Nebraska Law Review

Volume 78 | Issue 2 Article 5

1999

E-mail Privacy: An Oxymoron?

Micalyn S. Harris
Winpro, Inc., msharris@adr-ny.com

Micalyn S. Harris*

E-mail Privacy: An Oxymoron?

TABLE OF CONTENTS

I. INTRODUCTION

Electronic communication, "e-mail," is wonderful. It provides fast, efficient, inexpensive, seemingly instant communication. No more telephone tag. No more overnighting documents via expensive messenger services. No wonder the use of e-mail is burgeoning. Even the most computer-phobic lawyers have embraced it.

Articles in newspapers and professional journals have alerted lawyers to the possibility that the absolute confidentiality of unencrypted e-mail traveling across the Internet cannot be assured. Concerns regarding the possibility that using e-mail may, in some circumstances, effectively waive the attorney-client privilege[1] have led several states to adopt legislation providing that the use of e-mail, in and of itself,

* Ms. Harris, a graduate of Wellesley College and the University of Chicago Law School, is Vice President, Secretary and General Counsel of Winpro, Inc., a computer software consulting, design and development company with offices in New Jersey and New York City's "Silicon Alley."

The author wishes to thank Louis J. Cutrona, Jr., Ph.D., President, Winpro, Inc., who patiently reviewed several drafts of this article for technical accuracy. The views expressed are solely those of the author.

1. *See, e.g., Court to Rethink Encryption Case*, N.Y. TIMES, Friday, Oct. 3, 1999 at C5.

does not destroy the attorney-client privilege.[2] Some state ethics committees have taken the position that, because of the possibility of interception, e-mail should not be used for attorney-client communication unless the messages are encrypted or the client has been made aware of the risk and consented to use of the "insecure" communication.[3] Other state ethics committees have taken the position that use of e-mail is no more subject to interception than is a telephone conversation, and therefore, there is a reasonable expectation that e-mail will remain private, making use of unencrypted e-mail across the Internet ethically acceptable.[4]

E-mail has been likened to cellular telephones,[5] landline telephones,[6] and use of postcards through the United States Postal Service.[7] At least one court (in considering the nature of unencrypted Internet transmission of sexually explicit materials) has recognized that it is not appropriate to consider e-mail to be a "sealed" mode of transmission.[8] The court, however, suggested that cautionary lan-

2. *See, e.g.*, N.Y. C.P.L.R. 4547 (McKinney Supp. 1990) (codifying for purposes of the rules of evidence that electronic communication, in itself, does not render privileged communication non-privileged). California considered, but did not adopt, similar legislation, whether because it was deemed unnecessary, or because e-mail is deemed by that legislature too insecure to place beyond challenge or for other reasons is not clear.

3. *See* Iowa Sup. Ct. Bd. of Professional Ethics and Conduct, Op. 96-01 (1996) [hereinafter Iowa Ethics Op. 96-01] (warning that the failure to obtain written consent for internet communications or to protect the transmissions with encryption would result in a violation of IOWA CODE OF PROFESSIONAL RESPONSIBILITY FOR LAWYERS DR 4-101); *see also* Arizona State Bar Ass'n, Comm. on Rules of Professional Conduct, Op. 97-04 (1997) [hereinafter Ariz. Ethics Op. 97-04] (recommending that lawyers use encryption or warn clients of the risks associated with e-mail). The Iowa opinion was later amended to allow counsel and client to agree on the type of protection afforded their communications. *See* Iowa Sup. Ct. Bd. of Professional Ethics and Conduct, Op. 97-01 (1997) [hereinafter Iowa Ethics Op. 97-01].

4. *See, e.g.*, Illinois State Bar Ass'n, Comm. on Professional Responsibility, Advisory Op. 96-10 (1997) [hereinafter Ill. Ethics Op. 96-10].

5. *See id.*; New York State Bar Ass'n, Comm. on Professional Ethics, Op. 709 (September, 1998) [hereinafter N.Y. Ethics Op. 709].

6. *See* Todd H. Flaming, *Internet E-Mail and the Attorney-Client Privilege*, 85 ILL. B.J. 183 (1997).

7. *See, e.g.*, William Freivogel, *Communicating with or About Clients on the Internet: Legal, Ethical, and Liability Concerns*, 17 ALAS LOSS PREVENTION J. 17, 18 (1996) (noting that technical articles frequently liken Internet messages to postcards, leading legal writers to conclude that "[t]here is no reasonable expectation of privacy"). Freivogel, however, disagrees with this analogy: "It is important to remember that the hacker's activity is as criminal as the wiretapper's." *Id.* (citing 18 U.S.C. §§ 2510-2520). The majority of states allow lawyers to transmit confidential information without encryption. *See* ALAS LOSS PREVENTION BULL., No. 98-27 (October 19, 1998). *But see* Richard E.V. Harris, *Electronic Communications and the Law of Privilege*, 11 CAL. LITIG. 14 (1997).

8. *See* ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 884 (1997).

guage similar to that commonly used on facsimile transmissions might be sufficient protection,[9] thus analogizing e-mail to those transmissions. The absence of uniformity indicates that none of these analyses is sufficiently persuasive to be regarded as definitive.

As a result, state bar associations, ethics committees, and commentators have taken positions ranging from (i) e-mail is not so insecure as to constitute failure to protect client confidentiality obligations, to (ii) e-mail, at least unencrypted e-mail traveling across the Internet, *is* that insecure, and therefore use of unencrypted e-mail traveling across the Internet may, in some cases, risk both a waiver of the attorney-client privilege and a breach of the lawyer's ethical obligations to protect clients' confidential information.

II. THE ISSUE

The central issue is: What are the legal, ethical and practical considerations involved in utilizing e-mail for attorney-client communication? Subsidiary issues include: Will the use of e-mail, in and of itself, risk forfeiting the attorney-client privilege in connection with a demand for discovery, on the ground that communication across the Internet via e-mail has been likened to sending a postcard through the mail, and using a postcard to communicate information may be seen as indicating that the information is not regarded by the sender as confidential? Even if the attorney-client privilege is not at risk, will an attorney using unencrypted e-mail be vulnerable to accusations of unethical practice for failure to protect a client's confidences? Is the use of e-mail, even if not unethical or a risk to the attorney-client privilege, unwise because there is a high risk of unintended disclosure with resulting damage to the attorney-client relationship?

III. AUTHOR'S SUMMARY

The author believes that the use of e-mail, in and of itself, should not waive the attorney-client or work-product privileges and should not, in and of itself, subject an attorney to liability for ethical violations or claims of unethical behavior based on a failure to adequately protect client confidences.

On the other hand, lawyers, and their clients, need to consider the fact that e-mail is a unique form of communication. E-mail feels like a telephone conversation, but technically, it is quite different, and produces a document that is likely to be casually worded and long-lived. Accordingly, attorneys and their clients are well advised to become familiar with their e-mail systems and to develop policies and proce-

9. *See id.* at 844-45.

dures designed to assure maximally-effective use and minimize the risk of unintended and inappropriate disclosure.

For purposes of analyzing whether attorney-client privilege is at risk, the key issue is whether, in communicating by e-mail, an attorney and client have a reasonable expectation of privacy. Because the factual situations and contexts in which e-mail is used vary widely, whether particular arrangements provide a "reasonable expectation of privacy," and thus conform to the evidentiary standard required in connection with asserting attorney-client privilege, is likely to be a question of fact.

