THE HIGH-TECH LEGAL PRACTICE: ATTORNEY-CLIENT COMMUNICATIONS AND THE INTERNET

LUCY SCHLAUCH LEONARD

INTRODUCTION

In today's business world, the use of new communication technologies is increasingly important in everyday life. Even attorneys, who are frequently thought of as "technophobes,"[1] are expanding their use of faxes, cordless telephones, cellular telephones, e-mail, voice mail, intranets, and the Internet in the conduct of their business.[2] Although some attorneys still refuse to use the new technologies in their practice,[3] the number of attorneys who use cellular phones and "surf the net" increases daily.[4]

The exact number of people on the Internet is unknown,[5] but most experts agree that it exceeds forty million.[6] They also estimate that the number of people who access the Internet increases by one million each month, and that about one-half of the people on the Internet use it in connection with their work.[7]

---

1. *See* Ian Olgeirson, *Internet Schminternet! Cyberskeptics Speak Out,* DENV. BUS. J., Oct. 4, 1996, at 25A, 29A, *available in* 1996 WL 10910565 (referring to the legal profession as "notoriously technophobic").

2. In this comment, all references to e-mail (unless otherwise specified) refer to external e-mail transmitted over the Internet. Many companies and law firms have internal e-mail systems which allow communication within the company. These communications do not travel across the Internet and do not present the same privacy problems that Internet communications present.

3. *See, e.g.*, Olgeirson, *supra* note 1, at 29A (quoting prominent Denver attorney Steve Farber as saying, "[computer technology] really has no value to what I do day to day").

4. *See id.*

5. *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996) (noting "[t]he nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment").

6. *See* ACLU v. Reno, 929 F. Supp. at 831 (citing the number of people with access to the Internet as approximately 40 million); Parry Aftab, *Monitoring Communications on the Internet,* N.Y. L.J., Sept. 30, 1996, at S2 (citing the number of people on the Internet in September of 1996 as between 15 and 30 million); Howard A. Zucherman et al., *Thinking of Going Public? An Overview,* 4 CAPITAL SOURCES FOR REAL ESTATE 4 (estimating that use of the Internet by the year 2000 will range from 150 to 200 million people).

7. *See* Aftab, *supra* note 6; *see also* ACLU v. Reno, 929 F. Supp at 831 (noting

In the legal field, the Internet is also taking a prominent role. Most attorneys who practice as corporate in-house counsel have access to the Internet, as do most law professors, federal judges, and many federal agencies.[8] Other sources estimate that between one-quarter and one-third of attorneys in private practice are using the Internet in their work.[9]

The ability to punch a button on a keyboard and send a document from Denver to Denmark within a few seconds not only saves time—it also saves money. The Electronic Messaging Association has determined that the total worldwide value of e-mail to business users is approximately $12.65 billion.[10] Whether an attorney is sending a document around the world or across the street, Internet technology makes the task more efficient. To illustrate this point, imagine an attorney who is working on a merger with a law firm across the country. Without the Internet, she faces document mailing delays using traditional mailing services known as "snail mail,"[11] or she faces the expense of faxing huge documents over long-distance telephone service. Although faxing is fast, it may require time for the data input of changes from various hard copies. Faxed documents may also come across unreadable. E-mail, on the other hand, can send documents in a matter of seconds without the expense or time associated with more traditional methods.

Indeed, as clients and the marketplace demand greater efficiency from attorneys, those attorneys who fail to use the technology available to them will find themselves less valuable to their clients. Attorneys who have "high tech" clients may also find that their clients insist on communication through e-mail. Though widely accepted in business, new technologies present

---

that the number of people on the Internet by the year 1999 is expected to be 200 million); Zucherman et al., *supra* note 6.

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

9. *See id.*

10. *See* Craig S. Ey, *E-Mail Continues to Revolutionize Communication*, BUS. J. - SAN JOSE, Sept. 9, 1996, *available in* 1996 WL 11868213. Furthermore, the use of e-mail continues to increase. According to one source, in 1992, only 2% of the U.S. population used electronic mail. By 1997, that figure had risen to 15%, and by the year 2000, the figure is expected to reach 50%. *See* William J. Cook, *Hypertext Bar Groups Need to Rethink Views of Privacy on the Internet*, CHI. LAW., Jan. 1998, at 63.

11. "Snail mail" is the common high-tech term for regular land-based postal service or express mail. *See* CYBER DICTIONARY 36 (abridged ed., 1996).

novel legal problems. By its nature, the law is often slow to respond to change.[12] Most legal questions presented by e-mail and the Internet have not been settled by the courts or legislatures. Because these new technologies are untested in the law, they represent a set of "wild cards" which present unknowable consequences.

Two legal issues should be of particular concern to practicing attorneys who are using the Internet or thinking of using it for communications. Whether communications made between attorneys and clients through e-mail are covered by the attorney-client privilege is uncertain and should concern any attorney who uses or is considering use of the Internet as a part of her practice. Similarly, whether an attorney violates the duty of client confidence by communicating sensitive material in an e-mail message is also unclear.

Since the law is unsettled, this comment suggests that the existing case law involving the postal service and land-line telephone communications provides the most useful framework for analyzing the privacy issues in attorney-client communications sent over the Internet. Those who argue in favor of applying the privilege to e-mail use an analogy to the postal service and land-line telephone communications to claim that there is a reasonable expectation of privacy in e-mail communications. These arguments are buttressed by the strong criminal sanctions against the interception of electronic communications. However, because these analogies are flawed, attorneys using the Internet should use encryption to ensure the privacy of their confidential Internet communications. In support of this conclusion, Part I of this comment analyzes the problems presented by e-mail communication and the relationship between this medium and the existing law of attorney-client privilege and the duty of client confidentiality. In Part II, analogies are drawn to the state of the law in other forms of communication including telephones, cordless and cellular telephones, fax machines, and postal mail.

---

12. There have been instances where the court system has been ahead of change, acting rather than reacting. For example, the courts were quick to respond to cases addressing segregation and abortion; however, this is the exception rather than the rule. Questions of privacy in cellular telephone technology have yet to be resolved by the courts and took years to be addressed by Congress. *See* discussion *infra* Part II.B.

I. PROBLEMS PRESENTED BY E-MAIL COMMUNICATIONS

A. E-Mail: A Primer

The Internet was developed in the late 1960s and early 1970s as part of a government project to create an indestructible defense system that would be able to function even if part of the system was destroyed by a nuclear attack.[13] The original government system, ARPANET,[14] was built on the premise that information could be "packetized" and sent over telephone lines using multiple paths.[15] The packets of information were designed to find their intended addresses and send messages back to the return address if problems arose and the message was unable to reach its destination.[16] Therefore, if any part of the network was destroyed by a nuclear attack, the message would still be able to find its way to its destination using other pathways.

Following the creation of ARPANET, the Internet grew as various organizations added on, and it was used mostly by academics and computer "techies."[17] As a result of the addition of these privately-owned computer networks, the Internet is not owned by any one party;[18] rather, it is a network of "perpetually

---

13. *See* Alison L. Sprout, *Waiting to Download*, FORTUNE, Aug. 5, 1996, at 64, *available in* 1996 WL 8827980.

14. *See* MARK VELJKOV & GEORGE HARTNELL, POCKET GUIDES TO THE INTERNET: VOLUME 4: THE INTERNET E-MAIL SYSTEM 1 (1994). In ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), the findings of fact included the following:

> The Internet had its origins in 1969 as an experimental project of the Advanced Research Project Agency ("ARPA"), and was called ARPANET. This network linked computers and computer networks owned by the military, defense contractors and university laboratories conducting defense-related research.... As it evolved far beyond its research origins in the United States to encompass universities, corporations and people around the world, the ARPANET came to be called "DARPA Internet," and finally just the "Internet."

Id. at 831.

15. *See* ACLU v. Reno, 929 F. Supp. at 832.

16. *See id.*

17. *See id.* at 831 ("In 1981, fewer than 300 computers were linked to the Internet....").

18. *See id.* at 832. The court found:

> [N]o single entity—academic, corporate, governmental, or non-profit—administers the Internet. It exists and functions as a result of the fact that hundreds of thousands of separate operators of computers and computer networks independently decided to use common data transfer protocols to exchange communications and information with other computers.... There is no centralized storage location, control point or communications channel for the Internet....

Id.

open connections between computers."[19] Because the Internet was created in this piecemeal fashion, and with the intent of using many pathways to transfer information, e-mail messages sent through the Internet use a variety of different nodes and servers to travel to their final destinations.[20] A wide-area backbone system which is owned, in part, by a private, non-profit corporation called Advanced Networks and Services ("ANS")[21] links these privately-owned computer networks. The Internet now uses telephone companies, service providers, universities, and other computer "nodes"[22] to transfer a message from origin to destination.[23]

Since the Internet uses "packetization" to send information, an e-mail message is generally not sent in one piece. Rather, a communication is separated into different packets, or envelopes. These packets of information include a portion of whatever is being sent (for instance, a program, message, or document) as well as the address to which it is being sent, a return address, and an identification code.[24] The address portion of the envelope contains all of the information required to locate the intended recipient. For example, the address "schlauch@ucsub.colorado.edu" contains information about the "local" recipient (schlauch) and information about the "host" system (ucsub at the University of Colorado).[25] The same information is coded for the return address. The identification code is designed to aid the receiving system put the document back together again.

The packets are sent over the Internet using a "store and forward" system. This means that the packets are sent from server to server, stored temporarily at each location, and then forwarded to another server along the path. Simultaneously, the network uses routers to determine which path will take the message to the intended destination. "A router looks at each

---

19. *See* Merrill, *supra* note 8, at 22.

20. *See* Sprout, *supra* note 13, at 66.

21. *See* HOWARD M. FRIEDMAN, SECURITIES REGULATION IN CYBERSPACE § 1-5 (1997).

22. "Nodes" are "points of connection into a network. . . . In packet switched networks, they are the packet switches which form the network's backbone." NEWTON'S TELECOM DICTIONARY 415 (11th ed. 1996).

23. *See* Sprout, *supra* note 13, at 66; *see also* Daniel F. Hunter, Note, *Electronic Mail and Michigan's Public Disclosure Laws: The Argument for Public Access to Governmental Electronic Mail*, 28 U. MICH. J.L. REFORM 977, 981-82 (1995).

24. *See* Hunter, *supra* note 22, at 980.

