Extending the Attorney-Client Privilege: Do Internet E-mail Communications Warrant a Reasonable Expectation of Privacy

Sean M. O'Brien
Suffolk University Law School

Follow this and additional works at: https://dc.suffolk.edu/jtaa-suffolk

Part of the Litigation Commons

Recommended Citation
EXTENDING THE ATTORNEY-CLIENT PRIVILEGE: DO INTERNET E-MAIL COMMUNICATIONS WARRANT A REASONABLE EXPECTATION OF PRIVACY?

“For an attorney entrusted with ethical responsibilities to preserve client confidences, what use is the speed and flexibility of e-mail if there is no reasonable assurance of confidentiality?”

I. INTRODUCTION

The communications boom of the late twentieth century produced the Internet and electronic mail (“e-mail”), enabling people to efficiently communicate on a worldwide scale. Questions about a person’s reasonable expectation of privacy in Internet e-mail communications remain unanswered. Courts have held e-mail commun-


2 See Betty Ann Olmsted, 63 DEF. COUNS. J. 523, 524 (1996) (indicating e-mail easiest and most effective way to communicate worldwide almost instantaneously). “The communication of e-mail messages through the Internet may become the standard form of communication in the future.” Donald S. Skupsky, Discovery and Destruction of E-mail, in THE INTERNET AND BUSINESS: A LAWYER’S GUIDE TO THE EMERGING LEGAL ISSUES 59 (Joseph F. Ruh, Jr. ed., 1996). According to a 1997 American Bar Association Law Firm Technology Survey, “91 percent of firms with more than 20 lawyers and 44 percent of firms with 20 or fewer lawyers are already using the Internet to communicate with clients.” Stuart J. Chanen, ‘Return to Sender’ Won’t Cut It, ABA J. 84 (March 1998).

3 Internet e-mail communication travels through the sender’s and recipient’s servers and through intermediate providers. See Skupsky, supra note 2, at 49 (discussing Internet e-mail messages being recorded on recipients, senders, and intermediate systems). Private networks and direct computer communications do not require intermediate providers. See id. (explaining private e-mail services enable sender’s and receiver’s to utilize single network without intermediary computers).

Communications sent through private and closed computer networks warrant a reasonable expectation of privacy and are subject to the attorney-client privilege. In contrast, courts have not yet determined if Internet e-mail communications are subject to the attorney-client privilege. This note, therefore, will focus on the applicability of the attorney-client privilege to e-mail communications over the Internet.

(observing lawyer's use of e-mail raises privilege issues not resolved by courts and bar associations). The attorney-client privilege only applies to communications that afford a reasonable expectation of privacy. See generally Katz v. United States, 389 U.S. 347 (1967) (stating landline telephone communications afford reasonable expectation of privacy within Fourth Amendment); Askin v. McNulty, 47 F.3d 100 (4th Cir. 1995) (finding radio portion of cordless phone communication not afforded privacy expectation under the Fourth Amendment); United States Fidelity and Guar. Co. v. Canady, 194 W. Va. 431, 460 S.E.2d 677 (1995) (holding facsimile communications are privileged). A reasonable expectation of privacy is derived from Fourth Amendment protections prohibiting unlawful searches and seizures. See Katz, 389 U.S. at 351 (noting Fourth Amendment protects people's privacy, not places).

5 See National Employment Serv. Corp. v. Liberty Mut. Ins. Corp., No. 93-2528-G, 1994 WL 878920, at *3 (Mass. Super. Ct. Dec. 12, 1994) (holding e-mail communications over private network between corporate in-house counsel and employees of same corporation subject to attorney-client privilege to extent communication sought legal advice or anticipated litigation); see also United States v. Maxwell, 45 M.J. 406 (U.S.A.F. 1996) (finding private, internal network e-mail communication possess reasonable expectation of privacy). In Maxwell the court, in determining the validity of a search warrant, distinguished the America Online e-mail system at issue from Internet e-mail communications. See id. at 417 (observing Internet has less secure e-mail system than America Online's private e-mail network).