Whether there is a sufficient "reasonable expectation of privacy" to support an assertion of the attorney-client and work-product privileges, which are rules of evidence, is separate from the issues relating to whether use of unencrypted e-mail raises ethical issues regarding potential failure to treat confidential client communications as confidential. In order to emphasize that distinction and separate facts, case law, and theoretical discussion, this article is divided into five sections: Factual Background; Case Law Regarding the Attorney-Client and the Related Attorney Work-Product Privileges; a Summary of State Ethical Opinions Regarding Use of E-mail; Risks; and Recommendations.

IV. FACTUAL BACKGROUND

Law firms are installing a variety of internal systems that permit lawyers to communicate with one another: some permit communication within a single office, some permit communication among regional offices, and some permit communication with one or more offices from outside the system. Corporations are also installing internal systems that permit lawyers to communicate with one another and with their corporate clients: again, within the corporate headquarters, from outlying locations, and from outside the internal system. Law firms are connecting electronically with their clients. Sometimes these are via direct, dedicated connections. Sometimes they permit clients to have limited access to a firm's internal system. Sometimes these arrangements give outside counsel access to the corporate client's system. Access, when given, may be provided in various ways. For example, access may be provided by an outside provider, such as AT&T or America Online, as a means of exchanging e-mail. These arrangements, in turn, may vary. For example, such e-mail may be exchanged either through the provider's general system or within a special, dedicated area of the system with limited access. Where attorney and client use different e-mail providers, the e-mail may move directly between providers, or, in order to move from one provider to another, may move across the Internet.

Some firms have systems that automatically encrypt all messages exchanged within the system and between the system and the outside world, in some cases without its users being aware of the encryption process. Some firms require passwords or other identification and authentication procedures before a message is sent or received. Some organizations have e-mail policies that set forth practices and procedures for using e-mail, including for what purposes it may and may not be used; others have no policies, procedures or limitations on the use of e-mail by employees, agents or others, including their lawyers.

E-mail on an internal "intranet" system may or may not be encrypted, and may be read by the system administrator (or not, if it is encrypted), depending upon the system and how it is configured and used. The variations among systems are even more diverse. Communication on a private intranet is likely to go straight to the organization's e-mail server and remain there until retrieved. Communication within a given service provider is likely to go to the service provider's server and remain there until retrieved. Communication from one service provider to another is likely to travel across the Internet, a process which may involve passing the message from server to server, across a varying number of servers and via a route that cannot be predetermined.

Simply stated, all e-mail is not created equal.

Where e-mail moves via a direct connection from the sender's to the receiver's system, for example, via modem to modem, the connection is, like a telephone call, simultaneous. Where, however, e-mail communication is across the Internet, the communication is made via a series of relays, that is, a "connectionless" system, and thus technically different from a telephone call or a facsimile connection.

The Internet can be envisioned as a huge number of computer systems linked together, some of which are set up to send and receive e-mail. (A system for this conceptual purpose may be of any size, from a small desktop computer to a large mainframe.) Each system set up to send and receive e-mail is able and willing to send and receive messages directed to anyone, to sort the messages and keep those addressed to it, and to pass on those messages addressed to other systems.

The Internet was originally designed by the United States Department of Defense, with the objective of assuring that messages reach their destinations somehow, even if parts of the Internet were cut off. Thus, the specific route, or even most likely route, of a particular message is never known with certainty in advance. It may be determined in retrospect, however. At the beginning of many e-mail messages that have traveled across the Internet is a list of addresses, generally unfamiliar to the final addressee. These are the addresses of the systems through which the message has passed en route to the

addressee. Long messages may be broken into "packets" which are reassembled at each intermediate system through which the message passes as well as at their final destination.

It is worth noting that the Department of Defense did not envision sending confidential information unencrypted. It had, and continues to have, different levels of encryption (and alternative communication channels), and depending upon its own set of classifications, it sends messages at whatever level of encryption is determined to be appropriate for the information involved. The more secret the information, the more complex the encryption code, and the longer the time required to encrypt and decrypt the message.

Each system that participates in the Internet has at least one system administrator. That person, in order to keep the system operating efficiently, may, like the system administrator of a commercial system, review messages on the system to assure the system's orderly functioning.[10] This review process by system administrators is not "interception" or "hacking." There is nothing illegal or improper in the owner of a computer system reviewing messages on the system. Where messages travel across the Internet, there may or may not be any contractual relationship (e.g., such as might be established between an e-mail user and a commercial service) between sender or receiver and these system owners requiring that confidentiality be maintained. There are statutory obligations of confidentiality imposed on commercial system administrators. These may or may not apply to unrelated non-commercial system administrators. Note, however, that obligations of confidentiality do not mean that such system administrators cannot see e-mail on their systems, but only that they have an obligation not to disclose the information to third parties, or to use the information for their personal benefit.[11] In fact, it is

10. Note that this review does not require "opening" messages. Unlike letters placed in envelopes, which must be opened to be read, to a system administrator, e-mail messages appear immediately following their address blocks, and are followed by the address block of the next message. Unlike the addressee, who generally sees a list of messages identified by sender and subject, the system administrator sees a continuous text that does not separate addresses from text.

11. *See* discussion *infra* Part VIII (Risk 1). The imposition of confidentiality obligations on non-commercial system administrators may raise a variety of issues relating to whether they will know the information is confidential, and whether, in some circumstances, they may have a duty to disclose or investigate, as for example if they come across e-mail indicating that a crime threatening death or serious bodily harm is about to be committed. *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989) (an account of a student system administrator who concluded he did have an obligation, as an administrator and citizen, to report a billing discrepancy in a university system. Exploration of the discrepancy uncovered unauthorized, Germany-based entry into a United States military computer system through the university's computer system).

clear that system administrators will, under appropriate circumstances, have legal access to confidential messages passing through the service provider's system. Therefore, disclosure of confidential information is a risk even when a third party administrator's obligations of maintaining its confidentiality may mean that the attorney-client privilege has not been jeopardized.

V. CASE LAW REGARDING THE ATTORNEY-CLIENT AND RELATED ATTORNEY WORK-PRODUCT PRIVILEGES

The attorney-client privilege is a rule of evidence that prohibits access by third parties to certain communications between attorney and client. It is generally cited in support of the asserting party's refusal to provide information or materials sought by the opposing party in the course of litigation.[12] Similarly, the related work-product privilege prohibits access by third parties to certain kinds of information created by an attorney, (and sometimes among attorneys), in connection with a particular matter in litigation. Because these communications are generally highly reliable and of great interest to opposing counsel and the trier of fact (judge or jury), in order to assert these privileges, there are stringent requirements as to how communications and other materials sought to be protected by these privileges must be handled. In general, failure to treat information sought to be protected by the attorney-client or work-product privilege as "confidential" risks waiving the privilege.[13]

Simply designating information as "privileged and confidential" does not, merely by virtue of such designation, entitle it to the protection of the attorney-client privilege, even when the information is directed to or comes from an attorney (whether in-house or outside counsel). Certain standards must be met. Various courts have enunciated these in various ways. The touchstones of maintaining the attorney-client privilege may be summarized as follows: (i) legal advice which is sought from a lawyer, in his or her capacity as such, and (ii) the communications relating to that purpose are made in confidence by the client and at its insistence permanently protected from disclosure by the client or the legal advisor.[14] In addition, for a corporation to assert the attorney-client privilege, the corporation must be able to show that: (i) the information was disclosed by a corporate employee

12. *See* FED. R. CIV. P. 26(b)(1) ("Parties may obtain discovery regarding any matter, not privileged . . . ."); FED. R. EVID. 501 ("[T]he privilege of a witness . . . shall be governed by the principles of the common law . . . .").

13. *See* 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2311 (John T. McNaughton ed., rev. ed. 1961).