25. *See id.*

packet of information and passes it along to another router that helps it toward its destination, after determining the best path available at that moment. That means bypassing any routers that might be on the fritz or backed up."[26]

Once the e-mail message reaches the destination server, it is stored on that computer. At this point, the message will be saved for the recipient to read. Once the recipient reads the file, she may save it, forward it to someone else, or delete it. However,

> Many individuals mistakenly believe that deleting a file permanently erases that file. A computer does not erase files; the computer only marks a file as no longer needed, and makes the space immediately available for storing new files. The computer erases the information only when the computer over-writes the file with another file.[27]

Therefore, depending on the size of the computer memory on the receiving and sending systems, and depending on the company's computer backup practices, the message may be retained for months or indefinitely. "Deleted" material can be retrieved easily by an experienced user with a utility program widely available at software stores.[28] There are also companies that specialize in finding deleted computer files.[29] Thus, retrieval of these "deleted" computer files is easy so long as the computer has not overwritten the space on the computer's hard drive.[30]

E-mail communications are different from any other form of communication used by attorneys because they are saved in numerous locations and these saved messages are difficult to destroy. Letters or other items sent through "snail mail" are not copied at each post office through which they travel. The same is true of telephone conversations or faxes. Additionally, these

---

26. Sprout, *supra* note 13, at 67.

27. Patrick R. Grady, *Discovery of Computer Stored Documents and Computer Based Litigation Support Systems: Why Give Up More Than Necessary*, 14 J. MARSHALL J. COMPUTER & INFO. L. 523, 529 (1996).

28. *See* Heidi L. McNeil & Robert M. Kort, *Discovery of E-Mail*, OR. ST. B. BULL., Dec. 1995, at 21, 22.

29. One company specializing in this service is Data Technology Services, Inc. of Denver, Colorado. According to their spokesman, many computer programs come with a user's guide that will give directions for retrieving a deleted computer file. *See* Telephone Interview with Jay Mariley, Computer Specialist, Data Technology Services, Inc. (Dec. 29, 1997).

30. *See id.*

other forms of communication are much more easily destroyed. This important difference may well cause courts to treat e-mail communications differently.

B. The Ease of Intercepting E-Mail

Another reason why courts may treat electronic mail communications differently is the threat of interception.[31] The first potential problem with e-mail privacy arises in the author's computer, before the message is sent. The message, once written, is stored for an indefinite amount of time, and many networks can be cracked and accessed by computer "hackers," "crackers," and "phreakers."[32] The same problems exist at the receiving end of the transmission.

There are numerous ways to infiltrate a network.[33] One popular method is called "spoofing."[34] When a spoofer attacks a

---

31. *See* ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:409 (1998).

> [U]nencrypted e-mail messages are in text format and in theory may be read by individuals at these interim locations or by curious employees at the lawyer's own Internet service provider. In addition, hackers and professional snoopers can exploit "sniffer" software and powerful search engines to find messages of interest by targeting addresses, names, or particular words . . . .

Id.

32. *See generally* Marlyn Kemper Littman, *Protecting Electronic Data: A Losing Battle?, in* SAFEGUARDING ELECTRONIC INFORMATION 20 (Jana Varlejs ed., 1996). The term "hacker" originally referred to "[a] person who 'hacks' away at a computer until his program works." *Id.* However, because of misuse by the press and in the 1983 movie "War Games," hacker has since come to refer to someone who breaks into computer systems for fun and sport. NEWTON'S TELECOM DICTIONARY, *supra* note 20, at 284. A "cracker" is "[a] person who 'cracks' computer and telephone systems by gaining access to passwords, or by 'cracking' the copy protection of computer software. A cracker usually does illegal acts. A cracker is a 'hacker' whose hacks are beyond the bounds of propriety and usually beyond the law." *Id.* at 155. A "phreaker" is someone who uses technology to "attack the public telephone system and get free long distance service." *Id.* at 462. For a discussion of the differences between hackers, crackers, and phreakers, as well as a good discussion of the ethical duties of an attorney in regards to e-mail, see Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail* (visited Mar. 26, 1998) <http://www.computerbar.org/netethics/bjones.htm>.

33. Many web sites exist to provide information on cracking networks. *See The Underground Home Page* (visited Jan. 29, 1998) <http://underground.org>; *Phrack Magazine Home Page* (visited Jan. 29, 1998) <http://freeside.fc.net/phrack>; *SATAN Release Home Page* (last modified Apr. 24, 1995) <http://www.cs.ruu.nl/cert-uu/satan.html>.

34. *See* Littman, *supra* note 32, at 23.

network, the target computer is fooled into believing that it is receiving a friendly message.[35] Once inside the system, the spoofer is able to access the network.[36] It is very difficult to tell that a network has been attacked by a spoofer, so the network administrator may never know there has been an invasion or that the network is prone to such attacks.[37] Another frequently used infiltration technique is the use of a widely available tool called SATAN, or Security Administrator Tool for Analyzing Networks.[38] SATAN was designed to aid network administrators in identifying and fixing potential weaknesses that create vulnerable areas in their networks.[39] However, because the tool is publicly available on the Internet, it is used by crackers as well.[40] Therefore, unless the attorney's and the client's network are both uncrackable, a message may be vulnerable from the moment it is written.[41]

An e-mail message is also vulnerable while in transit on the Internet. Along its journey, the message is saved on any number of nodes and is accessible by network administrators.[42] Furthermore, crackers use programs called "sniffers" to intercept information as it travels through a network.[43] A sniffer program is designed to pick up all transmissions sent on a network or all transmissions with a specified recipient or sender.[44] Without even knowing your password, the sniffer can reassemble and read any non-encrypted e-mail message sent on the Internet.[45] Similarly, crackers use spoofer programs to emulate the intended recipient's computer and receive any mail intended for another

---

35. *See id.*

36. *See id.*

37. *See id.*

38. *See SATAN Release Home Page* (last modified Apr. 24, 1995) <http://www.cs.ruu.nl/cert-uu/satan.html>.

39. *See id.*

40. *See Overexposed?*, COMPUTER BUS. REV., Jan. 1, 1997. "60% of the hackers used specialist software to help them break into computer systems. Specifically, cracker programs such as Unix Password Cracker and Crack were the most common and frequently used together with SATAN and packet sniffers, [and] spoofing . . . ." *Id.*

41. *See generally* Littman, *supra* note 32.

42. *See* Electronic Communications Privacy Act of 1986 § 201(a), 18 U.S.C. § 2701 (1994).

43. *See* Aaron Grossman, *Is Opposing Counsel Reading Your E-Mail?*, MASS. LAW. WKLY., Nov. 18, 1996, at B4.

44. *See* Jones, *supra* note 32.

45. *See id.*

machine.[46] The spoofing machine sends a reply to the originating computer to indicate the message was received.[47] The spoofer is then able to retain the message, forward it to the intended recipient, forward it to others, or change the message.[48]

Interception of electronic communications is a federal felony under the Electronic Communications Privacy Act ("ECPA").[49] The ECPA was passed in 1986 as an amendment to the 1968 Federal Wiretapping Act[50] in an effort by Congress to close loopholes in the Act that had been created by advances in technology.[51] The ECPA provides criminal and civil penalties for the unauthorized access of stored electronic communications.[52] Similarly, the Federal Wiretapping Act provides civil and criminal penalties for contemporaneous interception of any wire or oral communication.[53] Together, the two acts provide civil and criminal penalties for the interception of e-mail.

Although the acts prohibit interception and unauthorized access of stored electronic communications, they do authorize third-party access to electronic communications in a number of circumstances. First, the ECPA allows a service provider or telephone service to access a communication if necessary to the operations of the server.[54] This includes access for system maintenance as well as monitoring to prevent illegal use of the system. Second, the ECPA authorizes access for law enforcement, administrative, and national security reasons.[55] And third, the Act allows the interception and use of electronic communications that are readily available to the public.[56]

In a 1995 symposium on the issue of privacy on the Internet, Joel Reidenberg, an Associate Professor of Law at Fordham

---

46. *See* Grossman, *supra* note 43.

47. *See id.*

48. *See id.*

49. 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.).

50. 18 U.S.C. §§ 2510-2521 (1994).

51. *See* Donald H. Seifman & Craig W. Trepanier, *Evolution of the Paperless Office: Legal Issues Arising out of Technology in the Workplace, Part I. E-Mail and Voicemail Systems,* EMPLOYEE REL. L.J., Winter 1995/96, at 5, 9.

52. *See* 18 U.S.C. § 2701 (1994) (criminal penalties include fines and up to two years in jail for repeat offenders); *id.* § 2707 (civil relief includes equitable and declaratory relief, damages, and attorney's fees).

53. *See* 18 U.S.C. § 2511 (1994) (criminal penalties); *id.* § 2520 (civil penalties).

54. *See* 18 U.S.C. §§ 2511, 2702 (1994).

55. *See id.* §§ 2511, 2516, 2701, 2702, 2703.

56. *See id.* § 2511(g).

University School of Law, discussed the ECPA provision allowing service providers access to communications: "[This provision] should terrify us as lawyers. The provision says that the system administration, for systems administration purposes, can essentially do anything. It is perfectly legitimate for a systems administrator to read all e-mail messages for those purposes."[57] Though Professor Reidenberg intended only to joke about the lack of control lawyers had over the Internet, the potential for third parties to be privy to confidential communications is clear.

Furthermore, the Internet is not a flawless system. As a direct result of its piecemeal development, the network is dependent on telephone lines designed to carry conversations lasting only a few minutes in length.[58] Internet transactions generally last much longer.[59] As a result, the telephone lines become jammed with information, and brownouts[60] frequently occur making it impossible to use the Internet in some locations.[61] Consequently, there are some places on the Internet where ten to twenty percent of all messages sent are lost, leading some commentators to suggest the Internet may soon become completely unusable.[62]

The instability of the medium itself combined with the ease of interception further distinguishes this method of communication from any other existing form of communication. As a result, prevailing legal analysis of communications between an attorney and her client are not easily applied to this new medium. Because our present understanding of the attorney-client privilege and the duty of client confidence is based on traditional

---

57. Symposium, *The Privacy Debate: To What Extent Should Traditionally "Private" Communications Remain Private on the Internet?*, 5 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 329, 382 (1995).

58. *See* Sprout, *supra* note 13, at 66.

59. *See id.* Though electronic mail messages take only a few seconds to send, other Internet users can spend hours "surfing the net." It is these users who are putting a great strain on the Internet.

60. A "brownout" is a partial elimination of or a reduction in service availability. The term was originally used to refer to a partial elimination of or a reduction in electric service to some degree less than a blackout and has now been applied to electronic communications. *See* RANDOM HOUSE COMPACT UNABRIDGED DICTIONARY 268 (1996).

61. *See id.*

62. *See* Sprout, *supra* note 13, at 65 (quoting Bob Metcalfe, inventor of Ethernet technology as saying "[t]he Internet has outgrown what it was designed to do. It has become a house of cards.").

forms of communication, these duties cannot be blindly applied to electronic communications.