6 See Arthur L. Smith, E-Mail and the Attorney-Client Privilege (visited July 12, 1998) <http://www.computerbar.org/netethics/asmith.htm>, (stating few court decisions have held e-mail communications are protected by attorney-client privilege but no case focused on Internet e-mail); Harry M. Gruber, Note, E-Mail: The Attorney-Client Privilege Applied, 66 GEO. WASH. L. REV. 624, 625 (1998) (observing no court has held attorney-client privilege does not apply to e-mail communications); Lucy Schlauch Leonard, Comment, The High-Tech Legal
Part I of this note traces the history and policy of the attorney-client privilege, briefly discussing varied interpretations of the privilege at both federal and state court levels. Part II examines communication mediums such as landline telephones, cordless telephones, cellular telephones, direct computer to computer networks and private computer networks, noting the availability of the attorney-client privilege to some of these mediums. Part III discusses e-mail over the Internet, specifically analyzing the inherent security risks that endanger a reasonable expectation of privacy. Part IV focuses on the application of the attorney-client privilege to Internet e-mail communications, finding relevant analogies between Internet e-mail and other modes of communication presently protected under the privilege. This note concludes that courts and legislatures will determine that the attorney-client privilege is flexible enough to encompass Internet e-mail communications.

II. HISTORY AND POLICY OF THE ATTORNEY-CLIENT PRIVILEGE

Federal and state rules of civil procedure make any matter that is relevant and unprivileged discoverable. The attorney-client privi-

Practice: Attorney-Client Communications and the Internet, 69 U. COLO. L. REV. 851, 853 (1998) (offering Internet e-mail represents wild card untested in law presenting unknowable consequences).

7 See infra notes 12-33 and accompanying text (discussing attorney-client privilege history and policy).

8 See infra notes 34-82 and accompanying text (tracing application of attorney-client privilege to various communication mediums).

9 See infra notes 83-108 and accompanying text (analyzing security risk involved in Internet e-mail).

10 See infra notes 109-143 and accompanying text (analogizing application of attorney-client privilege as applied to various communication modes to Internet e-mail).

11 See infra note 144 and accompanying text (concluding Internet e-mail protected under attorney-client privilege in future).

12 FED. R. CIV. P. 26(b)(1) provides: Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking
lege limits discoverable matters by protecting the client from the mandatory disclosure of otherwise discoverable communications. The privilege only applies to communications between the attorney and client that are intended to be confidential. The attorney-client privilege is an exception to the general rule that a witness has a duty to testify. Neither the client nor the attorney on behalf of the client must testify to the contents of a privileged communication. A client holds the privilege, and may refuse to disclose, and prevent any discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition, and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. The information sought need not be admissible if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.

Id. MASS. R. CIV. P. 26(b)(1) states in pertinent part:

Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action. It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.

Id.


14 See In re Colton, 201 F. Supp. 13, 17 (1961) (opining privilege only applies to communications from lawyer to client giving legal advice or client to attorney if confidentiality intended).


16 Federal and state rules of evidence pertaining to discovery provide for privileged communications between an attorney and client. See generally FED. R. CIV. P. 26(b)(1); MASS. R. CIV. P. 26(b)(1).
other person from disclosing, confidential communications made between the client and the lawyer. The privilege must be expressly raised and asserted in a timely fashion in connection with a specific confidential communication. The attorney-client privilege serves as a testimonial and discovery shield for communications not otherwise privileged.

The attorney-client privilege may generally be claimed if the following elements are present: "(1) where legal advice of any kind is sought, (2) from a legal advisor in his capacity as such, (3) the communication relating to that purpose, (4) made in confidence, (5) by the client, (6) are at his instance permanently protected, (7) from the disclosure by himself or his lawyer, (8) except the privilege be waived." The party seeking to assert the attorney-client privilege


18 See Feagan, supra note 13, at 759.

19 FED. R. EVID. 501 provides:

Except as otherwise required by the Constitution of the United States or provided by Act of Congress or in rules prescribed by the Supreme Court pursuant to statutory authority, the privilege of a witness, person, government, State, or political subdivision shall be governed by the principles of common law as they may be interpreted by the courts of the United States in the light of reason and experience.

Id. MASS. GEN. L. ch. 233, § 20 provides in pertinent part: "Any person of sufficient understanding, although a party, may testify in any proceeding, civil or criminal, in court or before a person who has authority to receive evidence...."

Id.