14. *See* Radiant Burners, Inc. v. American Gas Ass'n, 320 F.2d 314, 318-19 (7th Cir. 1963) (citing 8 WIGMORE, *supra* note 13, §§ 2285, 2292); *see also* 8 WIGMORE, *supra* note 13, § 2321.

acting within the scope of the employee's corporate duties, (ii) the employee was seeking legal advice from counsel, (iii) the information was considered confidential when made available, and (iv) its confidentiality has been maintained.[15]

Maintaining confidentiality within a corporation requires that communication of the privileged information be limited to those employees and agents of the corporation who have a need to know it.[16] If the information becomes generally available, (within the corporation), it is regarded as not being treated as confidential information and, at least arguably, the privilege may have been waived.[17]

The related work-product privilege permits withholding certain information from discovery to prevent invasion of the privacy of an attorney's trial preparation.[18] Like attorney-client privileged materials, work-product materials must be treated as confidential, although the scope of people to whom these materials may be disclosed may be broader than the disclosure permitted in connection with maintaining the attorney-client privilege.[19]

The attorney-client privilege is absolute although the client may waive it. Waiver may also occur (in fact, may be most likely to occur) inadvertently. Where the client does not continue to treat information as confidential, the attorney-client privilege may be lost. For example, such loss may occur when attorney-client privileged information is discussed with employees of a corporation who attend a meeting (and by analogy, receive documents or participate in e-mail discussions) outside the scope of their duties to the corporation.[20] During the course of litigation, counsel may, for example, argue that the use of e-mail involved the risk of interception and the possibility of disclosure to a third party, such as a third party system administrator, or that e-mail messages were sent to a wider group of employees than those who had a need to know. Either argument could be used to support the proposition that the information sent via e-mail was not handled as confidential, and, therefore, the attorney-client and work-product privileges had been waived. The author believes that such an argu-

15. *See* Upjohn Co. v. United States, 449 U.S. 383, 391-95 (1981).

16. *See id.* at 395.

17. *See id.* at 391-95.

18. See *Hickman v. Taylor*, 329 U.S. 495, 508 (1947), in which the court held that "memoranda, statements and mental impressions" fell outside the attorney-client privilege. The Court nevertheless determined them to be worthy of protection from discovery by opposing counsel. *See id.* at 512-13. To meet this perceived need for protection from discovery, the *Hickman* Court established a "work-product" privilege. *See id.* at 511 (quoting Hickman v. Taylor, 153 F.2d 212, 223 (3d Cir. 1945)).

19. *See, e.g.*, Diversified Indus., Inc. v. Meredith, 572 F.2d 596, 603 (8th Cir. 1978) (en banc).

20. *See, e.g., Upjohn*, 449 U.S. at 394.

ment, relating to application of the rules of evidence, should not prevail, and several states, including New York, have adopted legislation to the effect that merely transmitting e-mail across the Internet will not, in and of itself, waive the attorney-client privilege for purposes of the rules of evidence.[21] The fact that such legislation was deemed needed, or at least advisable, however, indicates that in the absence of such legislation, there is a risk that the attorney-client or work-product privilege might be lost simply by using unencrypted e-mail to communicate information otherwise protected by these privileges.

VI. SUMMARY OF ETHICS COMMITTEE OPINIONS REGARDING E-MAIL COMMUNICATIONS

The risk of actual loss of confidentiality is a separate issue from the ability to secure the protection of the attorney-client and work-product privileges under the rules of evidence.[22] Under Model Rule 1.6, a lawyer has an ethical obligation to "hold inviolate" confidential information of the client.[23] Initially, different states took inconsistent positions regarding whether the use of unencrypted e-mail constitutes a breach of a lawyer's ethical obligation to maintain confidentiality regarding a client's confidential information or a waiver of the attorney-client privilege on the grounds that by using e-mail, information was not being handled in the requisite confidential manner.

Focusing on the possibility of interception of e-mail, the Ethics Committee of the Illinois Bar Association (and those following its reasoning) came to the opposite conclusion from the Ethics Committee of the Iowa Bar. Iowa concluded that because it is possible for e-mail messages to be intercepted, lawyers should not use e-mail for sensitive communications unless the messages are encrypted or the client has consented to the "non-secure" communication.[24] Iowa initially determined that encryption would be adequate protection,[25] but after issuing its original opinion, the board reconsidered, and concluded that

21. *See supra* note 2 and accompanying text.
22. Disclosure to a company's system administrator is similar to disclosure to a secretary, and thus should not waive the privilege. When, however, messages are sent across the Internet, system administrators outside the sending or receiving organization, and their respective service providers, may have legal access to these messages because e-mail may be relayed through third parties' systems. Note that e-mail seen by system administrators is continuous. Each message immediately follows the address and is immediately followed by the address of the following message. Thus, a system administrator reviewing e-mail in the ordinary course of system administration (for example, to determine why response time had become unusually slow) would routinely see both the address and the message. Encryption would conceal the sense of the message, but indicate its length.
23. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6, n.2 (1999).
24. *See* Iowa Ethics Op. 96-01, *supra* note 3.
25. *See id.*

the means of protection should be determined by mutual agreement between the lawyer and client.[26] Arizona's ethics committee also focused on the question of interception, but took a more cautious approach, initially concluding that the answer to whether a lawyer "should" communicate with clients via unencrypted e-mail was "[m]aybe."[27] The committee concluded that a lawyer "may" communicate with a client via unencrypted e-mail without sacrificing the attorney-client privilege, but that it was "preferable," if "practical," to use encryption software or a password to protect the communication.[28]

Illinois came to the conclusion that one has a reasonable expectation of privacy when sending unencrypted e-mail over the Internet, and its reasoning has subsequently been followed by several other states, including South Carolina, Vermont, North Dakota and Kentucky. In its analysis, Illinois focused on the fact that a particular e-mail message was unlikely to be "intercepted" when traveling across the Internet and noted that the Electronic Communications Privacy Act[29] made it a crime to intercept an e-mail message. Based on these facts, Illinois concluded that such interception was no more likely than interception of a telephone conversation and therefore, that there was a reasonable expectation of privacy in using e-mail across the Internet and encryption was not necessary either to meet ethical obligations of confidentiality or to protect the confidentiality of sensitive information.[30]

VII. CASE LAW REGARDING USE OF E-MAIL

Research reveals no cases holding that use of e-mail waived the attorney-client privilege, no cases holding that use of e-mail waived work-product immunity, and no cases finding that use of e-mail for attorney-client communications was unethical.

Research also revealed no cases deciding whether: (a) the interception of confidential information sent by e-mail waives the attorney-

26. *See* Iowa Ethics Op. 97-01, *supra* note 3.

27. Using a question and answer format for its opinion, in response to the question, "Should lawyers communicate with existing clients, via e-mail, about confidential matters?," Arizona answers, "Maybe," and suggests, "Lawyers may want to have the e-mail encrypted with a password . . . . Alternatively, there is encryption software available . . . ." Ariz. Ethics Op., *supra* note 3, at 5.

28. The Arizona Committee concluded that although it is not unethical for a lawyer to use e-mail to communicate with clients, it supported encryption: "this Committee simply suggests that it is preferable to protect attorney/client communication to the extent it is practical." *Id.*

29. 18 U.S.C. §§ 2510-2522 (1994).

30. *See* Ill. Ethics Op. 96-10, *supra* note 4; *see also* N.Y. Ethics Op. 709, *supra* note 5; North Dakota State Bar Ass'n, Ethics Comm., Op. 97-09 (1997) [hereinafter N.D. Ethics Op. 97-09]; South Carolina Bar, Ethics Advisory Comm., Op. 97-08 (1997) [hereinafter S.C. Ethics Op. 97-08]; Vermont Bar Ass'n, Comm. on Professional Responsibility, Op. 97-5 (1998) [hereinafter Vermont Ethics Op. 97-5].

client privilege or breaches the attorney's obligations of confidentiality, (b) the monitoring of e-mail containing confidential information by a third party system administrator, who has no (contractual) obligations of confidentiality to the attorney or the client, waives the attorney-client privilege or breaches the attorney's obligations of confidentiality, or (c) the use of e-mail breaches an attorney's obligations of confidentiality regarding client confidences so as to form a basis for a successful malpractice suit.