C. *Attorney-Client Privilege and Client Confidence*

Though often confused, attorney-client privilege and client confidence are conceptually different.[63] Attorney-client privilege is an evidentiary rule, designed to protect a client from the government forcing her attorney to disclose confidential information.[64] Communications that qualify for this protection are called "privileged communications." Client confidence, on the other hand, is a duty derived from the agency relationship between an attorney and her client and is expressed in the American Bar Association's Model Rules of Professional Conduct and Model Code of Professional Responsibility.[65] Communications under these rules are "ethically protected." Together, these two doctrines define the rights and responsibilities of an attorney regarding confidential communications.

1. Attorney-Client Privilege

Although different courts have created various formulations of the attorney-client privilege, the general ideas embodied in the rule are universal to federal and state courts alike. The rule of attorney-client privilege is the oldest of all privileges[66] and is intended to protect the client "in order that he may be free to disclose to his attorney matters of confidence and importance without fear that the trust will be violated."[67] If the privilege

---

63. *See* Geoffrey C. Hazard, *Ethics*, NAT'L L.J., Jan. 25, 1993, at 17; *see also* ABA, LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:303 (1992) ("[I]t is clear that the ethical principle of confidentiality is not co-extensive with the attorney-client privilege.").

64. *See* Hazard, *supra* note 63; *see also* COLO. REV. STAT. § 13-90-107(1)(b) (1997); FED. R. EVID. 501.

65. *See* Hazard, *supra* note 63; *see also* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1983); MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1980).

66. *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) ("[T]he attorney-client privilege is the oldest of the privileges for confidential communications known to the common law.").

67. Wilcoxon v. United States, 231 F.2d 384, 386 (10th Cir. 1956), *cert. denied*, 76 S. Ct. 834 (1956); *see also Upjohn*, 449 U.S. at 389 (holding that the purpose of the privilege "is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and

applies to a communication, the lawyer cannot be compelled by a court to disclose the contents of that communication.[68] The basic formula used to determine whether something is covered by the attorney-client privilege is:

> (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.[69]

Applying this formula to a communication using e-mail, only two of the eight criteria seem to present potential problems for e-mail and attorney-client privilege: whether the communication is made in confidence and whether the privilege is waived by the use of e-mail.[70]

a. Communications Made in Confidence

For the attorney-client privilege to attach to a communication, the "communication must be made in confidence of the relationship and under circumstances from which it may reasonably be presumed that it will remain in confidence."[71] For example, if a conversation between an attorney and his client takes place in loud voices in a crowded restaurant, the conversa-

---

administration of justice").

68. *See, e.g., Upjohn*, 449 U.S. at 383.

69. *In re* Horowitz, 482 F.2d 72, 80-81 n.7 (2d Cir. 1973), *cert. denied*, 414 U.S. 867 (1973) (citing 8 JOHN HENRY WIGMORE ON EVIDENCE § 2292 (McNaughton rev. ed. 1961)).

70. The other elements of the attorney-client privilege test do not present new problems for e-mail communications because they are not affected by the medium used to communicate. Only the analysis of whether a communication is confidential and the analysis of a potential waiver are changed by the method of communication.

71. *Wilcoxon*, 231 F.2d at 386; *see also, e.g.*, United States. v. Schwimmer, 892 F.2d 237, 234 (2d Cir. 1989) (holding that the attorney-client privilege "requires a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given"); United States v. Melvin, 650 F.2d 641, 645 (5th Cir. 1981) ("[A] communication is protected by the attorney-client privilege . . . if it is intended to remain confidential . . . and understood to be confidential."); Ullmann v. State, 647 A.2d 324 (Conn. 1994) (holding that the privilege only protects those communications made in confidence for the purposes of receiving legal advice; information about the client, including name, address, and telephone number, is not information given in confidence).

tion is not taking place under circumstances from which there arises a reasonable presumption of confidence. There can be no reasonable expectation that no one will overhear, and therefore, there is no reasonable expectation that the communication will be private. Thus, the communication must take place in a manner that furthers the actual confidentiality of the communication—for instance, in an attorney's private office with the door closed. Furthermore, "[i]t is of the essence of the attorney-client privilege that it is limited to those communications which are intended to be confidential. 'The moment confidence ceases . . . privilege ceases.'"[72] Thus, if there are third parties present during the communication, the communication is not confidential unless those third parties are necessary to the communication.[73]

In addition, as set out in *In re Grand Jury Proceedings*,[74] the attorney-client privilege does not apply if the client knows the information will be made known to third parties. In that case, an attorney attempted to assert the attorney-client privilege to protect the substance of conversations between himself and his clients regarding a private placement of securities.[75] The court held that the communications could not be privileged on the grounds that the information disclosed was intended to be part of a prospectus for the securities.[76] Finding there was no intention to keep the information confidential because the intent was to

---

72. United States v. Tellier, 255 F.2d 441, 447 (2nd Cir. 1958) (citing Parkhurst v. Lowten, 2 Swanst. 194, 216 (1819)) (holding that communication between an attorney and a client is not confidential when the expectation was that the substance of the conversation would be transmitted by the attorney to a third party).

73. *See, e.g., Schwimmer*, 892 F.2d at 237 (holding the attorney-client privilege extends to communications with an accountant assisting an attorney in defense of the client where the attorney directed the client to speak freely with the accountant); United States v. Evans, 954 F. Supp. 165 (N.D. Ill. 1997) (holding there could be no privilege for communications between a client and attorney when an attorney friend of the client was also present); State v. Cascone, 487 A.2d 186, 189 n.3 (Conn. 1985) (holding that although the presence of third parties generally will eliminate any privilege from a conversation, "the presence of agents or employees of an attorney or a client, if necessary to the consultation, will not preclude a reasonable expectation of confidentiality"); State v. Colton, 384 A.2d 343 (Conn. 1977) (finding there could be no attorney-client privilege in a conversation between a witness and an investigator when a third party representing the defendant was also present); La Faive v. DiLoretto, 476 A.2d 626, 631-32 (Conn. App. 1984) (questioning of plaintiff regarding a conversation with her attorney during recess was "an invasion of the attorney client privilege," since the communication was confidential).

74. 727 F.2d 1352 (4th Cir. 1984).

75. *See id.*

76. *See id.* at 1358.

publish the information to potential investors, the court noted "the privilege does not apply to the situation where it is the intention or understanding of the client that the communication is to be made known to others."[77]

At least two jurisdictions have also gone so far as to hold that a client must take affirmative action to preserve confidentiality.[78] Similarly, another court has held that a client must take reasonable steps to maintain the confidentiality of privileged documents and that a client's failure to do so may be taken as evidence of lack of intent to preserve confidentiality.[79] In *In re Horowitz*,[80] the court was faced with the question "whether confidentiality is lost by placing written communications between lawyer and client in a place where they are available to others."[81] There, the purportedly privileged documents were indiscriminately intermingled with other unprivileged documents of the corporation.[82] The documents were treated in the same manner as all other documents and generally were available to the company's accountant.[83] Holding that the privilege could not apply to such a communication, the court commented that "[o]ne measure of their continuing confidentiality is the degree of care exhibited in keeping, and the risk of insufficient precautions must rest with the party claiming the privilege."[84]

Therefore, in order to qualify as privileged, there must be a reasonable expectation of privacy in e-mail communications. Additionally, in some jurisdictions, a court must determine whether using e-mail constitutes an affirmative action to preserve confidentiality and whether it qualifies as taking all possible precautions. Some would argue that the existence of the ECPA

---

77. *Id.*

78. *See, e.g., In re* Horowitz, 482 F.2d 72, 82 (2d Cir. 1973) ("It is not asking too much to insist that if a client wishes to preserve the privilege under such circumstances, he must take some affirmative action to preserve confidentiality."); Bower v. Weisman, 669 F. Supp. 602, 605 (S.D.N.Y. 1987) (holding document not privileged because it was not confidential when left out on a table in a public room of a hotel suite and that one asserting privilege should take "all possible precautions to ensure confidentiality").

79. *See In re Grand Jury Proceedings*, 727 F.2d at 1356.

80. 482 F.2d 72 (2d Cir. 1973).

81. *Id.* at 81.

82. *See id.* at 82.

83. *See id.*

84. *Id.* (citing United States v. Kelsey-Hayes Wheel Co., 15 F.R.D. 461, 465 (E.D. Mich. 1954)).

gives electronic communication users a reasonable expectation of privacy. However, it is not clear that the existence of a statutory prohibition creates a reasonable expectation that no one will commit the prohibited act.[85] For example, a driver with the right-of-way approaching an intersection cannot simply assume that no other car will pull out in her path and, therefore, cannot close her eyes. Comparably, simply because it is a felony to intercept an electronic communication does not necessarily mean that an attorney can reasonably assume that no one will intercept such a communication.[86] Arguably, the ease of interception and the instability of the Internet create serious doubts about the reasonableness of privacy in e-mail communications.

The ECPA also contains a provision creating a legal fiction in order to maintain privilege in electronic communications that have been intercepted.[87] Section 2517(4) provides 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."[88] This provision has not been addressed by the courts, and while it purports to answer the question of attorney-client privilege due to interception, it does not address other issues that arise, including saved e-mail on the sender or recipient's computer and malpractice liability under the duty of client confidentiality.

There is one way to virtually guarantee e-mail privacy: encryption. Encryption is a method by which an encoding algorithm

---

85. In an article warning attorneys to use caution when using cellular and cordless telephones, the author noted "[i]nterception, no matter how criminal, is possible, and lawyers should use good sense when using portable telephones. Indeed, client relations considerations should require a lawyer to find out whether a portable phone is being used and discuss the implications of that fact with the client." William Freivogel, *Cellular and Cordless Telephones, Privilege, Confidentiality and Liability*, ALAS LOSS PREVENTION J., May 1997 at 7, 8.

86. *See* ABA, LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:401 (1996) (noting that criminal prohibition does not guarantee that no one will intercept a communication).

> Although federal law makes intentional interception of cordless and cellular phone communications a crime, some radio hobbyists eavesdrop on these conversations .... Although intentional interception of e-mail constitutes a federal crime, concern exists about the security of unencrypted e-mail because messages travel in plain text format and pass through intermediary computers en route to their destination.

Id.

87. *See* 18 U.S.C. § 2517(4) (1994).