20 8 JOHN H. WIGMORE, WIGMORE ON EVIDENCE § 2292 (McNaughton rev. ed. 1961). In United States v. Wilson, the First Circuit held the following four elements must be shown by the person seeking to claim the privilege:
has the burden to show the communication should be afforded the privilege. The privilege may be waived if confidential communications are purposefully or inadvertently disclosed to a third party, or will knowingly be disclosed to a third party in the future. The privilege only extends to communications intended to remain confidential that are made under circumstances where a reasonable expectation of privacy exists. A communication made in circum-

_ the person sought to a client of the counsel; (2) that counsel was acting as a lawyer in connection with the matter at issue; (3) the matter to which the privilege is asserted relates to the facts communicated for the purpose of securing legal opinion, legal services or assists in a legal proceeding; (4) the privilege has not been waived._

798 F.2d 509, 512 (1st Cir. 1986).


22 See United States v. Gann, 732 F.2d 714, 723 (9th Cir. 1984) (finding defendants attorney-client privilege claim fails because third party present). In United States v. Keystone Sanitation Co., the court stated:

_Many courts consider the following factors to determine if an inadvertent disclosure loses its privilege: the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of document production, the number of inadvertent disclosures, the extent of the disclosure, any delay and measure taken to rectify the disclosure, whether the overriding interests of justice would or would not be served by relieving the party of error._


23 See United States v. Blasco, 702 F.2d 1315, 1329 (11th Cir. 1983) (stating privilege exists if communication intended to remain confidential and made under circumstances were confidentiality reasonably expected and understood). Communications made in the presence of third parties may not be reasonably expected or intended to remain confidential. _Id.; see also Reorganization_, 425 Mass. at 422, 681 N.E. at 841 (explaining modern trend that privilege not lost when both attorney and client take reasonable precautions to ensure _
stances where there is a reasonable expectation of privacy, however, may be subject to waiver of the privilege despite intentions to maintain confidentiality if the communication is not kept confidential.24

Of the now existing common law communication privileges, the attorney-client privilege is the oldest.25 The Supreme Court of the United States first recognized the privilege in 1888.26 Every state recognizes some form of the attorney-client privilege either by way of statute, common law, or rules of evidence.27 Most states have incorporated the attorney-client privilege into their evidence code and confidentiality); cf. id. at 422, 681 N.E. at 841 (citing Wigmore recognized privilege survives when attorney acts in bad faith toward client and discloses communications).


27 See Ford Motor Company v. Leggat, 38 Tex. Sup. Ct. J. 920, 924, 904 S.W.2d. 643, 647 (1995) (opining one state may offer broader attorney-client privilege than another state). Most jurisdictions have codified the common law privilege by statute, offering the same protection common law offered. See Matthews, supra note 15, at 280 (quoting 8 JOHN H. WIGMORE, WIGMORE ON EVIDENCE § 2290, at 555-56 (McNaughton rev. ed. 1961)).
at least twenty state legislatures have codified the privilege.\textsuperscript{28} Under federal law, the attorney-client privilege exists by way of the Federal Rules of Evidence.\textsuperscript{29}

The purpose of the privilege is to encourage and facilitate the unrestricted flow of information between attorney and client, promoting "broader public interests in the observance of law and the administration of justice."\textsuperscript{30} Scholars justify the modern attorney-client privilege with a utilitarian analysis, believing a lawyer most effectively serves a client if the client can fully disclose information to the attorney without the fear of discovery.\textsuperscript{31} Opponents of the attorney-client privilege argue that it may impede investigation of truth and must narrowly be interpreted.\textsuperscript{32} Courts, consequently,


\textsuperscript{29} See FED. R. EVID. 501 (providing for privilege of person or witness).

\textsuperscript{30} Upjohn, 449 U.S. at 389. Individuals may seek legal representation with the knowledge that they can discuss matters openly with an attorney because the privilege often protects such communications from compelled disclosure. \textit{See id.} at 383 (explaining sound legal advice depends upon lawyer being fully informed by client). The privilege is based on the need for the lawyer to know everything relating to the client’s reasons for seeking representation if the lawyer’s professional duties are to be successfully carried out. \textit{See} Trammel v. United States, 445 U.S. 40, 51 (1980).

