ABA Committee's approach of issuing formal opinions on matters of general interest to the bar and informal opinions responding to more specific inquiries.[218] Some states have developed their own systems of opinion issuance.[219]

In all states, however, the typical purpose of ethics opinions is to assist lawyers in interpreting the ethics rules of their states.[220] The committees examine the lawyer codes adopted by their states and determine ethical courses of conduct given fact patterns posed by bar members. By posing a question to his or her state's ethics committee as to the appropriate use of electronic mail, an attorney may therefore increase his or her understanding of the ethical duty with respect to e-mail use, and decrease the potential for disciplinary sanctions.

b. The Opinions

Attorneys in both North Carolina and Iowa have presented the issue of electronic mail use to their state bar ethics committees.

---

216. *See supra* note 122 and accompanying text; *see also* Elsa Kramer, *The Ethics of E-Mail: Litigation Takes On One Of The Challenges of Cyberspace*, RES GESTAE, Jan. 1996 at 24, 27 ("All security experts are in agreement about the necessity of encrypting e-mail. . . ."); Merrill, *supra* note 28, at 23 ("[I]t is possible today for a user to use public key cryptography to encrypt the data itself in a completely secure manner.").

217. CHARLES W. WOLFRAM, MODERN LEGAL ETHICS 65 (1986).

218. *See* Whitney A. McCaslin, *Empowering Ethics Committees*, 9 GEO. J. LEGAL ETHICS 959, 974 (1996).

219. *See id.*

220. *See id.* at 964.

i. North Carolina

A North Carolina attorney posed an inquiry to the North Carolina State Bar requesting an interpretation of "a lawyer's ethical obligation when using electronic mail to communicate confidential client information."[221] The North Carolina attorney asked whether the electronic mail medium could be used and if so whether it could be used without security technology. The response opinion, entitled "Modern Communications Technology and the Duty of Confidentiality," was published on April 13, 1995.[222] The opinion concluded that while utilizing electronic mail, or any other insecure medium of communication,[223] precautions need to be taken to protect client confidentiality.[224] The precautions are not explicitly technological, but are twofold:

> First, the lawyer must use reasonable care to select a mode of communication that, in light of the exigencies of the existing circumstances, will best maintain any confidential information that might be conveyed in the communication. Second, if the lawyer knows or has reason to believe that the communication is over a telecommunication device that is susceptible to interception, the lawyer must advise the other parties to the communication of the risks of interception and the potential for confidentiality to be lost.[225]

The Bar thus concluded that while using electronic mail or any other technology "susceptible to interception,"[226] the lawyer's first duty is to use reasonable care to select a mode of communication which best maintains confidentiality. The lawyer's second duty is to inform the client or peer with whom he or she is communicating via telecommunication modes susceptible to interception, that confidentiality may be lost.[227]

ii. Iowa

An Iowa attorney has also recently inquired into the propriety of communicating confidentially with clients via electronic mail, asking whether an Iowa law firm could use the Internet for electronic communications with clients.

---

221. North Carolina State Bar, Published Op. 215 (1995).
222. *Id.*
223. *See id.* (discussing the insecurity of cordless and cellular telephones as well).
224. *See id.*
225. *Id.*
226. *Id.*
227. *See id.*

The responding Formal Opinion, "Lawyer Home Page or Web Site on the Internet," dated August 29, 1996, explicitly interprets the lawyer's ethical responsibility of maintaining confidentiality as including a duty to use technology.[228] The Iowa Supreme Court Board of Professional Ethics and Conduct opined that the ethical duty to maintain client confidences found in DR 4-101[229] requires that "sensitive material" sent to or received by clients by e-mail must be "encrypted or protected by password/firewall or [another] generally accepted . . . security system."[230] Written acknowledgment by a client of the risk of violation of DR 4-101, and consent to e-mail's use, can be obtained instead.[231] This ethical opinion places a duty on the attorney to either secure sensitive material with technology, or obtain informed consent from the client regarding e-mail use.

iii. The Opinions' Applicability

The Iowa and North Carolina ethics committees' intentions are meritorious, encouraging attorneys to use the most secure mode when communicating with clients. Should the lawyer codes be read to impose a duty to use technology, though?