There is case law indicating that a "reasonable expectation of privacy" in an e-mail transmission depends upon the specific technology and factual situation involved, and finding a reasonable expectation of privacy when the e-mail is sent between persons subscribing to the same commercial provider.[31] There is also case law stating that messages sent across the Internet are not "sealed."[32]

These cases, and the general dearth of cases dealing with sending unencrypted e-mail across the Internet, have led to uncertainty as to whether a court would find a reasonable expectation of privacy concerning such communications. As a result, some commentators have warned that "current statutes and case law are inadequate to provide the expectation of privacy necessary to invoke the protection of the attorney-client privilege" when unencrypted e-mail is sent across the Internet,[33] while others have asserted that unencrypted e-mail communications should be considered privileged.[34]

It is worth noting that the reasonable expectation of privacy is not, in and of itself, a function of either statutes or case law, but rather, of the application of overarching legal principles and public policy to an entire set of factual circumstances in each particular case. Nevertheless, the mere fact that there is currently a body of commentary warning of the absence of existing law to provide a foundation for a reasonable expectation of privacy regarding these communications

31. *See* United States v. Maxwell, 42 M.J. 568, 576 (U.S.A.F. Crim. App. 1995) (finding that defendant transmitting pornographic materials via e-mail from a provider within the *same* private on-line computer service as that used by the receiver, and requiring passwords for access, had a reasonable expectation of privacy), *rev'd in part on other grounds*, 45 M.J. 406 (C.A.A.F. 1996). *Maxwell* was a Fourth Amendment search and seizure case, and did not involve transmissions relayed across the Internet through multiple service providers. Its applicability to transmissions across the Internet is questionable.

32. *See, e.g.*, ACLU v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd*, 521 U.S. 884 (1997).

33. *See* William P. Matthews, *Encoded Confidences: Electronic Mail, The Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273, 299 (1996); *see also* Charles R. Merrill, *E-mail for Attorneys from A to Z*, 443 PLI/PATENTS 187 (Dec. 1996); Peter R. Jarvis & Bradley F. Tellam, *The Internet: New Dangers of Ethics Traps*, OR. ST. B. BULL., Dec. 1995, at 17, 17.

34. *See, e.g.*, Morgan Chu & Perry Goldberg, *E-Mail and the Attorney-Client Privilege in California*, CAL. LITIG., Fall 1997, at 18, 23.

has created a sense of unease regarding the use of e-mail for privileged and confidential communications. As indicated, even some ethics committees and commentators who do not believe that sending unencrypted e-mail messages across the Internet forfeits the attorney-client privilege nevertheless emphasize the potential risks of unwanted disclosure of sensitive information and recommend various protective measures, from warning language similar to that typically included on the cover pages of messages sent by facsimile, to the use of encryption. Some commentators have mentioned the possibility of exposure to a malpractice suit if the risk of inadvertent or unintended disclosure becomes reality.[35] These discussions are often characterized by uncertainty and ambivalence.[36]

VIII. THE RISKS

Clearly, there are risks, among them, the following:

Risk #1: A court will find that the mere use of unencrypted e-mail across the Internet to communicate otherwise privileged information constitutes a waiver of the attorney-client or work-product privilege.

A court might conclude that mere use of unencrypted e-mail across the Internet waived the attorney-client or work-product privilege on several grounds. First, under appropriate circumstances, a court might accept an argument that both sender and receiver knew, or should have known, that unencrypted e-mail traveling within an intra-firm system is read by people who have no "need to know" or that e-mail traveling across the Internet may be read by third party system administrators. Thus, because the use of e-mail involved the possibility of disclosure to such a third party, or because the e-mail messages were sent to a wider group of employees than those who had a need to know, the attorney-client and work-product privileges would be deemed to have been waived. The author believes that such an argument relating to internal distribution may prevail if internal policies disregarded obligations to limit distribution. Such obligations, however, apply to "hard" copy as well as e-mail. The primary difference is the ease with which e-mail is widely distributed.

---

35. *See* Jarvis & Tellam, *supra* note 33, at 17.

36. The ambivalence is illustrated by a reported e-mail interview, in which the commentator stated that he did not believe use of unencrypted e-mail exposed a lawyer to charges of acting unethically, but that using it was "unconscionably poor judgment." It appears that such a position is untenable. At least arguably, exercise of "unconscionably poor judgment" is, or should be, a breach of ethics. At a minimum, "unconscionably poor judgment" is likely to provide a basis for a client's termination of an attorney-client relationship, even if not a successful malpractice suit. *See* Jerry Lawson, *An Encryption Primer for Attorneys*, *in* LAWYERS ON LINE: A GUIDE TO USING THE INTERNET VI-7 (1995).

With regard to sending unencrypted e-mail across the Internet, the author believes that merely communicating through unencrypted e-mail should not waive the attorney-client or work-product privileges. Several states, including New York, have adopted legislation to this effect for purposes of the rules of evidence,[37] but the legislation provides both comfort and a warning. The fact that such legislation exists indicates that at least some legislatures believe that inadvertent waiver should not be inferred from use of unencrypted e-mail. On the other hand, the fact that such legislation was deemed needed, or at least advisable, indicates that in the absence of such legislation, there is a risk, or at least a perceived risk, that the attorney-client or work-product privilege might be lost simply by using e-mail to communicate information otherwise protected by these privileges.

A court might also choose to analyze a particular fact situation by analogizing e-mail to a telephone conversation. If, however, the court focuses on the technical differences between telephone calls and e-mail sent across the Internet, it might conclude there is no reasonable expectation of privacy when sending unencrypted e-mail across the Internet. Although some state ethics committees (following the Illinois' Ethics Committee) have found that these technical differences do not pose any significant threat to privacy, a careful analysis of that reasoning might ultimately lead a court to reject it.

The analysis might develop as follows: Illinois, and the states that follow its reasoning, rely heavily on the fact that "[i]nterception or monitoring of e-mail for purposes other than assuring quality of service or maintenance is illegal under the Electronic Communications Privacy Act . . . ."[38] But interception of an electronic communication, as defined by the Electronic Communications Privacy Act ("ECPA") relates only to messages moving across the Internet.[39] Once messages are "delivered" (and delivery may be to servers en route as well as to the final addressee), they are "stored" on a server, and reading them while they are stored on a server does not constitute interception.[40] In addition, the ECPA arguably regulates only "provider[s] of wire or

37. *See supra* note 2 and accompanying text.

38. S.C. Ethics Op. 97-08, *supra* note 30; *see also* Ill. Ethics Op. 96-10, *supra* note 4; 18 U.S.C. § 2511(2)(a)(i) (1994). Vermont and North Dakota have also concluded that the use of unencrypted e-mail does not violate obligations to treat communications with clients as confidential. *See* N.D. Ethics Op. 97-09, *supra* note 30; Vermont Ethics Op. 97-5, *supra* note 30.

39. *See* 18 U.S.C. §§ 2510 & 2511(1)(a) (1994).