88. *Id.*

is used to turn a message into unreadable text for transmission.[89] Once the message arrives at its proper destination, the recipient uses a code to decrypt the message and return it to readable text.[90] This system works with two "keys," a public key for encryption and a private key for decryption.[91] The public key is widely disseminated so that anyone wanting to send something to the holder of the encryption system can code the message using the public key.[92] The private key is known only to the system holder who is then the only party able to decode the messages encrypted with her public key.[93] Encryption software has become increasingly popular because of the insecure nature of the Internet.[94] A number of different encryption systems are readily available and are fairly easy to use.[95]

Another potential security measure which may soon be widely available is the "electronic postmark."[96] The United States Postal Service has spent three years and $20 million developing an electronic postmark which is designed to authenticate the identity of senders and receivers of electronic mail.[97] The postmark was originally tested in fifteen firms in various industries and was expected to be released to businesses by the end of 1997.[98] However, at the end of 1997, the postmark had not yet been released. Each postmark is expected to cost twenty-two cents.[99] The Postal Service also intends to develop return receipt, certified, and registered electronic mail.[100] If the electronic postmark performs as expected, it may well be a way to ensure Internet security. Furthermore, it may provide increased legal

---

89. *See* Littman, *supra* note 32, at 28-29.
90. *See id.*
91. *See* Jones, *supra* note 32.
92. *See id.*
93. *See id.*
94. *See* G. Burgess Allison, *Technology Update,* LAW PRAC. MGMT., Apr. 1996 at 16, 18.
95. *See* Merrill, *supra* note 8, at 23. Two encryption tools in particular are PGP ViaCrypt ("Pretty Good Privacy") and RSA Data Security ("Rivest, Shamir & Adelman").
96. *See* Todd Copilevitz, *Special Delivery in Cyberspace,* DALLAS MORNING NEWS, Mar. 3, 1997, at 1C.
97. *See Postal Service to Offer E-Mail Authentication,* COMPUTERWORLD, Feb. 20, 1997, at 57.
98. *See id.* Test industries include health, finance, and law. *See id.*
99. *See id.*
100. *See id.*

sanctions against interceptors who tamper with the federal mail system.

b. *Waiver of Privilege*

When the attorney-client privilege is present, the client is the exclusive holder of the privilege.[101] The communication will remain privileged even after the termination of the professional relationship, as long as the communication meets the criteria of a confidential communication and the client does nothing to waive the privilege.[102] Generally, if the client discusses or otherwise reveals the communication to a third party, the communication is no longer protected by the attorney-client privilege.[103]

However, "[t]here is no consensus . . . as to the effect of inadvertent disclosures of confidential communications. A few courts [have held] that where there has been a disclosure of privileged communications to third parties, the privilege is lost, even if the disclosure is unintentional or inadvertent."[104] The

---

101. *See, e.g.*, Hunt v. Blackburn, 128 U.S. 464, 470 (1888) (holding privilege belongs to "the client alone"); United States v. Frazier, 580 F.2d 229, 230 (6th Cir. 1978) ("[T]he attorney has no right to waive the privilege and only the client can waive it."), *cert. denied*, 439 U.S. 930 (1978); *In re* Grand Jury Proceedings, 73 F.R.D. 647, 652 (M.D. Fla. 1977) (finding an attorney cannot assert the privilege if the client has waived it); Timken Roller Bearing Co. v. United States, 38 F.R.D. 57, 64 (N.D. Ohio 1964) ("[O]nly the client can unseal his attorney's lips."). For an excellent summary of these cases, see CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, EVIDENCE § 5.6, at 352 (1995). For Colorado case law see Mountain States Tel. & Tel. Co. v. DiFede, 780 P.2d 533 (Colo. 1989); A. v. District Court, 550 P.2d 315 (Colo. 1976); *In re* E.H. and S.W., 837 P.2d 284, 291 (Colo. Ct. App. 1992) (holding "privilege is personal to the client").

102. *See* MUELLER & KIRKPATRICK, *supra* note 101, § 5.26, at 430.

103. *See* Wilcoxon v. United States, 231 F.2d 384, 386 (10th Cir. 1956).

104. Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (finding no error in district court's decision finding attorney-client privilege for inadvertently produced materials); *see also* Texaco P.R., Inc. v. Department of Consumer Affairs, 60 F.3d 867, 883 (1st Cir. 1995) (holding that the waiver of privilege by inadvertent disclosure of documents also waived the privilege for all other related documents); *In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984) (citing with approval *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina Inc.*, 91 F.R.D. 254 (N.D. Ill. 1988)); Weil v. Inv./Indicators, Research & Management, Inc., 647 F.2d 18, 24 (9th Cir. 1981) ("'[I]nadvertence' of disclosure does not as a matter of law prevent the occurrence of the waiver"); FDIC v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992) (finding no privilege in document disclosed to opposing counsel saying "one cannot 'unring' a bell"); International Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 450 (D. Mass. 1988) (denying motion for protective order for documents produced inadvertently during disclosure noting "a strict rule that 'inadvertent' disclosure results in a waiver of the privilege would probably do more than anything else to

courts applying this strict rule of waiver base their reasoning on the idea that the amount of care exercised with the confidential communication reflects the relative importance of the confidentiality of the communication.[105] Other courts, however, do not apply a "strict responsibility" rule. Instead, some evaluate the facts on a case-by-case basis to determine whether the client has waived the privilege.[106] These courts weigh factors including the

---

instill in attorneys the need for effective precautions against such disclosure"); *In re* Standard Fin. Management, 77 B.R. 324, 330 (Bankr. D. Mass. 1987) (allowing inadvertent disclosure holding that "mistake or inadvertence is, after all, merely a euphemism for negligence, and, certainly . . . one is expected to pay a price for one's negligent actions"); Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 258 (N.D. Ill. 1981) (holding "even inadvertent communication to third parties, such as bystanders or eavesdroppers, destroys the privilege, at least where the eavesdropping is not surreptitious and the attorney and client have made little effort to insure that they are not overheard"); Duplan Corp. v. Deering Milliken Inc., 397 F. Supp. 1146, 1162 (D.S.C. 1974) (rejecting the contention that waiver of the attorney-client privilege requires intentional relinquishment of that right); Underwater Storage, Inc. v. U.S. Rubber Co., 314 F. Supp. 546, 549 (D.D.C. 1970) (inadvertently disclosed document loses privilege when "[i]ts confidentiality was breached thereby destroying the basis for the continued existence of the privilege"); Clark v. State, 261 S.W.2d. 339 (Tex. Crim. App. 1953), *cert. denied*, 346 U.S. 855 (1953) (telephone operator may testify regarding contents of otherwise privileged telephone conversation heard by eavesdropping).

105. *See In re* Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989) (holding that "the amount of care taken to ensure confidentiality reflects the importance of that confidentiality to the holder of the privilege").

106. *See Alldread*, 988 F.2d 1425 (adopting a test that balances the facts on a case-by-case basis and holding that such a test is preferable because it "serves the purpose of the attorney-client privilege, the protection of communications which the client fully intended would remain confidential, yet at the same time will not relieve those claiming the privilege of the consequences of their carelessness"); Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 105 (S.D.N.Y. 1985) (holding that the determination of whether privilege remains after an inadvertent waiver must be based on "the reasonableness of the precautions to prevent inadvertent disclosure, the time taken to rectify the error, the scope of the discovery and the extent of the disclosure"); Transamerica Computer Co. v. International Bus. Mach. Corp., 573 F.2d 646 (9th Cir. 1978) (finding no waiver of privilege to certain documents accidentally delivered in discovery when discovery included 17 million pages of documentation); Prescient Partners L.P. v. Fieldcrest Cannon, Inc., No. 96 Civ. 7590 (DAB)(JCF), 1997 WL 736726 (S.D.N.Y. Nov. 26, 1997) (applying the balancing test, and finding no waiver where a paralegal turned over privileged documents due to the paralegal's poor health); Aramony v. United Way of Am., 969 F. Supp. 226 (S.D.N.Y. 1997) (applying the *Lois Sportswear* factors and finding no waiver); Hartford Fire Ins. Co. v. Garvey, 109 F.R.D. 323 (N.D. Cal. 1985) (adopting *Lois Sportswear* balancing factors, applying them to a waiver of work-product privilege and finding waiver where available precautions were not taken to protect confidentiality of the document); Abamar Housing & Dev., Inc. v. Lisa Daly Lady Decor, Inc., 698 So. 2d 276 (Fla. Dist. Ct. App. 1997) (holding the "relevant circumstances" test to be the best of the three tests and finding no waiver where 23

reasonableness of precautions taken, the number and extent of any disclosures, and the interest of justice in determining whether finding disclosure is reasonable.[107] Other courts have created an almost per se rule that an inadvertent disclosure shall not constitute a waiver.[108]

In some jurisdictions then, waiver can result from failure by the attorney or the client to take precautions to keep a communication confidential.[109] Similarly, a client can waive the attorney-

---

documents were inadvertently produced in a discovery process that included 21 boxes of documents).

107. *See Lois Sportswear*, 104 F.R.D. at 105 (factors to be weighed include: (1) the reasonableness of the precautions taken to prevent inadvertent disclosure; (2) the time taken to rectify the error; (3) the scope of the discovery and the extent of the disclosure; and (4) overarching issues of fairness); *see also* Berg Elec., Inc. v. Molex, Inc., 875 F. Supp. 261 (D. Del. 1995).

108. *See* Kondakjian v. Port Authority, No. 94 Civ. 8013 (AGS)(DFE), 1996 WL 139782, at *3 (S.D.N.Y. Mar. 28, 1996) (recommending adoption of a rule prohibiting attorneys from examining documents inadvertently disclosed, and noting "[a] single mistaken touch on a computer keyboard may be enough to send an errant fax or misdirect electronic mail and instantaneously send information to the wrong person"); Berg Elec., Inc. v. Molex, Inc., 875 F. Supp. 261 (D. Del. 1995); Georgetown Manor, Inc. v. Ethan Allen, Inc., 753 F. Supp. 936 (S.D. Fla. 1991) (no waiver of transcript of attorney-client conversation where the transcript was disclosed to opposing counsel due to attorney negligence); Helman v. Murry's Steaks, Inc., 728 F. Supp. 1099, 1104 (D. Del 1990) (inadvertently disclosed documents should not waive the privilege because "it would fly in the face of the essential purpose of the attorney-client privilege to allow a truly inadvertent disclosure of a privileged communication by counsel to waive the client's privilege"); Mendenhall v. Barber-Green Co., 531 F. Supp. 951, 954-55 (N.D. Ill. 1982) (holding: "if we are serious about the attorney-client privilege and its relation to the client's welfare, we should require more than . . . negligence by counsel before the client can be deemed to have given up the privilege"); O'Mary v. Mitsubishi Elec. Am., 69 Cal. Rptr. 2d 389, 399 (Cal. Ct. App. 1997) (declining to adopt a "gotcha" theory of waiver where there is no voluntary waiver by the client).