The existing, explicit duty of confidentiality found in the lawyers codes imposes upon the legal community the duty to *not reveal* client confidences. The language of the Model Rules is negative: "A lawyer shall *not* reveal. . . ."[232] DR 4-101 of the Model Code also states the attorney's basis for discipline in the negative.[233] Relying on this negative language of the codes, one recognizes that knowing or intentional revelations of client confidences are improper. The Model Code even incorporated a knowledge requirement into its DR 4-101, prohibiting a lawyer from "knowingly" revealing client confidences.[234]

Within this negative duty, however, is the positive duty to *protect* client confidences. The Model Code's Canon 4 expressly states that the axiomatic norm is preservation.[235] Comment to the Model Rules states that "[t]he common law recognizes that the

---

[228] Iowa Supreme Court Board of Professional Ethics and Conduct, Formal Op. 96-1 (1996).

[229] Iowa's DR 4-101 is identical to the Model Code's DR 4-101. *See* IOWA CODE OF PROFESSIONAL RESPONSIBILITY FOR LAWYERS DR 4-101 (1993).

[230] Iowa Supreme Court Board of Professional Ethics and Conduct, Formal Op. 96-1 (1996).

[231] *See id.*

[232] MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6(a) (1995) (emphasis added).

[233] *See supra* note 83.

[234] *See* MODEL CODE OF PROFESSIONAL RESPONSIBILITY DR 4-101(B) (1983).

[235] *See supra* note 82.

client's confidences must be protected from disclosure."[236] By focusing on the positive duty, rather than the negative duty, it is easier to recognize that negligent revelation is likewise prohibited. The attorney *must not* take steps that will reveal client confidences, and the attorney *must* take steps to preserve client confidences.

It is under the guise of preservation and protection that North Carolina and Iowa have incorporated the duty to use technology into their readings of their lawyers' codes. How better to protect client confidences than with technological protections on the medium through which the confidence is transmitted? Technology lessens the danger of losing confidentiality in the first place.

The explicit imposition of a technology specific duty in the Iowa opinion fails, though, because it will discourage e-mail's use. First, the incorporation of specific security controls in the opinion discourages e-mail's use because it implies that electronic mail is unique from other communication technologies. Special controls are explicitly stated as required for use with e-mail, but if, as the Introduction to this Note suggests, eavesdropping on communications has been a problem since the invention of the telegraph,[237] then why is the adoption of a duty to protect with specific technology only appropriate for e-mail? What special technologies need to be used to insure the maintenance of confidentiality over cellular telephones, cordless telephones, facsimile machines or the telex?[238] Because Iowa has not explicitly informed its constituency of any special technological protection requirements for these media, the Iowa bar may lead to the incorrect conclusion that e-mail is relatively more insecure than any of the other communication media available. This discourages e-mail use, an undesirable outcome considering the great benefits e-mail offers the attorney and client.[239]

Second, the use of language such as "encryption" and "password/firewall" may promote the misperception that e-mail is more insecure than other communication technologies. The controls that must be placed upon e-mail to ensure its security sound ominous, much more so than the commonly accepted protection on a fax machine transmission: a confidential legend.[240] For attorneys who

---

[236] MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 cmt. (1995).

[237] *See supra* notes 4-8 and accompanying text.

[238] Each of these media are used in the legal profession, but each has limitations. For an overview of communications technologies used in the legal profession, see generally WRIGHT, *supra* note 2.

[239] *See supra* Part II.B.

[240] *See* Bruckner-Harvey, *supra* note 167, at 393 (discussing the use of a confidential legend to prevent waiver of the attorney-client privilege after an inadvertent disclosure of a fax).

know little about electronic mail or the technology involved with it, a reading of Iowa's opinion may deter them from ever finding out more. E-mail will be rejected as too troublesome.