\textsuperscript{31} See WRIGHT, supra note 25, at § 5472 (suggesting social good derived from proper performance of function of lawyers acting for clients outweighs harm from suppression of evidence). Traditionally, the lawyer held the privilege based upon the reasoning lawyers should not violate "his obligation as a gentleman to keep secret a matter told him in confidence." \textit{Id.}

\textsuperscript{32} See United States v. Nixon, 481 U.S. 683, 710 (1974) (cautioning privilege impedes grand jury’s truth-seeking function and therefore not expansively construed); \textit{see also} Note, \textit{Developments in the Law-Privileged Communications}, 98 Harv. L. Rev. 1454, 1454 (1985) (acknowledging attorney-client privilege hinders legal system’s truth seeking objective, instead favoring other societal interests). The privilege arguably only suppresses evidence of what a client said to the attorney, therefore only impeding the use of impeachment testimony. \textit{See} WRIGHT, supra note 25, at § 5472 (stating proponents of privilege
weigh the need for full disclosure against the need for full and frank communication between an attorney and client.\textsuperscript{33}

III. MODERN COMMUNICATIONS AND PRIVILEGE

A. Landline Telephones

In \textit{Katz v. United States},\textsuperscript{34} the Supreme Court of the United States held the Fourth Amendment of the United States Constitution protects landline telephone conversations from unreasonable search and seizure.\textsuperscript{35} Landline telephone conversations are subject to constitutional protections resulting from an individual's reasonable expectation of privacy when using this medium.\textsuperscript{36} Consequently, the attorney-client privilege is applicable to landline telephone conver-

believe costs are minimal). \textit{But see id.} at § 5472 (asserting opponent's believe privilege conceals reality consequently cloaking much client and lawyer wrongdoing).

\textsuperscript{33} See Feagan, \textit{supra} note 13, at 760 (opining courts balance need for full disclosure and desirability of encouraging communication).

\textsuperscript{34} 389 U.S. 347 (1967).

\textsuperscript{35} \textit{See id.} at 353 (holding Government's activities in electronically listening to landline telephone conversation violated reasonably relied upon privacy expectations and constituted search and seizure). U.S. CONST. amend. IV provides:

\begin{quote}
The right of the people to be secure in the persons, houses, papers, and effects, against unreasonable searches and seizures, and no Warrants shall issue, but upon probable cause, supported by an Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.
\end{quote}


sations because a reasonable expectation of privacy exists with regard to this form of communication. The reasonable expectation of privacy need not be an absolute guarantee for the attorney-client privilege to extend to a landline communication.

Aside from constitutional and common law protections for landline telephone calls, there are federal and state statutory prohibitions against interception and unauthorized use of such calls. Under the federal Electronic Communications Privacy Act, a client does not waive the attorney-client privilege if a landline communication is intercepted. Landline telephone calls intercepted in violation of federal law may not be used as evidence in any American proceeding. Similarly, the Massachusetts Eavesdropping Act provides in pertinent part:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of

---

37 See United States v. Alter, 482 F.2d 1016, 1026-27 (9th Cir. 1973) (finding establishment of prima facie evidence of improper electronic surveillance of telephone calls is required to preserve privileged matter); see also Jarvis, supra note 36, at 471 (declaring no one would doubt attorney-client privilege applies to landline telephone conversations).

38 See Jarvis, supra note 36, at 472 (stating landline calls not usually intercepted but such occurrences do not destroy individual's expectation of privacy).


40 18 U.S.C. § 2517(4) (1994) provides in pertinent part: "No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provision of this chapter shall lose its privileged character." Id.

41 Id.

hibits the use of wire or oral communications in a criminal trial if obtained in violation of state law.\textsuperscript{44} Intercepted wire communications, including landline telephone calls, will not lose any privilege under Massachusetts law.\textsuperscript{45} At federal and state levels, landline communications are afforded strong legal prohibitions and constitutional protections, justifying a reasonable expectation of privacy.\textsuperscript{46}

\section*{B. Cordless and Cellular Communications}

A reasonable expectation of privacy in a communication medium may be considered a condition precedent to the attachment of the attorney-client privilege.\textsuperscript{47} Several jurisdictions have found that cordless and cellular communications do not offer a reasonable expectation of privacy.\textsuperscript{48} In addition, ethic's opinions have asserted

\begin{quote}
the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.
\end{quote}

\textit{Id.}

\textsuperscript{43} \textsc{Mass. Gen. Laws} ch. 272, § 99(P) provides: “Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom...that the communication was unlawfully intercepted.” \textit{Id.}

\textsuperscript{44} \textit{Id.}


\textsuperscript{46} \textit{See} \textsc{Jarvis, supra} note 36, at 473 (suggesting reasonable expectation of confidentiality and privacy for landline calls results from statutory prohibitions); \textsc{David Hricik, Confidentiality \& Privilege in High-Tech Communications}, 60 \textsc{Tex. B.J.} 104, 107 (1997) (explaining interception and misdirection of landline communications occur but legal protections are offered).