109. *See* Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (finding no error in district court's decision finding attorney-client privilege for inadvertently produced materials); *see also* Texaco P.R., Inc. v. Department of Consumer Affairs, 60 F.3d 867, 883 (1st Cir. 1995) (holding that the waiver of privilege by inadvertent disclosure of documents also waived the privilege for all other related documents); *In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984) (citing with approval *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina Inc.*, 91 F.R.D. 254 (N.D. Ill. 1988)); Weil v. Inv./Indicators, Research & Management, Inc., 647 F.2d 18, 24 (9th Cir. 1981) ("'[I]nadvertence' of disclosure does not as a matter of law prevent the occurrence of the waiver"); FDIC v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992) (finding no privilege in document disclosed to opposing counsel saying "one cannot 'unring' a bell"); International Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 450 (D. Mass. 1988) (denying motion for protective order for documents produced inadvertently during disclosure noting "a strict rule that 'inadvertent' disclosure results in a waiver of the privilege would probably do more than anything else to instill in attorneys the need for effective precautions against such disclosure");

client privilege if a third party is privy to the communication.[110] Thus, in the context of communications over the Internet, a court could find a waiver of the privilege if an e-mail communication were accessed by a third party, or if a court were to determine that use of the medium itself did not qualify as a sufficient precaution because the messages were potentially accessible. The ABA/BNA Lawyer's Manual on Professional Conduct advises that waiver may arise if "confidential communications are intercepted and disclosed to opposing counsel or other unintended recipients by a third party or if confidential material is mistakenly faxed or e-mailed to the wrong person."[111] Arguably, there is a potential for waiver of the privilege in the use of electronic communications.

This potential for waiver is greater due to the narrow construction given to the privilege by courts.[112] It is frequently noted that the attorney-client privilege is "in derogation of every man's evidence, . . . [and] is an obstacle to the investigation of the truth, [therefore,] . . . [i]t ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle."[113] Although the formulation of the attorney-client privilege

---

In re Standard Fin. Management, 77 B.R. 324, 330 (Bankr. D. Mass. 1987) (allowing inadvertent disclosure holding that "mistake or inadvertence is, after all, merely a euphemism for negligence, and, certainly . . . one is expected to pay a price for one's negligent actions"); Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 258 (N.D. Ill. 1981) (holding "even inadvertent communication to third parties, such as bystanders or eavesdroppers, destroys the privilege, at least where the eavesdropping is not surreptitious and the attorney and client have made little effort to insure that they are not overheard"); Duplan Corp. v. Deering Milliken Inc., 397 F. Supp. 1146, 1162 (D.S.C. 1974) (rejecting the contention that waiver of the attorney-client privilege requires intentional relinquishment of that right); Underwater Storage, Inc. v. U.S. Rubber Co., 314 F. Supp. 546, 549 (D.D.C. 1970) (inadvertently disclosed document loses privilege when "[i]ts confidentiality was breached thereby destroying the basis for the continued existence of the privilege"); Clark v. State, 261 S.W.2d. 339 (Tex. Crim. App. 1953), *cert. denied*, 346 U.S. 855 (1953) (telephone operator may testify regarding contents of otherwise privileged telephone conversation heard by eavesdropping).

110. *See id.*

111. *Electronic Communications*, ABA/BNA LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:401 (Oct. 30, 1996).

112. *See* Weil v. Inv./Indicators, Research & Management, 647 F.2d 18 (9th Cir. 1981) (privilege must be strictly construed because it impedes full and free discovery of the truth); Underwater Storage, Inc. v. United States Rubber Co., 314 F. Supp 546 (D.D.C. 1970) (holding that "[t]he attorney-client privilege has such an effect on the full disclosure of the truth that it must be narrowly construed").

113. *In re* Horowitz, 482 F.2d 72, 81 (2d Cir. 1973), *cert. denied*, 414 U.S. 867 (1973) (citing 8 JOHN HENRY WIGMORE, WIGMORE ON EVIDENCE § 2192, at 70, and

varies from jurisdiction to jurisdiction, generally "the privilege is not easily invoked and is easily destroyed."[114] Because some courts are willing to find waiver of privilege even where the disclosure is inadvertent, and because most courts apply the privilege narrowly, waiver of privilege can easily arise as a problem in any form of communication. However, the potential for waiver in electronic communication appears to be even greater.

2. Client Confidence

While not law, the ABA Model Rules of Professional Conduct and Model Code of Professional Responsibility are affirmative commands proscribing ethical attorney conduct. Violations of these rules expose an attorney to disciplinary action by the bar.[115] Model Rule 1.6 requires that a lawyer shall not reveal information pertaining to her client.[116] The comments to that rule explain that a "lawyer must make every effort practicable to avoid unnecessary disclosure of information related to the representation."[117] Similarly, Canon 4 of the Code of Professional Responsibility provides that "a lawyer should preserve the confidences and secrets of a client."[118] Both rules require an attorney to take affirmative action to ensure the privacy of the client's communications.[119]

---

§ 2291, at 554 (McNaughton rev. ed. 1961)), *quoted with approval in* United States v. Pipkins, 528 F.2d 559, 563 (5th Cir. 1976).

114. Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 258 (N.D. Ill. 1981).

115. The Bar Associations in 43 states and the District of Columbia have adopted the Model Rules in some form. California follows neither the Rules nor the Code and instead has its own professional conduct regulations. Illinois, New York, North Carolina, Oregon, and Virginia all have adopted a combination of the Model Code and the Model Rules. *See* STATE ETHICS RULES, ABA/BNA LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA) 01:3-4 (Aug. 20, 1997); MAINE RULES OF COURT, (West 1997). Georgia, Iowa, Nebraska, Ohio, Tennessee, and Vermont have regulations based on the Model Code. *See* GEORGIA RULES OF COURT ANNOTATED, (Michie 1998); IOWA RULES OF COURT, (West 1998); NEBRASKA COURT RULES AND PROCEDURE, (West 1998); RULES GOVERNING THE COURTS OF OHIO, (Anderson 1997-98); TENNESSEE COURT RULES ANNOTATED, (Michie 1997-98); VERMONT COURT RULES ANNOTATED, (Michie 1997).

116. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1983).

117. MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6. cmt. (1983).

118. MODEL CODE OF PROFESSIONAL RESPONSIBILITY Canon 4 (1980).

119. The rules are derived from the common law of agency which prohibits an agent from disclosing or using any confidential information related to the principal.

The rule of client confidence has a broader scope than the attorney-client privilege.[120] First, the confidence rule includes all information relating to a client's representation, while the privilege concerns only communications and what is learned or observed as a result of that communication.[121] Furthermore, the confidence rule prohibits disclosure to any third party, while the privilege is only applicable against a legal authority.[122] Because of this broad coverage, an attorney's conduct may be adequate to maintain the attorney-client privilege and at the same time be violative of the client confidence rule. Such conduct could subject an attorney to disciplinary action or malpractice claims.

Though several bar associations have adopted formal ethics opinions on the subject of the confidence rule as it relates to modern communications,[123] only a few have addressed the issue as it concerns the use of e-mail. Of those associations addressing the issue, four have found that there should be a reasonable expectation of privacy in electronic communications on the Internet,[124] while three have concluded that e-mail is an insecure medium and, therefore, requires that the attorney inform the client of the potential loss of confidentiality.[125] The split of authority on the issue reflects the uncertainty in the legal

---

See Protected Information ABA/BNA LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:302 (May 20, 1992).

120. See Hazard, *supra* note 63.

121. *See* MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1983); Hazard, *supra* note 62; *see also* People v. Merideth, 631 P.2d 46 (Cal. 1981).

122. *See, e.g.*, COLO. REV. STAT. § 13-90-107(1)(b) (1997); Hazard, *supra* note 63.

123. *See, e.g.*, Colorado Bar Ass'n Ethics Comm., Op. No. 90 (1992) (concluding that a lawyer using electronic communication devices such as cordless and cellular telephones, computer modems, e-mail, and faxes must exercise reasonable care); Illinois Bar Ass'n Ethics Comm., Op. 90-7 (1990) (finding no confidentiality in cellular telephones); Iowa Bar Ass'n Ethics Comm., Op. 90-44 (1991) (finding no confidentiality in cellular telephone conversations); Massachusetts Bar Ass'n Ethics Comm., Op. 94-5 (1994) (finding no confidentiality in cellular telephone conversations); New Hampshire Bar Ass'n Ethics Comm., Op. 1991-92/6 (1992) (finding no confidentiality in cellular telephone conversations); New York Bar Ass'n Ethics Comm., Op. 1994-11 (1994) (finding no confidentiality in cellular telephone conversations).

124. Those state bar associations are: Illinois, North Dakota, South Carolina, and Vermont. *See* Illinois Bar Ass'n Ethics Comm., Op. 96-10 (May 16, 1997); North Dakota Bar Ass'n Ethics Comm., Op. 97-09 (1997); South Carolina Bar Ethics Comm., Op. 97-08 (Sept. 1997) (reversing earlier opinion concluding that e-mail was not confidential); Vermont Bar Ass'n Ethics Comm., Op. 97-5 (1997).

125. *See* Arizona Bar Ass'n Ethics Comm., Op. 97-04 (1997); North Carolina State Bar, *Modern Communications Technology and the Duty of Confidentiality*, RPC 215 (July 1995); Iowa Bar Ass'n Ethics Comm., Op. 96-1 (1996).

community as a whole. In those jurisdictions cautioning attorneys in the use of e-mail, the existence of formal ethics opinions arguably creates a standard of reasonable care.[126] An attorney's failure to use the degree of care and skill standard in the community may result in attorney malpractice if the failure is the proximate cause of a client's injury.[127]

---

126. Whether evidence of an ethical rule or an ethics opinion can be used as evidence of the community standard of care varies from jurisdiction to jurisdiction. *See* Avianca, Inc. v. Corriea, 705 F. Supp. 666 (D.D.C. 1989) (rules can be evidence of a minimum level of professional conduct); Griva v. Davison, 637 A.2d 830 (D.C. 1994) (evidence of violation of ethics rules can prove breach of fiduciary duty); Fishman v. Brooks 487 N.E.2d 1377 (Mass. 1986) (holding that expert testimony concerning an ethical violation is not appropriate, but expert testimony about attorney duty of care is appropriate and can be based on failure to conform to ethical rules); Mirabito v. Liccardo, 5 Cal. Rptr. 2d 571 (Cal. Ct. App. 1992) (permitting introduction of ethical rules as evidence of malpractice); Lipton v. Boesky 313 N.W. 2d 163 (Mich. Ct. App. 1981) (holding that "a violation of the code is rebuttable evidence of malpractice"). *But see* Hizey v. Carpenter 830 P.2d 646 (Wash. 1992) (holding that a jury cannot be informed of ethical rules in a legal malpractice action).