North Carolina's opinion also fails because it too discourages attorneys from using electronic mail, but for a different reason: ambiguity. The North Carolina State Bar states that attorneys do not have to use the most infallible method of communication, but they must use the best method.[241] This statement leaves unanswered whether secured electronic mail may be used in place of the fax machine or telephone. North Carolina has not told its lawyers which communication medium is, in fact, the best. Nor has it told its bar how it should go about determining what communication medium is the best. In order safely to comply with the North Carolina opinion members of the North Carolina bar will likely forgo use of electronic mail and use a communications technology with which they are more secure, but which offers fewer benefits than the e-mail format.

Imposing a specific duty to use technology is thus inappropriate. The Iowa opinion that attempted to do so poses a threat of preventing increased use of e-mail in the legal community. The imposition of a very broad duty to use the "most secure" method of communication is also unworkable. The North Carolina opinion simply restates the question posed, serving only to confuse its Bar.

Both opinions do recognize, however, the positive duty of the attorney to preserve and protect client communications. It is this positive duty that should be taken from the opinions and incorporated into the appropriate strategy.

B. The Appropriate Strategy

The appropriate strategy to adopt in bar opinions is recognition that there is a duty implicit in the Model Code and Model Rules to take all steps reasonable under the circumstances to protect client communications when using modern communication technologies such as electronic mail. This encourages e-mail using attorneys to examine the legal protections and the technological protections afforded electronic mail. It will encourage the use of an adequate combination of both, without failing for the reasons that Iowa's and North Carolina's opinions fail.

---

[241] *See supra* note 221.

1. Why Bar Opinions?

Bar Association opinions are the appropriate place to establish the duty of care with respect to the use of e-mail. Opinions offer an issuing state's attorneys an interpretation of their ethical duty of confidentiality, enabling attorneys to modify their conduct before confidentiality is lost. If confidentiality is mistakenly lost, there may be less chance of disciplinary action taken against the attorney as he or she will have acted in accordance with the state bar's suggestions. Bar opinions are also the appropriate medium because they are not permanent. Ethics opinions are not opinions on questions of law.[242] Matters important to lawyers that are timely are appropriate inquiries;[243] if the legal landscape changes, so can the opinion. Matters regarding the duties associated with the use of a specific technology are timely. Already, changes in electronic mail are occurring in the telecommunications industry[244] that, if adopted by the legal profession, will cause lawyers again to rethink the nature of their confidentiality duty. Bar opinions provide the forum for frequent reexamination of the issue.

Bar opinions are also important because they can effectively stimulate the adoption of a community standard. Attorneys look to opinions, before any harm results, for an indication of what "the herd" is and should be doing.[245] Attorneys then adapt their behavior to "the herd's." If harm does occur, reliance on the community standard can be used as a defense in an attorney malpractice case. Likewise, in cases in which it must be shown that reasonable steps were taken to prevent an inadvertent disclosure of client communications, adherence to the community standard may be used to show reasonable precautions taken.

Iowa's and North Carolina's attempts to aid their attorneys in developing a strategy for controlling the risks associated with electronic mail are accurate to the extent that each relies on an ethics opinion to convey the strategy. Their proposals fail, however, because the strategies they convey are improper. The appropriate strategy is found in The Restatement of the Law Governing Lawyers.

---

242. *See* WOLFRAM, *supra* note 217, at 67.

243. *See id.* at 66-67.

244. A cellular phone with an attached miniature keyboard permits users to send and receive electronic mail wirelessly. *See* Wayne Cunningham *Forget PC's: The Internet is Going Pocket-Sized*, THE NET, Dec. 1996, at 12. Alphanumeric pagers can now receive electronic mail from a PC. *See E-Mail You Can't Escape*, THE NET, Mar. 1997, at 27.

245. *See* WOLFRAM, *supra* note 217, at 65.

2. The Positive Duty

The Restatement of the Law Governing Lawyers accurately summarizes the duty of confidentiality that the attorney holds. To safeguard client confidences the lawyer has a duty "not to use or disclose [client] information if doing so poses a risk to the interests of the client."[246] This negative duty is representative of the principle set forth in Rule 1.6 of the Model Rules and DR 4-101 of the Model Code. The lawyer shall not reveal the confidences of the client unless the revelation falls into one of the excepted categories.