40. *See* Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994). The decision has its critics. *See, e.g.*, David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, GEO. J. LEGAL ETHICS 459, 474-76 (1998). The analysis is based in part on the belief that messages broken into packets are reassembled only at their final destination. In fact, they are reassembled at each server en route to their destination. *See* Jonathan B. Postel, *Simple Mail Transfer Protocol*, RFC 821 (Aug. 1982) (vis-

electronic communication service[s], whose facilities are used in the transmission of a wire or electronic communication,"[41] and there is a risk that the reference will be construed to refer only to commercial providers.

If the reference is so construed and limited, messages passed through the systems of organizations which are at best only incidentally "providers" of electronic communications services (for example, universities and large corporations) may not be protected by any of the obligations imposed by the ECPA, including any obligations of confidentiality. (Since the ECPA also provides certain protections to those it covers, imposing confidentiality obligations on system administrators of non-commercial third party systems might also entail extending the protections of the ECPA to these entities, which a court might be reluctant to do in the absence of clear legislative direction on the issue.) Even if confidentiality obligations are imposed on private parties, if a court were to view unencrypted e-mail moving across the Internet as more like a postcard than a letter in a sealed a envelope, a confidentiality obligation similar to that imposed upon United States Postal employees might not be sufficient to eliminate the risk of loss of confidentiality for purposes of the attorney-client and work-product privileges.

In any event, the risk of actual disclosure remains. As indicated above, computer systems of all sizes, from a single desktop computer to large mainframes, have at least one system administrator whose job is to assure that the system operates smoothly. A system administrator for an organization's e-mail system does not, in the normal course, have a "need to know" attorney-client privileged information, but may, in connection with managing the company's computer system, have a need to access all the information on the system, including unencrypted e-mail. As indicated above, review by an organization's system administrator appears to be similar to review by a secretary of documents typed for a lawyer, and should not waive the attorney-client privilege. Where, however, the review may in fact be made by an unaffiliated third party system administrator, and particularly where it is in fact so made, there is a risk that a court would conclude that the information had not been treated with sufficient care to provide a reasonable expectation of privacy.[42]

---

ited Aug. 30, 1999) <http://www.cis.ohio-state.edu/htbin/rfc/rfc821.html> [hereinafter RFC 821].

41. 18 U.S.C. § 2511(2)(a)(i) (1994).

42. Note that when individuals receive e-mail, the sender's name appears on a list and the addressee then clicks on the name to "open" the message. The separation of sender's name and message occurs at the addressee's terminal. The system administrator sees addressee and message in a continuous scroll. *See* RFC 821, *supra* note 40.

While Illinois recognized that a (third party) system administrator could lawfully read part or all of a confidential message, it concluded that the opportunity for illegal interception by such system administrators did not make it unreasonable to expect privacy of the message.[43] The reference to "illegal interception" is troubling because the Illinois opinion recognized that a system administrator has a legitimate right to monitor messages, and because both the ECPA and case law recognize that accessing stored messages is not an interception.

A recent attempt to include accessing stored e-mail messages within the definition of "interception" by likening such messages to store voice-mail was rejected by the Ninth Circuit in *United States v. Smith*.[44] The *Smith* Court determined that voice mail was governed by the Stored Communications Act, making it illegal to access a message while it is stored, whereas e-mail is governed by the Wiretap Act (ECPA), making access illegal when contemporaneous with transmission, but leaving access while the communication is stored on a server unregulated by the ECPA prohibitions on interception. In other words, the Ninth Circuit determined that reading stored e-mail messages was not, under the applicable law (the ECPA), "interception."[45]

If other courts follow the Ninth Circuit, they may conclude that the Illinois analysis is technically faulty and unpersuasive, and, therefore, that the conclusion that the use of unencrypted e-mail across the Internet will not compromise confidentiality or risk forfeiture of the right to assert the attorney-client privilege is unwarranted because of the absence of a reasonable expectation of privacy.

To summarize, because the technology makes it possible for third party system administrators to view e-mail legitimately, the telephone analogy may be unreliable. Unlike telephone conversations, which are ephemeral, e-mail messages create a document. Although

43. *See* Ill. Ethics Op. 96-10, *supra* note 4.

44. 155 F.3d 1051, 1056 (9th Cir. 1998).

45. *See Smith*, 155 F.3d at 1056. In *Smith*, the government argued that the retrieval of stored voice mail was like the retrieval of stored electronic communications, and, therefore, was governed by the Stored Communications Act, *see* 18 U.S.C. §§ 2701-2711 (1994), and not the Wiretap Act (formerly 47 U.S.C. § 605, updated by the ECPA in 1986, but the court used the old name interchangeably). The Ninth Circuit, in rejecting the government's analogy, made a distinction between wire communications (phones and voice mail), for which the ECPA specifically includes the storage of such information in the definition of "interception," *see* 18 U.S.C. § 2510(1) (1994), and electronic communications (transmission of electronic signals), which does not include storage in the ECPA definition of "interception." *See* 18 U.S.C. § 2510(12) (1994). The court found that the ECPA exclusion of storage in the definition of "interception" means that for electronic communications, interception must be contemporaneous with transmission and therefore accessing stored e-mail was not "interception." *See Smith*, 155 F.3d at 1057.

e-mail messages travel over telephone lines, the technology causes them to move through a series of computer system e-mail servers, some of which may belong to entities which are not regulated interstate communications service providers, and thus the risk of disclosure is not limited to "tapping" into a particular conversation in progress.[46] Accessing messages delivered to intermediate systems en route is not "interception" and is not "illegal." Moreover, the ability of a third party system administrator to access messages on a mail server is routine and therefore foreseeable. In addition, not all mail servers are regulated Internet service providers, and whether entities other than Internet service providers have confidentiality obligations is uncertain. Even if entities other than Internet service providers have confidentiality obligations, it is not clear that they are different from those of United States postal employees, and information on a postcard placed in the United States Mail may not be regarded as having been treated as confidential information for purposes of, for example, discovery demands.

A recent resolution by the ABA House of Delegates calling upon courts to afford e-mail communications the same reasonable expectation of privacy as a telephone call[47] may or may not overcome the influence of a 1986 suggestion of the ABA Standing Committee on Lawyers' Responsibility for Client Protection that lawyers should not discuss confidential matters via e-mail unless they are assured "either through bar approval or through the lawyer's own informed evaluation" that a system operator will maintain confidentiality.[48] Because

46. In this sense, e-mail seems like voice mail, which can be accessed and "read" at a later time. As indicated above, courts may treat e-mail and voice mail differently. To the extent voice mail tapes are retained, not erased immediately after being retrieved, they may also create a "document" which is preserved and retrievable at a later time. Thus, establishment and maintenance of corporate policies regarding the retention and destruction of voice mail tapes is also advisable.

47. *See Conference Report,* [14 Current Reports] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 392, 394 (Aug. 19, 1998); *see also* ABA Formal Op. 99-413 (Mar. 10, 1999) *in* [Manual] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 1101:181.

48. *See* STANDING COMM. ON LAWYERS' RESPONSIBILITY FOR CLIENT PROTECTION, ABA, LAWYERS ON LINE: ETHICAL PERSPECTIVES IN THE USE OF TELECOMPUTER COMMUNICATION 67 (1986), *noted in* [Manual] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 55:409; *see also* STANDING COMM. ON ETHICS AND PROF. RESPONSIBILITY, ABA, RECENT ETHICS OPINIONS, Formal Op. 95-398 (Oct. 27, 1995) [hereinafter RECENT OPINIONS 95-398]. The formal opinion noted that under Rule 5.3, an attorney who gives a third party computer maintenance company access to client files "must make reasonable efforts to ensure . . . that the service provider has in place, or will establish, reasonable procedures to protect the confidentiality of [client] information . . . ." RECENT OPINIONS 95-398, *supra,* at 2. Reasonable efforts were seen to include attorney oversight to make sure the provider understands the obligations of maintaining confidentiality, and the Committee further recommended that the attorney obtain written assurance of confidentiality from the service provider. *See id.*; *see also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.4(b) (dealing with an attorney's obligation to advise a client on all matters nec-

there is no way for a lawyer to evaluate whether the system administrators of third party systems through which a message may pass will maintain confidentiality, the Standing Committee's suggestion may also be seen as supporting a court's finding that in particular circumstances, there was no reasonable expectation of privacy in connection with an e-mail message.