\textsuperscript{47} \textit{See} \textsc{Nunez, supra} note 17, at 490-91 (contending confidentiality co-terminus with privacy and without privacy there is no privilege).

\textsuperscript{48} \textit{See} \textsc{Askin v. McNulty}, 47 F.3d 100, 103-04 (4th Cir. 1995) (holding radio wave portion of cordless phone communication not afforded privacy expectation under Fourth Amendment); \textsc{McKamey v. Roach}, 55 F.3d 1236, 1239-40 (6th Cir. 1995) (finding cordless telephones are broadcast over radio waves for all to hear affording no Fourth Amendment protection); \textsc{People v. Chavez}, 44 Cal. App. 4th 1144, 1153, 52 Cal. Rptr. 2d 347, 353 (Ca. App. Ct. 1996) (holding radio portion of cordless telephone call did not encompass expectation of privacy); \textit{see...
that the attorney-client privilege does not protect cordless or cellular communications.\textsuperscript{49} These judicial decisions and ethic’s opinions, many of which pre-date the 1994 amendments to the federal statutes, reflect a general belief that cordless and cellular technologies do not provide the requisite reasonable expectation of privacy necessary to extend the attorney-client privilege.\textsuperscript{50}

Cordless telephone communications are a hybrid between FM radio frequencies with radio range and the traditional landline telephone.\textsuperscript{51} While the landline portion of a cordless telephone call is deemed to provide a reasonable expectation of privacy, the radio segment of the call has no such expectation attached.\textsuperscript{52} “Cordless


\textsuperscript{50} 18 U.S.C. § 2510, 1994 Amendment struck out “provision which excluded radio portion of a cordless telephone communication that is transmitted between handset and base unit from the definition of electronic communication.” \textit{Id.}

\textsuperscript{51} \textit{See} Lapidus, \textit{supra} note 4, at 39 (explaining FM radio frequency portion of cordless telephones similar to operating radio station and broadcasting your message). Once the cordless telephone communication is being carried through the landline, statute and expectations inherent in landline communications control the call. \textit{See} Hricik, \textit{supra} note 46, at 108 (opining landline segment of cordless phone call has reasonable expectation of privacy).

\textsuperscript{52} \textit{See generally} \textit{supra} note 51-55 and accompanying text (discussing radio portion of cordless telephone call).
phone calls are only rarely intercepted or interrupted.”

Some courts, acknowledging the steady growth of technology, have protected the radio portion of cordless communications under state law and the Fourth Amendment. The majority of courts, however, hold the radio portion of cordless telephone communications do not offer a reasonable expectation of privacy.

Cellular telephone communications, similar to cordless communications, were considered “ordinary radio waves wandering along public airwaves, not subject to legal protection from interception.” In fact, cellular communications are broadcast within a range of frequency not susceptible to inadvertent interception (unlike cordless communications) absent specially adapted scanners. Cellular

53 Jarvis, supra note 36, at 476. Regardless of the frequency that cordless telephone calls are intercepted or interrupted, two things are true: “cordless telephone calls may be intercepted by someone nearby using a police scanner, radio, baby monitor, or another cordless phone, and pre-1994, cordless calls were not afforded the statutory protection landline and cellular communications were under federal law.” Id. But see Hricik, supra note 46, at 108 (stating inadvertent disclosures occurred frequently with cordless phones).

54 See United States v. Smith, 978 F.2d 171, 177-78 (5th Cir. 1992) (finding advancing technology in cordless telephone communications adequately creates reasonable expectation of privacy under Fourth Amendment). The Smith court held that Fourth Amendment protection of cordless communications depends upon the technology used in each instance. Id. See State v. McVeigh, 224 Conn. 593, 623, 620 A.2d. 133, 148 (1993) (upholding state law prohibiting unlawful interception of cordless communications). But see Askin v. McNulty, 47 F.3d 100, 104-05 (4th Cir. 1995) (commenting legislature proper forum for evaluating new technology and its impact on privacy rights).