127. *See generally* Alldread v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993) (finding no error in district court's decision finding attorney-client privilege for inadvertently produced materials); *see also* Texaco P.R., Inc. v. Department of Consumer Affairs, 60 F.3d 867, 883 (1st Cir. 1995) (holding that the waiver of privilege by inadvertent disclosure of documents also waived the privilege for all other related documents); *In re* Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984) (citing with approval *Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina Inc.*, 91 F.R.D. 254 (N.D. Ill. 1988)); Weil v. Inv./Indicators, Research & Management, Inc., 647 F.2d 18, 24 (9th Cir. 1981) ("'[I]nadvertence' of disclosure does not as a matter of law prevent the occurrence of the waiver"); FDIC v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992) (finding no privilege in document disclosed to opposing counsel saying "one cannot 'unring' a bell"); International Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 450 (D. Mass. 1988) (denying motion for protective order for documents produced inadvertently during disclosure noting "a strict rule that 'inadvertent' disclosure results in a waiver of the privilege would probably do more than anything else to instill in attorneys the need for effective precautions against such disclosure"); *In re* Standard Fin. Management, 77 B.R. 324, 330 (Bankr. D. Mass. 1987) (allowing inadvertent disclosure holding that "mistake or inadvertence is, after all, merely a euphemism for negligence, and, certainly . . . one is expected to pay a price for one's negligent actions"); Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 258 (N.D. Ill. 1981) (holding "even inadvertent communication to third parties, such as bystanders or eavesdroppers, destroys the privilege, at least where the eavesdropping is not surreptitious and the attorney and client have made little effort to insure that they are not overheard"); Duplan Corp. v. Deering Milliken Inc., 397 F. Supp. 1146, 1162 (D.S.C. 1974) (rejecting the contention that waiver of the attorney-client privilege requires intentional relinquishment of that right); Underwater Storage, Inc. v. U.S. Rubber Co., 314 F. Supp. 546, 549 (D.D.C. 1970) (inadvertently disclosed document loses privilege when "[i]ts confidentiality was breached thereby destroying the basis for the continued existence of the privilege"); Clark v. State, 261 S.W.2d. 339 (Tex. Crim. App. 1953), *cert. denied*, 346 U.S. 855 (1953) (telephone operator may testify regarding contents of otherwise privileged telephone conversation heard by eavesdropping); RONALD E. MALLEN & JEFFREY M.

Because current encryption technology makes it so easy to ensure a reasonable degree of privacy on the Internet, it is no stretch to assume that attorneys who have an affirmative duty to ensure privacy or "make every effort practicable to avoid unnecessary disclosure"[128] are under a duty to encrypt their e-mail communications. Regardless of what the industry standard may be, lawyers are well advised to remember *T.J. Hooper*.[129] In that case, the court determined that the industry standard was negligent in itself. In this well-known opinion, Justice Learned Hand wrote: "[T]here are precautions so imperative that even their universal disregard will not excuse their omission."[130] Encryption, because of its safety, ease, and availability may well be just such a precaution.

This degree of reasonable care and the affirmative duty applies to the use of e-mail communications. Consequently, sending an e-mail message through the Internet may violate an attorney's ethical duty to take affirmative steps to maintain client confidences. Furthermore, depending upon how one characterizes the e-mail communication, it may not carry a reasonable expectation of confidentiality, in which case the attorney-client privilege may not apply. For example, a conversation between an attorney and a client that is held in a private room outside the presence of third parties is privileged.[131] If a client is in a crowded area talking to his attorney with a megaphone, the communication is not privileged.[132] To ascertain whether e-mail communications are confidential, one must determine at what point on this spectrum these communications lie; whether they are more like talking in a private room or speaking with a megaphone. In determining how courts will apply the privilege and the duty of confidence to electronic communications, it is appropriate to

---

SMITH, LEGAL MALPRACTICE, §§ 18.2-18.6 (4th ed. 1996).

128. MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 cmt. (1983).

129. 60 F.2d 737 (2d Cir. 1932), *cert. denied*, 287 U.S. 662 (1932) (holding that although there was not a general practice in the tugboat industry of equipping boats with radio receivers, the tugboat owners involved in the case were negligent in their failure to equip their boats with such devices. The lack of radio recievers was the direct cause of the loss of the boats, and the tug owners were liable to the owners of lost cargo).

130. *Id.* at 740.

131. *See* MUELLER & KIRKPATRICK, *supra* note 101, § 5.13, at 379.

132. *See id.* § 5.13, at 384.

examine the analysis courts have already applied to e-mail communications and to other forms of communication.

II. CONFIDENTIALITY IN E-MAIL AND POSSIBLE ANALOGIES IN THE LAW

A. E-Mail in the Courts

Few courts have addressed the novel problems that e-mail and the Internet present because the technology is so new. However, a number of courts have addressed the general topic of e-mail and privacy. Not surprisingly, the decisions span the privacy spectrum.[133] In the few cases that have gone to trial on the issue of company e-mail, the courts have held that an employee has no expectation of privacy in company e-mail.[134] Several courts have held that an employer may monitor the e-mail communications of employees so long as the employer has not made assurances to the contrary.[135] On the other hand, at least one court has found that a subscriber to an online computer service *did* have a reasonable expectation of privacy in the e-mail messages he sent using that service.[136]

---

133. *See, e.g.*, Bohach v. Reno, 932 F. Supp. 1232 (D. Nev. 1996) (finding that police officers had no reasonable expectation of privacy in an e-mail paging system run by their city employer); Smith v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (holding that an employee has no right to privacy in company e-mail); United States v. Baker, 890 F. Supp. 1375 (E.D. Mich. 1995) (dicta in criminal rape conspiracy case characterized e-mail messages sent over the Internet as "private"); Strauss v. Microsoft Corp., No. 91 Civ. 5928 (SWK), 1995 WL 326492 (S.D.N.Y. June 1, 1995) (holding that employee e-mails were admissible against company in sex-discrimination suit); United States v. Maxwell, 42 M.J. 568 (A.F.C.M.R. 1995), *rev'd on other grounds* 45 M.J. 406 (C.A.A.F. 1996) (finding a reasonable expectation of privacy in an e-mail transmission sent through the America Online Internet service provider).

134. *See, e.g., Bohach*, 932 F. Supp. at 1232; *Pillsbury*, 914 F. Supp. at 101; *Strauss*, 1995 WL 326492. For an excellent discussion of the issues involved in company e-mail privacy, see Julia Turner Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923 (1992).

135. *See Pillsbury*, 914 F. Supp. at 101 (holding: "[o]nce plaintiff communicated the alleged unprofessional comments to a second person . . . over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.").

136. *See Maxwell*, 42 M.J. at 568. In this case, the defendant was a subscriber to America Online and had used his e-mail service to send and receive child pornography. Defendant argued that the search of his America Online files producing the evidence was a violation of defendant's Fourth Amendment rights. *See id.*

To date, only a few cases have directly addressed the issue of attorney-client privilege in e-mail. The first case is a Massachusetts trial court opinion—*National Employment Service Corp. v. Liberty Mutual Insurance Co.*[137] The plaintiff in that case sought production of thirty-two e-mail communications sent between defendant's in-house counsel and the defendant's other employees.[138] The court held that the e-mail messages were protected by the attorney-client privilege because they were a series of messages concerning legal issues.[139] However, because this case involved an internal e-mail system that did not use the Internet for delivery, Internet privacy issues were not addressed by the court.

Another case, *State v. Canady*,[140] also held that an e-mail message was covered by the attorney-client privilege. The holding in this case was based on the principle that the privilege applied to the substance of the communication, not the method of communication. The court noted, however, that the findings of fact in the trial court's opinion were sparse and indicated that upon reconsideration, the court could find that the privilege had been waived.[141] The cases concerning e-mail and confidential communications, therefore, are less than definitive.

B. Telephone Communication Cases

It is accepted that if an attorney and client have a conversation on the telephone, each in her own office with the doors closed, the communication is confidential.[142] However, outside the mundane territory of ordinary land-line telephone conversations, the issues become substantially less clear. New technolo-

---

137. No. 93-2528-G, 1994 WL 878920 (Mass. Super. Ct. Dec. 12, 1994).
138. *See id.*
139. *See id.*
140. 460 S.E.2d 677 (W. Va. 1995).
141. *See id.* at 689 n.17.
142. *See* United States v. Hall, 488 F.2d 193, 196 (9th Cir. 1973). In *Hall*, the court held, "[w]hen a person talks by telephone, he can reasonably assume privacy." However, this is not to say that all traditional land-line telephone calls are completely under the auspices of a reasonable expectation of privacy. In fact, some parts of land-line conversations are not reasonably private. *See* United States v. Parrillo, 34 M.J. 112 (C.M.A. 1992) (holding that there is no reasonable expectation of privacy on a telephone once the communication has reached the other end).

gies in telephone communications such as cordless and cellular telephones have raised new privacy issues.

The first case to deal with privacy issues arising from the use of cordless telephones was the early 1970s case, *United States v. Hoffa*.[143] In that case, Jimmy Hoffa and his fellow defendants challenged the evidentiary use of their conversations overheard by the Federal Bureau of Investigation. Those conversations were made over mobile telephones using F.M. radio signals. The court[144] held that there was no privacy in the communications, stating simply: "[s]urely, there was no expectation of privacy as to the Hoffa calls in Detroit which were exposed to everyone in that area who possessed a F.M. radio receiver or another automobile telephone tuned in to the same channel."[145] Of the nine calls overheard in that case, a number of them involved communications between the defendants and their attorneys.[146] The court held that neither the subject nor the parties involved in these conversations were important; no privacy could attach to these conversations because there was no reasonable expectation of privacy.[147]

Courts have followed the reasoning set forth in *Hoffa* and have expanded the arguments underlying the outcome of that case. For example, in 1973, the Ninth Circuit held that there is no reasonable expectation of privacy in conversations held over radio-telephones in automobiles.[148] That case, *United States v. Hall*,[149] expanded the discussion to include the Federal Crime Control Act ("FCCA"),[150] which made it unlawful for private persons to "intercept and divulge wire or radio communications."[151] In *Hall*, the defendants had used the radio-telephones to discuss information pertaining to their intent to distribute marijuana.[152] A woman listening to her radio while cleaning her

143. 436 F.2d 1243 (7th Cir. 1970).

144. The court was acting on remand from the Supreme Court. *See* Hoffa v. United States, 385 U.S. 293 (1966).

145. *Hoffa*, 436 F.2d at 1247.

146. *See id.*

147. *See id.*

148. *See Hall*, 488 F.2d at 193.

149. 488 F.2d 193.

150. Federal Crime Control Act of 1968, Pub. L. No. 90-351 § 802, 82 Stat. 212. Relevant sections include 47 U.S.C. § 605 and the Federal Wiretapping Act, 18 U.S.C. §§ 2510-2520 (1994).

151. *Hall*, 488 F.2d at 195.