Risk #2: A court will apply the U.S. Mail analogy, regard unencrypted e-mail sent across the Internet as analogous to sending information on a postcard, and conclude that information sent unencrypted across the Internet is not being handled as if it were confidential.

The South Carolina ethics opinion recognized that "the same potential exists for the illegal interception of regular mail, the interception of a facsimile, and the unauthorized wiretapping of a land-based telephone" and concluded, "[b]ecause the expectation is no less reasonable than the expectation of privacy associated with regular mail, facsimile transmissions, or land-based telephone calls . . . use of e-mail is proper under Rule 1.6."[49] South Carolina did not discuss the efficacy of the use of confidentiality language on a facsimile cover sheet or the distinction between mailing information on a postcard and placing the message in an envelope, but did warn, "a finding of confidentiality and privilege . . . should not end the analysis. . . . [For] information that a prudent attorney would be hesitant to discuss by facsimile, telephone, or regular [(presumably in a sealed envelope)] mail . . . [a] lawyer should discuss with a client such options as encryption in order to safeguard against even inadvertent disclosure . . . when using e-mail."[50]

As indicated above, asserting the attorney-client and work-product privileges requires handling the materials sought to be protected as confidential. There is a considerable body of literature, both technical and in the popular press, describing e-mail as "like a postcard."[51] There is, therefore, a risk that a court will accept the postcard analogy, and conclude that sending unencrypted e-mail across the Internet indicates that the information so sent is not being treated as confidential. If that is a court's position, it is a short step to the conclusion that

---

essary to make an informed decision about the representation). The ABA Committee noted that if a breach of confidentiality occurs within the service provider's company, and the breach could be seen as a "significant factor" with regard to the representation, disclosure of the breach to the client might be required under Rule 1.4(b). RECENT OPINIONS 95-398, *supra*, at 3. The opinion's reasoning also extends to other third party service providers, e.g., data processing and printing providers. *See id.* at 2.

49. S.C. Ethics Op. 97-08, *supra* note 30; *see also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1998) (duty of confidentiality).

50. S.C. Ethics Op. 97-08, *supra* note 30; *accord* N.D. Ethics Op. 97-09, *supra* note 30; Vermont Ethics Op. 97-5, *supra* note 30.

51. *See* discussion in Freivogel, *supra* note 7, at 18.

sending unencrypted e-mail across the Internet waives the attorney-client and work-product privileges because assertion of these privileges requires handling the information as confidential.[52]

Risk #3: A court will apply the cellular telephone analogy, and conclude that when e-mail is sent across the Internet, it will be regarded as having a reasonable expectation of privacy only if it is encrypted.

There are a number of cases involving communications by cellular or cordless telephone. This mode of communication has been deemed similar to e-mail because of the transmission of communications into an "environment" in which messages can be intercepted relatively easily, and may even be inadvertently overheard.[53] In general, the older cases involving cellular telephones (which use a broadcast technology, which is different from the technology employed on the Internet) held that there was no reasonable expectation of privacy in such communications because of the likelihood of interception. More recently, however, cellular telephone technology has improved. Encryption is automatic in certain equipment, and there is at least one case suggesting that with improved technology (by implication, scrambling, a kind of encryption), there may be a reasonable expectation of privacy.[54]

The propriety of using cellular telephones to communicate confidential information with clients has been the subject of several state ethics committee opinions. New Hampshire sees technology as key in analyzing whether there is a reasonable expectation of privacy with regard to the use of cellular telephones and other forms of mobile communications.[55] The annotation to its Ethics Committee Opinion on the subject states: "A lawyer may not discuss client confidences or other information regarding representation with the client or a third

52. Such a position might have implications beyond waiver of the attorney-client and work-product privileges. For example, the conclusion that sending unencrypted e-mail across the Internet fails to treat it as confidential might have implications for handling information an organization wishes to protect as a trade secret.

53. To the extent statutes have made interception of cellular telephone communication illegal, it may be argued that these cases are less useful as precedents than when such statutes do not exist, on the theory that such statutes are comparable to the ECPA.

54. *See, e.g.,* Tyler v. Berodt, 877 F.2d 705, 706 (8th Cir. 1989); *see also* People v. Fata, 559 N.Y.S.2d 348 (N.Y. App. Div. 1990); State v. Delaurier, 488 A.2d 688 (R.I. 1985); State v. Smith, 438 N.W.2d 571 (Wis. 1989). *But cf.* United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992); State v. McVeigh, 620 A.2d 133 (Conn. 1993) (suppressing cordless telephone conversation). None of these discussions deals with the possible impact of the location of the speakers (e.g., taxi, commuter train, street or baseball game) when using their cellular telephones.

55. *See* New Hampshire Bar Ass'n, Ethics Comm., Formal Op. 1991-92/6 (April 16, 1992) (*Confidentiality of Mobile Communications*) [hereinafter N.H. Ethics Op.]; *accord* North Carolina State Bar Ass'n, Op. RPC 215 (1995) (*Modern Communications Technology and the Duty of Confidentiality*).

party on a cellular or other mobile telephone without the client's informed consent, unless a scrambler-descrambler or similar device is used."[56]

Arizona took an approach to cellular telephone communication that is consistent with its approach to e-mail confidentiality, concluding:

> [T]he time has not yet come when a lawyer's mere use of a cellular phone to communicate with the client - without resort to a scrambling device or exculpatory language at the call's beginning – constitutes an ethical breach.
>
> . . . Nevertheless, there is a genuine risk that a third party may intercept harmful information. Consequently, the lawyer should exercise caution when discussing client matters with opposing counsel on any portable telephone.[57]

By contrast, in Illinois, the state bar association opined, "[m]obile communications are not secure as to maintaining confidentiality of conversations and participants in those conversations have no right to expect to maintain privacy of their conversation."[58] As noted above, however, Illinois did not follow this reasoning in analyzing e-mail communication.

Risk #4: A court will look to an organization's internal e-mail policies regarding e-mail, and make determinations regarding reasonable expectations of privacy, as well as meeting the standards set forth in *Upjohn*,[59] based on the organization's written policies and internal practices and procedures.

E-mail moving within an organization generally moves from the sender to a central server to the addressee. Messages on the central server will be accessible to the organization's system administrator, but this accessibility should not affect the availability of either the attorney-client or work-product privileges. The system administrator is acting as an agent of the sender or receiver, and if examination of e-mail is required in order to manage the system, such an administrator probably has a "need to know" that would fall within the protection of *Upjohn*.[60] Problems may, however, arise in an organization in which e-mail is "automatically" sent to an entire department or other designated group of people, some of whom do not have a "need to know" and, therefore, do not fall within the protection of *Upjohn*. Theoretically, the risk is no different from the risk of sending out paper

56. N.H. Ethics Op. *in* [1991-95 Ethics Opinions] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 1001:5703 (annotation).

57. Arizona State Bar Ass'n, Comm. on the Rules of Professional Conduct, Op. 95-11 (1995).

58. Illinois State Bar Ass'n, Comm. on Professional Responsibility, Op. 90-7 (1990) (citing ILLINOIS RULE OF PROFESSIONAL CONDUCT 1.6(a)); *see also* Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989); Edwards v. Bardwell, 632 F. Supp. 584 (M.D. La. 1986), *aff'd*, 808 F.2d 54 (5th Cir. 1986).