55 See supra notes 51-55 and accompanying text (discussing expectation of privacy for radio portion of cordless communications).

56 See Nunez, supra note 17, at 484 (observing state of cellular communications prior to Federal Communications Commission allotting fixed ranges of frequencies).

57 See Lapidus, supra note 4, at 39 (characterizing frequencies used in cellular communications). Unlike cordless phones, cellular phones may not be intercepted by readily available consumer products. See Hricik, supra note 46, at 109. Cellular telephone calls “are rarely intercepted or conflated with the calls
communication is within the definition of 18 U.S.C. § 2510 (1), prohibiting unauthorized interception or use while providing for all privileges. Intentionally intercepted cellular or cordless communications may not be introduced into evidence regardless if a claim of privilege is available. Federal and state prohibitions against the intentional interception of cellular communications has not made such interceptions technologically more difficult. In consideration of the 1994 Amendments to the federal statute and advances in cellular technology, cellular communications provide a reasonable expectation of privacy sufficient to sustain the attorney-client privilege and Fourth Amendment protection.

C. Direct Computer Communications and Private Networks

The expectation of privacy in direct computer to computer and private network computer communications rivals that of landline telephone calls. The fact communications in the form of digital "bits and bytes rather than by [human] voice" are transmitted via land-based telephone lines should not affect the attorney-client privilege's availability. Consequently, all constitutional and statutory protections, prohibitions, and privileges available to land-

---


59 Jarvis, supra note 36, at 477.

60 See id. at 477 (opining criminal and civil prohibitions against intentional interceptions have not made interceptions more challenging). Cellular pirates and scanners purchased prior to 1993 may intercept cellular communications, although such a practice is illegal. See Hricik, supra note 46, at 108 (indicating scanners used to intercept cellular communications are illegal to sell in United States).

61 See Jarvis, supra note 36, at 476 (asserting cellular calls have same protections as landline calls).

62 See id. at 478 (indicating direct communications occurring by computer over land-based lines has same protections as traditional telephone calls).

63 Id. at 478; see also Hricik, supra note 46, at 110.
line communications are applicable to private network computer communications. 64

Facsimile transmissions ("faxes") are considered direct computer to computer communications, sending digital signals over traditional land-based telephone lines. 65 Faxes are subject to Fourth Amendment protections and the attorney-client privilege. 66 Despite possible misdirection or interception of a fax transmission, a reasonable expectation of privacy is still afforded this medium. 67 Misdirected fax transmissions may be at risk of losing their privilege, but a fax properly directed is subject to the claim of privilege. 68 Fax transmissions and other direct computer to computer communications over land-based lines maintain their privileged character if properly directed. 69

There are generally two forms of private network computer communications. First, commercial on-line services such as Amer-

64 See supra notes 34-46 and accompanying text (providing analysis and discussion of landline telephone communications).

65 See Hricik, supra note 46, at 110 (characterizing faxes as electronic, computer-to-computer digital communication).

66 See United States Fidelity and Trust Co. v. Canady, 194 W. Va. 431, 441-42, 460 S.E.2d 677, 687-88 (1995) (holding fax communication as privileged); see also Jarvis, supra note 36, at 478 (stating no one doubts faxes subject to attorney-client privilege); Hricik, supra note 46, at 110 (finding faxes subject to attorney-client privilege).

67 Suppose a fax is properly directed and received by a fax machine in an attorney's office. The fax sent may contain information of a privileged nature. The fax sits in the tray of the machine for hours, subject to the eyes of anyone working in the office, housekeeping crews, and a steady influx of clients. Although the fax, in this particular situation, may not be private, courts tend to find a properly directed fax maintains its privilege. Note, however, that ethic opinions have addressed a lawyer's duty upon receiving a misdirected fax. See 6 PROF. LAW. 26, 26 (1994) (quoting ABA Standing Committee on Ethics and Professional Responsibility Opinion 94-382).