152. *See id.* at 194.

home unintentionally intercepted the calls on her radio.[153] She informed the police of the suspicious behavior and the defendants were arrested and convicted.[154] Defendants argued on appeal that the intercepted conversations should be suppressed because they were acquired in violation of the FCCA.[155]

The FCCA was important because it gave the court a basis for discerning between "oral" and "wire" communications. If the radio-telephone conversations were oral communications, they required a demonstration of the speaker's reasonable expectation of privacy in order to be confidential.[156] Yet, because of the way those terms were defined by the FCCA, if the communications were held to be wire communications, the expectation of privacy was understood.[157] The *Hall* court stated:

> Broadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megatelephone than it is to the privacy afforded by a wire. As with any broadcast into the air, the invitation to listen is afforded to all those who can hear. In the instant case, the eavesdroppers merely tuned their radio receivers to the proper station. It is obvious that conversations initiated from a radio-telephone more logically fall within the category of "oral communication."[158]

Yet even after describing the cordless telephone communications in this manner, the court held that if one part of the communication took place on a land-line telephone, the entire communication qualified as a wire communication and was presumed private.[159] This decision proved to be contentious in future decisions by other courts because of the anomalous results that followed from its application.[160] Under the *Hall* rationale, if one party is on a cordless telephone speaking with a party on a land line, it is irrelevant that the conversation can be easily

---

153. *See id.* at 194-95.
154. *See id.* at 195.
155. *See id.* at 194.
156. *See id.* at 196.
157. *See id.*
158. *Id.* at 196-97.
159. *See id.*
160. *See* Tyler v. Berodt, 877 F.2d 705 (8th Cir. 1989); State v. Smith, 438 N.W.2d 571 (Wis. 1989); State v. Delaurier, 488 A.2d 688 (R.I. 1985); State v. Howard, 679 P.2d 197 (Kan. 1984); State v. Fata, 529 N.Y.S.2d 683 (Co. Ct. 1988).

overheard because the land-line communication is over wire which gives it a presumption of privacy.

A series of decisions in the 1980s declined to follow this part of *Hall* and held that cordless telephones could not be considered a confidential method of communication.[161] These decisions were also supported by the ECPA.[162] Part of the ECPA overruled *Hall*'s holding that cordless communications are "wire" if one part is land-line based. However, "the emerging view [was] that cordless telephone transmissions were not 'wire communications' even before the 1986 amendment."[163]

These decisions were largely based on the ease of interception of cordless telephone communications broadcast by F.M. radio signal. Both the *State v. Smith*[164] and *State v. Howard*[165] courts noted that there had been testimony at trial regarding the lack of privacy on cordless telephones. In *State v. Smith,* the court cited a Federal Communications Commission ("FCC") requirement that cordless telephones "must bear the legend, 'Privacy of communications may not be ensured while using this telephone.'"[166] The court regarded this FCC requirement as a societal pronouncement that there should be no expectation of confidentiality in cordless telephone conversations.[167]

This rule of law, however, like all things related to high technology, was bound to change. In 1992, the Fifth Circuit announced its ruling in *United States v. Smith.*[168] While upholding the rules of *Howard* and *State v. Smith* as to the admissibility

---

161. *See Tyler*, 877 F.2d at 705; *State v. Smith*, 438 N.W.2d at 571; *Delaurier*, 488 A.2d at 688; *Howard*, 679 P.2d at 197; *Fata*, 529 N.Y.S.2d at 683.

162. 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.). Although a 1994 amendment eliminated exceptions for the interception of cordless telephone calls and made interception illegal, the cases decided before that amendment are instructive nonetheless. *See* Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994).

163. *Tyler*, 877 F.2d at 706.

164. 438 N.W.2d at 573.

165. 679 P.2d at 199.

166. 438 N.W.2d at 577 (citing 47 C.F.R. § 15.236 (1987)); *see also* FCC warning requirement, 47 C.F.R. § 15.214(c) (1995).

167. *See State v. Smith*, 438 N.W.2d at 577; *see also* McKamey v. Roach, 55 F.3d 1236, 1240 (6th Cir. 1995) (finding no confidentiality in a cordless telephone conversation and noting that the telephone owner's manual cautioned that "'[i]t is not possible to ensure privacy of communication'" when using the cordless telephone).

168. 978 F.2d 171 (5th Cir. 1992).

of evidence gained by an eavesdropping neighbor under the ECPA, the court discussed the expectation of privacy under the Fourth Amendment. The defendant in *United States v. Smith* was charged with drug trafficking offenses as a result of his neighbor's eavesdropping on defendant's conversations conducted on a cordless telephone.[169]

The court in *United States v. Smith* began the discussion of the reasonable expectation of privacy under the Fourth Amendment by explaining that what is "really involved" is the "societal understanding" concerning what deserves protection.[170] In this vein, the court elaborated on how important communications technology had become in our society, noting that "[n]o one would dispute that the importance of telecommunications today has outstripped anything imagined twenty five years ago."[171] Further, the court cited statistics on the use of cordless telephones[172] and suggested that cordless telephones will one day replace land-line telephones altogether. If this were the case, the court stated, then the decision of whether cordless telephone conversations are private might answer the question of "whether *any* telephone conversation" is private.[173] While upholding *Howard* and the other cordless telephone cases, the court stated that "[t]here is nothing magical about a telephone line," and that the inquiry in these cases should be on a case-by-case basis in which courts must look to the type of technology used to determine whether there is a reasonable expectation of privacy.[174] A bright-line rule is inappropriate because communications technology is improving so rapidly.[175] The court noted that the cordless telephones on the market since 1992 often scramble the radio signal so that even those people with scanners cannot understand the conversation.[176] However, as a direct result of the case-by-case basis on which these decisions will be made, the state of the law on cordless telephones remains unclear. Thus, it is reasonable to

169. *See id.*
170. *Id.* at 177.
171. *Id.*
172. *See id.* ("[N]early half of the 95 million U.S. households use cordless telephones.").
173. *Id.*
174. *See id.* at 179-80.
175. *See id.* at 180.
176. *See id.* at 179.

assume that in any given conversation held on a cordless telephone, privacy is not guaranteed.

Another modern communications device frequently used in business today is the cellular telephone. Cellular telephones present issues similar to those presented by cordless telephones.[177] Cellular telephones use radio waves to transmit from a local "cell" to and from the receiver. These waves can be intercepted with scanners that can be purchased at any local radio or electronics store.[178] In *State v. Wilson,*[179] the Illinois Appellate Court held that cellular telephone conversations could not be considered private because of the use of radio waves for transmission. An identical result was reached by the Georgia Appellate Court in *Salmon v. State.*[180] Similarly, in *Edwards v. Bardwell,*[181] the court held that it was not a violation of eavesdropping law for someone to listen to a cellular telephone call because of the insecure nature of the medium.[182] However, the court was presented with another problem in *Edwards*: the conversation in question was between an attorney and his client.[183] The court did

177. Though the issues are similar, the technology is different enough to warrant its own analysis. This is because the ease of interception of each technology is different. Cordless telephones are often used around the house and transmit signals using F.M. frequencies. These telephones require a base transmitter and generally transmit no more than approximately 1000 feet. Cellular telephones, of which there are two kinds, use different technology. Analog cellular telephones use radio frequencies that can be intercepted by police scanners or illegally modified, commercially available scanners. Although it is more difficult to intercept these conversations than a cordless telephone conversation, it can be accomplished as evidenced by a Florida couple's interception of a highly sensitive conversation between Newt Gingrich, his attorney, and several high-ranking Republican Congressmen in January of 1997. The second type of wireless telephone technology is the digital cellular. This system converts a telephone conversation to a computer binary code of 0s and 1s. Though originally thought to be a very secure form of communication, the code was cracked by two computer hackers in March of 1997. *See* Wendy R. Liebowitz, *Cell, Cordless and Digital Telephones Raise Privilege, Privacy Questions*, NAT'L L.J., Aug. 25, 1997, at B20; Mitchell C. Shelowitz, *Attorney-Client Privilege and Wireless Communications*, N.Y. L.J., Feb. 3, 1997, at 1; Freivogel, *supra* note 84.

178. These same scanners also pick up cordless telephone conversations, police and fire dispatch communications, and even the neighbor's baby monitor.

179. 554 N.E.2d 545 (Ill. App. Ct. 1990).

180. 426 S.E.2d 160 (Ga. Ct. App. 1992) (holding there could be no expectation of privacy in a cellular telephone conversation where the telephone used radio waves to transmit the conversation).

181. 632 F. Supp. 584 (M.D. La. 1986).

182. *See id.* at 589.

183. *See id.*

not address the issue of privilege, stating instead: "Plaintiff claims that the conversation between him and his attorney is subject to the attorney-client privilege. It may or may not so qualify because of the method used to broadcast it, but no one is attempting to offer the contents of that conversation in evidence."[184] Instead, the tapes of the conversations were sealed.[185]

Since cellular and cordless telephone calls are not necessarily private, it is possible to predict how the courts might treat e-mail communications. Clearly, conversations held strictly on a land line are reasonably private. In contrast, communications that are not scrambled and are broadcast over radio waves are not reasonably private. E-mail falls between the two extremes. E-mail communications on the Internet do use land lines, so in some sense the cellular and cordless telephone cases do not apply—e-mail messages are not broadcast by radio waves at any point on their journey.[186] However, the cordless and cellular telephone cases are important for determining which factors courts will examine to determine whether privacy exists in new technology communication media.

In establishing whether a party has a reasonable expectation of privacy in Internet communications, a court may look at the communication medium itself. At least one popular Internet browser contains a warning to its users that the Internet is an insecure medium which can "pose a security problem."[187] Just as

---

184. *Id.*

185. *See id.*

186. It is likely that at some point Internet connections from remote modems using cellular technology will be widespread. It is also likely that in the near future some providers will use satellite relays to convey electronic messages on the Internet. However, because that is not the case currently, this comment focuses solely on land-line Internet connections.

187. MICROSOFT, INTERNET EXPLORER 3.0, at Help Menu, Security (1996). The menu also explains:

> The Internet works by sending information from computer to computer until the information reaches its destination. When data is sent from point A to point B, every computer in between has an opportunity to look at what's being sent. . . .
>
> For example, you are viewing a clothing catalog on the World Wide Web and you decide to buy a shirt. [You must provide the company with your personal information including your credit card number.] Unfortunately, one of the computers in between has been infiltrated by criminals who watch the data passing through that computer until they see something interesting, such as your credit-card number.
>
> How often does this happen? It's hard to say, but the important thing is that it's technically possible. And, as the Internet grows, it could happen more and more.

the court in *State v. Smith* looked to the warning on cordless telephones to find that the medium was not secure, a court could look to the Microsoft Internet Explorer warning and determine that there is no legitimate expectation of privacy.[188] If the sender of a message has such a warning on an e-mail system, it would not be hard for a court to determine that there was no reasonable expectation of privacy, or that the attorney had not acted in such a way as to maintain her client's confidences.