The Restatement goes one step further. The Restatement states that the lawyer "shall take steps reasonable under the circumstances to protect confidential client information . . . against use or disclosure by others that may adversely affect a material interest of the client."[247] This positive duty is found implicitly in the Model Rules and Model Code, and should be the foundation of ethics opinions broaching the subject of whether electronic mail can be used to carry confidential information in the practice of law.

Incorporating, into bar opinions, the duty of the lawyer to take steps reasonable under the circumstances is the appropriate strategy for two reasons. First, the positive duty standard is in alignment with the legal protections afforded electronic mail. To prevent disciplinary sanctions, for example, the attorney must not have negligently revealed client confidences. The negligence standard recognizes a duty to act reasonably under the circumstances. Also, a claim of attorney malpractice will only succeed if it can be shown that the attorney acted unreasonably vis-à-vis his or her colleagues. In addition, the relative conduct jurisdiction in inadvertent disclosure cases will examine whether the attorney took reasonable precautions to prevent the disclosure.

The second reason the positive duty is appropriate is because its adoption in bar opinions encourages the use of technology without explicitly mandating it. Attorneys will look to their state bar opinions for guidance, and be told that there is a duty to take affirmative steps to protect the contents of electronic mail communications. This will lead an attorney to examine the legal protections afforded the medium, enabling the attorney to determine for him- or herself whether or not the law provides adequate protection. The attorney will then determine whether he or she is required to take the additional step of employing security technology

---

[246] RESTATEMENT OF THE LAW GOVERNING LAWYERS § 111 cmt. (Tentative Draft No. 3, 1990).

[247] *Id.* § 111(2).

with his or her electronic mail communications. If the attorney wishes to use security technology, he or she can personally determine the nature of such security technology. In effect, Albert Gidari's business judgment approach will become mandatory.

3. The Model Opinion

The New York City Bar, in an opinion dealing with the use of cellular and cordless technologies in the practice of law, addressed whether confidential communications could be made over such modes of communication.[248] The New York City Bar adopted the language of the Restatement of the Law Governing Lawyers in answering the inquiry,[249] and provided a model that other states should adopt in addressing the question of how to control the risks associated with electronic mail. By modeling their opinions after New York City's, bars will inform their attorneys that the use of new communications technologies is appropriate if positive steps are taken to assess the medium's security. This assessment will then lead attorneys to the conclusion that the use of a reasonable amount of technology to secure the medium is sufficient risk management.

Bar association opinions should conclude:

> A lawyer who possesses . . . [confidential communications] must take "reasonable steps to secure the information against misuse of inappropriate disclosure" including steps necessary to assure that "the lawyer and the lawyer's associates or agents acquire, store, retrieve, and transmit confidential information for the lawyer's clients under systems and controls that maintain confidentiality.". . . . There is no question that [electronic mail is] a great convenience to the public in general. Lawyers, however, owe their clients a solemn duty of confidentiality, and thus should take steps to avoid the danger of . . . disclosure of client confidences . . . through the use of non-private means of communication.[250]

IV. CONCLUSION

Electronic mail is a mode of communication that is providing, and that will continue to provide, great advantages to the legal profession. The medium offers efficiency, speed, and a means of

---

[248] *See* New York City Comm. on Professional and Judicial Ethics, Formal Op. 1994-11 (1994).

[249] *See id.*

[250] *Id.*

effective written communication. Competitiveness in an increasingly technological society demands its use. But it is not without security risk. Hackers and unscrupulous system administrators may intercept communications and infallible users may cause an inadvertent disclosure of an e-mail's contents. The existing legal framework compounds the problem by remaining insufficient to provide adequate protection of electronic mail, but technology does exist that can provide the basis for enabling e-mail's use. Bar association ethics opinions, with their ability to adapt to a changing legal and technological environment quickly, should lead the way in creating community standards with respect to electronic mail. Rather than specifically imposing a duty to use security technology, though, the opinions need to recognize clearly that a general, affirmative duty to protect client confidences exists. This approach will encourage attorneys to use the medium, but only after a risk management assessment. The conclusion of the risk management assessment will be that an appropriate mix of reliance on legal and technological protections is the best strategy to use in association with electronic mail.

COLLEEN L. REST