68 See Jarvis, supra note 36, at 478 (commenting facsimile transmission are privileged electronic communications).

69 See generally Canady, 194 W. Va. 431, 460 S.E.2d 677 (holding fax transmissions protected under attorney-client privilege).
ica Online, CompuServe, and Prodigy provide users with e-mail access that is insulated from the Internet. While many on-line services provide gateways to the Internet, e-mail communications within a private network do not require Internet access. Second, internally accessed private networks allow e-mail computer communications that are often closed to external landlines. Internally accessed private networks are commonly found in corporations or law firms and allow attorneys to communicate with clients or other attorneys within the network.

Electronic communications via private computer networks constitute wire communications within the meaning of the federal statute. Courts have held communications over private networks are

---

70 See Karen L. Casser, Employers, Employees, E-Mail and the Internet, in THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO EMERGING LEGAL ISSUES, at 4 (Joseph F. Ruh, Jr. ed. 1996) (explaining commercial on-line services do not access Internet except when directing e-mail outside network). "[A]n e-mail message sent from the user with a CompuServe account to a user with an America Online account will travel over the Internet, but the users may not even be aware the Internet is involved." Id. at 4 n.9.

71 See Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2334 (1997) (characterizing America Online, CompuServe, and Prodigy as online services with gateways to Internet).

72 See Skupsky, supra note 2, at 49 (explaining sender posts e-mail message on private service and recipient receives it on same service). The posted e-mail message is recorded only on the host e-mail file server. See id. (noting no copies recorded on sender or recipient desktop).

73 See Hricik, supra note 46, at 110 (defining closed, private network). Private network communications, such as a corporate internal e-mail system, occur entirely over land-based telephone lines, often without access to external land-based telephone lines. See id. (discussing closed, private networks commonly used in corporations and law firms).

74 See supra note 73 and accompanying text (observing private networks do not require gateways to Internet).

subject to the attorney-client privilege. In *United States v. Maxwell*, the Military Court of Appeals held that an expectation of privacy exists in e-mail transmissions sent via America Online service. The *Maxwell* court found interception of e-mail by a hacker does not diminish one's expectation of privacy. America Online is considered a large semi-public host acting as a gateway to the Internet and Internet e-mail. The *Maxwell* decision should be narrowly construed as applying the attorney-client privilege to e-mail on private

---


78 See id. at 420 (finding Fourth Amendment protects transmitters of e-mail). Expectations of privacy in e-mail transmissions depend in large part on the type of e-mail involved and the intended recipient. Id. at 419. Messages sent to the public at large in the "chat room" or e-mail that is "forwarded" from correspondent to correspondent loses any semblance of privacy. Id. The court recognized the difference between a network e-mail communication such as America Online and a direct computer "real time" communication. Id. The America Online communication is stored in a centralized computer until the recipient opens the network and retrieves the mail whereas a direct communications are lost forever unless it is downloaded to disk. *Maxwell*, 45 M.J. at 418. America Online, however, offered contractual privacy protection that provided employees would not read or disclose subscribers' e-mail to anyone except authorized users. See id. at 417 (stating expectation of privacy depends upon type of e-mail and America Online e-mail provides such expectations).

79 See id. at 418.

80 See supra note 70-72 and accompanying text (discussing *Reno* and America Online). America Online allows users to communicate with other America Online subscribers on its own internal e-mail network. *Maxwell*, 45 M.J. at 410. "It is also possible to access other computer users outside the America Online computer subscription service...." Id.
computer networks.\textsuperscript{81} Other federal and state courts have declined to extend e-mail protections under the Fourth Amendment based on a perceived lack of confidentiality and privacy.\textsuperscript{82}

IV. INTERNET E-MAIL

A. E-mail Communication

Electronic mail ("e-mail") is an electronic medium, allowing computer users to communicate via digital signals with other user's internal or external to an organization's network of computers.\textsuperscript{83} E-mail occurs immediately, sending a message referred to as "mail" from the sender to the recipient's mailbox.\textsuperscript{84} Senders and recipients have mailboxes with distinguishing characteristics, which facilitate proper delivery of the mail.\textsuperscript{85} E-mail, as distinguished from traditional landline, cellular, and cordless calls, is an inconsonant form of communication, requiring senders and recipients to read and compose messages individually at different points in time.\textsuperscript{86} E-mail of-

\textsuperscript{81} But cf. supra note 66 and accompanying text (discussing attorney-client privilege and Fourth Amendment protections applied to direct computer communications).