A few bar associations have addressed the issue of confidentiality in cellular telephones. The state bar associations of Iowa, Illinois, New Hampshire, Massachusetts, and New York have all released ethics opinions warning attorneys that cellular telephone communications are not confidential.[189] These opinions instruct attorneys to inform their clients of the insecure nature of the medium and either obtain consent to use cellular telephones or refrain from discussing sensitive matters.[190] Applying these precautions by analogy to e-mail communications is warranted upon a determination that e-mail is not a secure medium.

The cordless and cellular telephone cases suggest that the ease of interception is the most important factor in determining whether there is a reasonable expectation of privacy in a communication using a particular medium. Therefore, it can be reasonably assumed that the ease of interception of e-mail will be an important factor in determining questions of confidentiality. If sniffers and spoofers are as easy to use and work as well as some sources claim, it may be hard to find a reasonable expectation of privacy in e-mail communications. Similarly, because e-mail communications use the "store and forward" system,[191] the messages are necessarily available (if only for certain purposes under the ECPA[192]) for third parties to read. This represents a significant distinction between e-mail and land-line telephones because telephonic conversations on land-line telephones are not

---

Id.

188. *See supra* text accompanying note 158.

189. *See* Illinois Bar Ass'n Ethics Comm., Op. 90-7 (1990); Iowa Bar Ass'n Ethics Comm., Op. 90-44 (1991); Massachusetts Bar Ass'n Ethics Comm., Op. 94-5 (1994); New Hampshire Bar Ass'n Ethics Comm., Op. 1991-92/6 (1992); New York Bar Ass'n Ethics Comm., Op. 1994-11 (1994).

190. *See supra* note 189.

191. *See* discussion *supra* Part I.A.

192. *See supra* text accompanying note 55.

generally preserved in any form once the telephone call is finished.

Additionally, there is an important difference between e-mail and cordless and cellular telephones. When cellular and cordless telephone communications are sent between the handset and the receiver, they are sent in one message. E-mail, on the other hand, is sent in a packetized format. Generally, this means that entire documents will not use the same path to travel from origin to destination. In some cases, this makes it more difficult to intercept an e-mail message than to intercept a cordless or cellular telephone call.

Finally, e-mail differs from telephonic conversations in one other critical area. E-mail is written communication, while telephone conversations are oral. Many messages are sent by written communication everyday. With so many differences between e-mail and other communications carried over telephone lines, it is important to analogize between e-mail and other forms of communication, particularly written communications.

C. Fax Communications

Facsimile communications ("faxes") differ from cordless and cellular telephone communications because they use land-line telephone technology for transmission, eliminating the security problems that cordless and cellular telephone technology present. Faxes also differ from e-mail communications because they are not copied or stored at points between the sender and the receiver, making them more secure than e-mail. The primary concerns that arise when considering the security of faxes are: the ease of misdirecting the fax and the potential for a third party to view the communication between the time it is printed by the receiving fax machine and the time it is delivered to the intended recipient.

One court has held that the attorney who invites facsimiles has the duty to prevent third parties from viewing the documents.[194] In *Gomberg v. Zwick, Friedman & Goldbaum, P.A.*, an attorney received a fax transmission that allegedly made defamatory statements about his client, Gomberg.[195] In his

194. *Gomberg v. Zwick, Friedman & Goldbaum, P.A.*, 693 So. 2d 1064 (Fla. Dist. Ct. App. 1997).

195. *See id.* at 1064.

defamation action against the sending law firm, Gomberg claimed that publication occurred when the fax was seen by other uninvolved attorneys in the recipient law office. The court granted summary judgement for the sending law firm because Gomberg's attorney had "invited the fax" by including his fax number on his letterhead. Therefore Gomberg's attorney, not the sending law firm, had the duty to protect the confidentiality of the communication.[196]

Another court addressing the issue of confidentiality in fax transmissions found the attorney-client privilege would apply to the substance of the fax communications at issue, but noted on remand the trial court could find that the privilege was waived.[197] Applying this reasoning to e-mail communications could result in a waiver of the attorney-client privilege if a court were to conclude that the use of e-mail required an attorney to take precautions to protect client confidences and that no such precautions were taken.

The American Bar Association's Committee on Professional Conduct ("Committee") has also addressed the issue of inadvertent disclosure of confidential communications as a result of a misdirected fax. In a formal opinion, the Committee noted that the proliferation of electronic communication tools in the workplace makes it "ever more likely that through inadvertence, privileged or confidential materials will be produced to opposing counsel by no more than the pushing of the wrong speed dial number on a facsimile machine."[198] While the Committee concluded that the misdirection of a fax should not result in the loss of the confidential nature of the communication, the Committee noted that not all courts are in agreement with this conclusion.[199] The American Bar Association later released an Electronic Communications Practice Guide[200] which warned attorneys that careless use of a fax machine resulting in disclosure of confidential information to a third party could result in malprac-

196. *See id.* at 1065-66.

197. *See* State v. Canady, 460 S.E.2d 677, 689-90 (W. Va. 1995) (noting that the factual findings were insufficient to completely decide the issue).

198. ABA Comm. on Ethics and Professional Responsibility, Formal Op. 92-368 (1992).

199. *See id.*

200. ABA/BNA LAWYER'S MANUAL ON PROFESSIONAL CONDUCT (BNA), at 55:401 (1995).

tice liability or a loss of attorney-client privilege.[201] A misdirection of an e-mail is also possible and would likely trigger identical problems.

D. Postal Service, Courier, and Other Land-Based Communications

E-mail is a form of written communication. Therefore, it may be more appropriate to compare sending an e-mail message to sending a letter with the postal service. When sending a letter through the postal service, one writes the letter, addresses it, stamps it, gives it to the post office to deliver, and usually assumes that it will arrive at its destination safely. The same process applies to e-mail: one writes the message, addresses it, hits the send key, and assumes that it will reach its destination unless a message is received to indicate the contrary. Attorneys send confidential documents through the post office, couriers, and other private package delivery companies every day.[202] These documents retain their attorney-client privilege even though they are sent through third parties[203] because society has an expectation that mail sent by postal carrier is private.

There are two possible explanations for the expectation of privacy in documents sent through the postal service. The first is that there is an agency relationship between the postal carrier and the package sender.[204] In other words, the postal carrier is the sender's agent for delivery, and acting as such, cannot lose the attorney-client privilege. The second is that senders simply have an expectation that the carrier will not open or read the package and will not allow a third party to do so either. When a letter or parcel is placed in the mail, it is sealed, and it is expected to remain that way. The carrier does not divulge the contents of the package and, thus, the contents remain confidential and subject to the attorney-client privilege.[205]

---

201. *See id.*

202. Hereinafter these possible package delivery services will be referred to as "postal carriers" or simply "carriers."

203. This is not necessarily true if the package is sent to the wrong address or is left open for everyone to read once it arrives at its destination. However, if the message is sent to the correct address, it is understood that there is a reasonable expectation of privacy in the communication.

204. *See* 1 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 78 (1963).

205. *See* John Montana, *Legal Issues in EDI*, RECORDS MGMT. Q., July 1, 1996,

The agency analogy has not been widely accepted because "[t]he 'post' is not a person" and, therefore, cannot act to perform the necessary acts of an agent.[206] The "societal understanding" rationale is slightly more palatable. When someone puts a letter into the mailbox, she expects that the letter will not be opened in the same way that she expects that a land-line telephone call will not be intercepted. The question then becomes whether there is the same reasonable expectation of privacy in e-mail.

The store and forward system may well cause that question to be answered in the negative.[207] Because e-mail messages are sent through a provider and many substations across the Internet, one message may well be saved and stored in any number of locations. In *ACLU v. Reno*,[208] the court made many findings of fact about the nature of the Internet, concluding that "[u]nlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)."[209] A court applying the attorney-client privilege or determining whether an attorney has fulfilled her duty of care might well come to the same conclusion.

There are other differences between e-mail and postal mail that may lead a court to determine that use of e-mail could constitute a waiver of the attorney-client privilege or violate the duty of confidence. For example, e-mail involves the repeated saving of the message. In addition, there is the difficulty of destroying the communication. If any provider or substation has good storage or backup systems, the message may be saved indefinitely at remote locations. Even if a message is deleted, it can survive in "shadow" form forever.[210] This is not the case with traditional "snail mail" where there is only one copy sent and it is not photocopied at every post office through which it passes. If the societal expectation of privacy is the rationale for those postal

---

at 39.

206. *See* CORBIN, *supra* note 203, at 335.

207. *See supra* Part I.A.

208. 929 F. Supp. 824 (E.D. Pa. 1996).

209. *Id.* at 834.

210. *See* James H.A. Pooley & David M. Shaw, *Finding Out What's There: Technical and Legal Aspects of Discovery*, 4 TEX. INTELL. PROP. L.J. 57, 64 (1995). "Shadow" data refers to files that have been deleted or erased by the user, but continue to exist in the computer's memory until that file space is written over. *See id.*

communications being protected by the attorney-client privilege, the question for e-mail must be whether society is willing to recognize a reasonable expectation of privacy in e-mail communications. The answer to that question is unclear.

CONCLUSION

It is generally accepted that e-mail is revolutionizing business. The legal profession must not leave itself on the fringe of this revolution; attorneys should embrace technology in order to effectively serve their clients. However, because attorneys owe a duty of care and confidence to their clients, attorneys must exercise caution when using new technology. Until these issues are decided by the courts or by legislatures, attorneys are left with only their best judgment to guide them. In the world's most litigious society, it is not difficult to imagine a multitude of attorney malpractice cases over these issues in the meantime. Furthermore, the threat of attorney discipline for ethics violations is ever present.

The prudent attorney, therefore, has a number of choices; she can: (1) encrypt all sensitive e-mail; (2) never send sensitive communications through the Internet; or (3) make certain that the client is aware of the dangers faced with Internet communications and allow the client to give an informed consent to using the Internet. If the attorney does not take these steps, she may face professional malpractice suits and disciplinary procedures for failure to exercise reasonable care.

The benefits of e-mail are many. In addition to those benefits discussed at the beginning of this comment, like cost and time savings, e-mail has other virtues. Because of the Internet, attorneys can access their e-mail remotely, allowing them to handle their clients' needs more efficiently, effectively, and quickly than ever before.[211] Attorneys may also be able to be more productive if they are not tied to their offices and are able to "telecommute" or work from remote locations. The telecommunications revolution will not pass by attorneys. However, attorneys are different from most Internet users because they have an affirmative duty to maintain privacy in some communications.

---

211. However, this may also mean that attorneys are always "on call" for their clients which may be a bit cumbersome and interruptive. Some attorneys may not see this as a benefit at all.

Attorneys must recognize this difference. Because of this ethical duty, attorneys simply may have to use another communication tool for *some* communications or encrypt their confidential communications. While the issues raised by Internet security should not scare attorneys away from using the Internet, a healthy fear of its potential problems is a positive quality.