59. *See* Upjohn Co. v. United States, 449 U.S. 383, 391-95 (1984).

60. *See id.*

("hard") copies to people who have no need to know, but the mechanics of electronic communication make broad distribution easier, and thus increase the likelihood of inappropriately broad distribution.

Additional risks arise in connection with retention and destruction of copies of electronic communications. In most organizations, backups are made automatically, at least weekly, and often daily. If the backup copies are available to all, without regard to or any effort to protect their confidentiality, it may be difficult to argue persuasively that the information is treated as confidential information.

Technology has made new types of review possible and these can create additional challenges. For example, many companies routinely scan their e-mail files for inappropriate or improper messages. These scans can range from a brokerage firm's scanning to assure that its brokers are not promoting stocks improperly (by searching for key phrases such as "guaranteed return") to corporations concerned about employee relations scanning for "steamy" messages. The scanning process itself is automatic. A simple scan "kicks out" messages which include the triggering key words or phrases, and then those messages are reviewed by human beings. To the extent that communications between attorney and client are reviewed by persons who do not have a need to know, the attorney-client and related work-product privileges may be at risk. Where messages to or from lawyers are reviewed by non-lawyers, an argument that the confidential nature of the communications is not being maintained might be successful. These risks may be considerably reduced by instituting appropriate internal procedures and internal structures: for example, by making the reviewer an agent of the organization's lawyer. In the absence of attention to possible pitfalls, however, the combination of scanning e-mail and review by a person who was neither an attorney nor an agent of an attorney, might result in inadvertent waiver of the attorney-client privilege.[61]

Arrangements that permit people to work from home or while they travel by giving off-site persons the ability to access an organization's intranet computer system from outside that system create additional challenges to maintaining confidentiality. System security is only as good as its weakest link. Security of internal systems can be enhanced in a variety of ways. For example, many internal systems "automatically" encrypt e-mail messages and include password protection mechanisms for each user. Such systems may provide high barriers to

61. In a corporate organization, the ethical issues of disclosure of confidential materials may be less urgent, but practical business issues, such as improper disclosure of inside information relating to or having an impact on the price of the company's securities, or inadvertent disclosure of trade secrets, may create business-related problems beyond those relating to attorney-client privilege or lawyer ethics.

casual access and the monitoring of messages, without authorized users being aware of the barriers.

Finally, an organization's stated treatment of e-mail communications may influence a court's determination of whether such communications are confidential, as well as how confidential they in fact are for purposes of keeping information limited to persons to have a need to know. For example, many corporations advise their employees that e-mail is not confidential, that it is to be used only for corporate business, and that it will be monitored. If such corporate policies are included in a manual or other written notices instructing employees that e-mail should not be used to communicate confidential information, it may be difficult for the corporation's lawyers to argue that use of such systems carries a reasonable expectation of privacy and, therefore, that it is acceptable to use such systems to communicate attorney-client privileged information. At least, the argument is weak in the absence of encryption, password, or other types of protection, or special internal rules regarding which communications are monitored and who handles such monitoring.

Risk #5: A court or ethics committee will determine that sending unencrypted e-mail across the Internet does not meet the ethical standards required of a lawyer to protect client confidences, and find malpractice based on such communication.

It is possible that a court or ethics committee would determine that sending unencrypted e-mail across the Internet does not meet the ethical standards required of a lawyer to protect client confidences, and find malpractice based on such communication, although such a conclusion seems unlikely and unwarranted. Still, given the availability of encryption software and the relative ease with which it can be used to protect e-mail communication, it is not inconceivable that a court would find, under egregious factual circumstances, that the failure to use encryption was deserving of ethical sanctions.

Risk #6: A client will determine that the lawyer's failure to consider the risks of using e-mail, explain them to the client, and obtain the client's consent to using that means of communication is a basis for terminating the attorney-client relationship.

Outside of states which require, under their ethical rules, that a lawyer obtain a client's consent to use of e-mail,[62] there is no ethical

62. *See, e.g.*, Iowa Ethics Op. 96-01, *supra* note 3; Iowa Ethics Op. 97-01, *supra* note 3. Missouri also takes the position that lawyers have an obligation to obtain clients' permission before using e-mail for confidential communications, after the attorney is satisfied that the client is aware of the risks of interception of the message as it travels through the Internet as well as through any network to which the computer may be connected. *See* Missouri Chief Disciplinary Counsel, Informal Op. 970230 (undated) *in* [Manual] LAWS. MAN. ON PROF. CONDUCT

obligation to discuss the issue, much less obtain client's consent to use of e-mail. Moreover, a client's agreement to a lawyer's unethical behavior does not make such behavior acceptable.

Nevertheless, when inadvertent disclosure of the content of an electronic communication creates serious problems for the client, if the lawyer has not discussed the risks of using unencrypted e-mail for confidential communications, the client is likely to blame the lawyer, thus impairing or ending an attorney-client relationship. Therefore, even when neither a legal nor an ethical duty is breached by the use of e-mail, if confidential information is prematurely disclosed, or inadvertently disclosed to a hostile party, the client may be lost.

IX. RECOMMENDATIONS: REDUCING THE RISKS

Recommendation #1: Take the time to understand and evaluate your organization's e-mail system, advise system administrators of their confidentiality obligations, and establish and implement appropriate internal procedures to protect and evidence confidential handling of confidential information and material.

Because "e-mail" encompasses a variety of communications systems, in a variety of settings, each with opportunities for a variety of configurations, what constitutes a reasonable expectation of privacy in any given situation depends upon the characteristics of the particular system involved, where it is, and how it is configured and used. All systems have system administrators, and those system administrators who are part of an organization's internal system can and should be advised of their obligations of confidentiality.[63] To the extent that they are required or requested to report certain types of information which comes into their possession through the e-mail systems they ad-

(ABA/BNA) 1101:5244 (annotation). Again, note that if the Ninth Circuit reasoning is followed, "interception" is separate from review by a third party system administrator. The author believes it is appropriate to emphasize that lawful review by third party system administrators is not interception, is not illegal, and may occur when messages are sent across the Internet.

63. Neither Arizona, Iowa, Illinois nor South Carolina opinions discuss whether actual or potential access to confidential information by system administrators would forfeit the attorney-client privilege because confidential information could be or had been disclosed to system administrators who constituted persons other than those with a "need to know." It seems clear that internal system administrators are like secretaries, i.e., agents with a need to know. It is more difficult to apply that rationale to third party system administrators, particularly if they are not administrators of commercial systems. They may have a need to look, but they do not, for the most part, need to know the contents of messages they review, and they may or may not have knowledge of the confidential nature of the contents of e-mail messages they review. As indicated above, encryption includes only text, not address, and indicates the length, but not the content, of a message. Thus, if the mere fact that two parties are communicating is confidential, encryption will not disguise that fact.

minister, if the information is from or directed to a lawyer, protection of the attorney-client and work-product privileges can be supported by having the information reported to an attorney. This evidences that the reporting person is acting as the attorney's agent, and not the agent of a non-attorney whose review might jeopardize the attorney-client privilege.

Group distribution arrangements should be instituted with care and reviewed regularly to assure that confidential communications are sent to an appropriately limited group. The risk of including inappropriate copy recipients of e-mail communications is, theoretically, no different from that for paper-based communications, but because of the ease of sending electronic communications and the often automatic setting for dissemination, special care must be taken to assure that electronic communications of materials sought to be protected based on their confidential nature (attorney-client and work-product privileges, and also information such as trade secret materials) are disseminated in accordance with the desired treatment. Thus, extra steps may be required in connection with electronic communications to assure that limited access and evidence of obligations of confidentiality are imposed on corporate personnel. These extra steps can provide clear and convincing evidence of an intention to protect confidentiality, thereby enabling the assertion of the attorney-client and work-product privileges, as well as meeting in-house attorneys' ethical obligations of confidentiality.

As stated above, a system's security is only as good as its weakest link. Accordingly, precautions not required within a system may be appropriate when communicating from outside. Establishing and implementing appropriate security measures to assure that access to the system is limited to authorized persons provides evidence of concern with confidentiality and indicates that reasonable steps have been taken to maintain it.

Procedures and policies should be written, disseminated, and implemented. These procedures and policies should be drafted with a view to how they will be used by the organization to support its position that it handles confidential information as such, and reviewed with a view of how it might be used by an opponent to establish the contrary. The policies should not only be written, but implemented, and should include policies relating to handling of backup copies to assure that if they contain confidential information, they, as well as the primary copies, are handled appropriately.

When an outside law firm and a client communicate frequently and communication includes long documents which are privileged and confidential, it may be advisable to establish a direct, modem to modem, line of communication with the client. In any event, it is advisable for the lawyer to investigate the client's e-mail policies and systems, and

consider treating e-mail communications with that client as the client itself treats them. If that alternative does not produce a satisfactory result, other arrangements, which will permit both parties to enjoy the convenience of electronic communications without sacrificing confidentiality, should be explored. These alternatives include, in addition to establishing a direct modem-to-modem connection, setting up a "secure socket" connection,[64] or using the same service provider and establishing a "private area" within that service to avoid the alternative of having communications move across the Internet and using encryption.

Recommendation #2: Recognize that when sending unencrypted e-mail, there is a risk of disclosure to system administrators, evaluate that risk, and take additional steps to guard confidentiality when that risk is deemed unacceptable.

Because of the manner in which e-mail is sent and received, there is an unavoidable risk of actual disclosure to system administrators. Whether or not these system administrators have confidentiality obligations, the risk of actual disclosure exists. Thus, where information is sufficiently sensitive to make actual disclosure unacceptable even if the persons to whom it may be disclosed have legal or moral obligations to maintain its confidentiality, additional steps are advisable to assure confidentiality. Such steps may include encryption, or modified e-mail arrangements, such as a modem to modem or secure socket connection.[65]

Recommendation #3: Check local statues, rules of court relating to evidence and ethics, and local ethics committee opinions regarding use of e-mail to communicate confidential information, and establish and institute practices and procedures in light of those rules and opinions.

Lawyers practicing in states in which local laws, decisions or ethics opinions impose requirements (for example, a requirement to discuss the use of electronic communication with clients and to obtain consent to its use)[66] will want to be aware of and comply with such requirements. Lawyers practicing in states in which local law, decisions and

64. A "secure socket" connection is a special type of Internet connection that automatically encrypts data en route between the two pre-established end points. Considerable technical expertise is required to make such a connection available, but once it is available, it is relatively easy to use.

65. This problem cannot be solved by having a dedicated password protected area within a single commercial system, as the system administrator of that system will still have the ability, and possibly the need, to review messages. There is, however, case law to the effect that for Fourth Amendment (search and seizure) purposes, persons sending messages within a single system have a reasonable expectation of privacy. *See* United States v. Maxwell, 42 M.J. 568 (U.S.A.F. Crim. App. 1995), *rev'd in part on other grounds*, 45 M.J. 406 (C.A.A.F. 1996).

66. *See supra* note 62.

ethics opinions do not speak to the issues of whether and when the use of electronic exchanges of information are appropriate will want to examine the issues and risks, and make an educated evaluation as to whether or not the use of e-mail in particular circumstances is, first, ethical, and even if it is, whether, in the particular circumstances, it is wise. Lawyers practicing in states in which local law, decisions or ethics opinions have taken the position that use of e-mail is ethical[67] will want to be aware that both the law and relevant technology are in the process of development and, therefore, also evaluate whether, in the particular circumstances, use of unencrypted e-mail across the Internet is wise.

Recommendation #4: Discuss use of e-mail with each client with whom e-mail is expected to be used for attorney-client communications, or sending work-product or other confidential communications.

The risks of having an unhappy client as a result of using e-mail can be reduced by conferring with that client regarding the specific risks of e-mail communication in light of the specific technology being used, and with due attention to related facts such as the client's internal system and characterization of its system (if any). Such discussion of the advantages and disadvantages of a particular mode of communication may also decrease the risk of being sued by that client for malpractice if the mode of mutually approved communication turns out to be less confidential than anticipated. Note, however, that although the risks of facing a malpractice suit and having an unhappy client can be reduced by discussing the relative risks and rewards of using e-mail communication, unless local rules provide otherwise, the ultimate responsibility for evaluating, for purposes of the rules of ethics, what modes of communication are ethical, remains with the lawyer.

X. CONCLUSION

The author believes that use of unencrypted e-mail between attorney and client should not, in and of itself, result in a waiver of the attorney-client privilege for purposes of the rules of evidence. She recognizes, however, there is a risk that in the absence of legislative guidance,[68] a court might decide under certain circumstances that communication via unencrypted e-mail constitutes a waiver of the attorney-client privilege for failure to treat information as confidential. In the absence of specific rules, counsel is well advised to consider the

67. *See, e.g.*, supra note 3; D.C. Bar Op. 281 (1998); Kentucky Bar Ass'n, Ethics Comm., Op. E-403 (1998) *in* [Manual] LAWS. MAN. ON PROF. CONDUCT (ABA/BNA) 1101:3903 (annotation).

68. *See supra* note 2.

possible risks, weigh them against the benefits, and proceed on the basis of that evaluation.

The conflicting views regarding e-mail confidentiality impact not only evidentiary issues, but also, the broader ethical issues as to whether communicating by e-mail may be deemed to constitute a breach of an attorney's obligation to protect client confidences. Whereas failure to guard confidential information adequately is punishable, in the context of litigation, by making the information available for discovery, failure to guard client confidences in breach of the lawyer's ethical obligations may result in that lawyer being sued for malpractice, and in egregious cases, having the lawyer's license to practice law suspended or revoked. Even the less drastic (and perhaps more likely) response of an unhappy client taking its business elsewhere when it believes its confidential information has been treated inappropriately can have devastating adverse effects on the lawyer's reputation and financial condition.

There is no doubt that e-mail provides a rapid, efficient, inexpensive, and, therefore, a highly desirable mode of communication. Possibly, the advantages of unencrypted e-mail communication, in all its forms, so far outweigh the risks of inadvertent disclosure that except in states whose ethics rules or opinions provide otherwise, a general conclusion that use of unencrypted e-mail is ethical is warranted. On the other hand, state ethics opinions differ, the rationales of some of these opinions may be based on erroneous or changing interpretations of the law, technology is fluid and evolving in ways which may impact reasonable expectations of confidentiality, and e-mail policies of the parties involved may have an impact on what expectations are reasonable in particular circumstances. Thus, lawyers are well-advised to consider the use of e-mail carefully, including the additional security and evidentiary value of encryption and modem-to-modem or secure socket communication, and to balance the inconvenience of making special arrangements with the advantages of the additional comfort they may provide.

Whatever the decision at a given point in time, so long as both law and technology remain subject to constant and rapid change, it will be appropriate to revisit the decision periodically to assure that past evaluations have not become outdated because their underlying rationales have become inaccurate, or no longer apply because the law or technology have changed. In short, so long as use of e-mail for confidential communication remains an issue on which reasonable people differ, regular review of practices and procedures to assure they remain in conformity with current legal, ethical and technical realities is appropriate.