\textsuperscript{82} See Matthews, supra note 15, at 292 (asserting both state and federal statutes afford no reasonable expectation of privacy to e-mail).

\textsuperscript{83} See Olmsted, supra note 2, at 523 (explaining fundamental function of e-mail). E-mail is one of the fastest growing branches of digital technology. \textit{Id.} It is estimated 40 million e-mail users will be sending some 60 billion messages by the year 2000. See John M. McKelway et. al., \textit{Law in Cyberspace: To the Internet and Beyond 1}, MASS. LAW. WKLY. 11 (April 1996).

\textsuperscript{84} See Matthews, supra note 15, at 274 (noting e-mail arrives within minutes of being sent).

\textsuperscript{85} See \textit{id.} (stating users have unique e-mail addresses to send and receive messages).

\textsuperscript{86} See Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2335 (1997) (observing e-mail messages sent are stored waiting for recipient to check mailbox).
fers a mode of communication on a worldwide basis that is cost effective, convenient, and efficient.\textsuperscript{87}

\section*{B. Internet E-mail and Security Risks}

The Internet originated out of an experimental project conducted by the Department of Defense in 1969.\textsuperscript{88} "The Internet enables tens of millions of people to communicate and access vast amounts of information from around the world."\textsuperscript{89} Serving as a premiere global network, the Internet is an aggregation of networks forming a single network.\textsuperscript{90} The Internet is accessible through several different sources, generally through hosts themselves, or through entities with host affiliation.\textsuperscript{91} Hosts serve as the gateway to the Internet.\textsuperscript{92}

\textsuperscript{87} See Robert L. Jones, \textit{Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail} (visited July 12, 1998) <http://www.computerbar.org/net ethics/bjones.htm> (discussing advantages of electronic communications versus paper-based communication). "Electronic messages move at the speed of light while paper moves at the speed of the United States Postal Service." \textit{Id.} Electronic messages save space, money, and are more rapidly and accurately accessible than paper documents. \textit{See id.} (maintaining cost of electronic messages is only fraction of cost of paper-based communication).

\textsuperscript{88} See Hricik, \textit{supra} note 46, at 112. The Internet is the product of a military program called ARPNET (Advanced Research Project Agency Network), created to make possible computers operated by the "military, defense contractors, and universities defense-related research" to communicate by redundant channels even if portions of the network are damaged by war. \textit{Reno,} 117 S. Ct. at 2334. "The Internet, originally intended as a fail-safe communications network in time of nuclear disaster, was designed more with ease of networked communications in mind than messaging security." \textit{Merrill, supra} note 1, at 14.

\textsuperscript{89} \textit{Id.}

\textsuperscript{90} See Matthews, \textit{supra} note 15, at 276 (characterizing Internet as single giant world-wide network). The Internet is decentralized in nature, creating a worldwide network that is owned by no one. \textit{See id.} at 277 (referring to Internet as "no man's land"). An estimated 200 million people are expected to have used the Internet by 1999. \textit{See Reno,} 117 S. Ct. at 2334 (finding 40 million people used Internet by March 1997).

\textsuperscript{91} \textit{See Reno,} 117 S. Ct. at 2334 (describing how an individual gains Internet access). Major online services, such as America Online, CompuServe, the
The Internet serves as the foundation upon which the global e-mail network operates. Unlike e-mail sent in a direct computer communication, Internet e-mail travels from the sender's computer through a land-based line to several intermediate computers, called hosts and routers that are owned by third parties, before reaching the recipient's mailbox. Routers aid the sender's and receiver's hosts in distributing Internet e-mail. E-mail messages, therefore, often pass through several intermediate computers owned and operated by miscellaneous public and private entities before actually reaching the recipient's mailbox. The consequence of hosts and routers is generally fast and efficient computer communication. However, legitimate privacy concerns exist in the legal community because hosts and routers that receive e-mail messages create opportunities for interception, misdirection and disclosure.

Microsoft Network, and Prodigy offer access to the Internet as semi-public hosts. See id. at 2334 (estimating 12 million individual subscribers to commercial online services in 1997). Phone lines and exchanges throughout the world connect the Internet. Lapidus, supra note 4, at 39.

See Hricik, supra note 46, at 112 (observing there are several million host computers). Each host computer has a unique Internet address for sending and receiving e-mail to the subscribers of that host. Id.

See Matthews, supra note 15, at 276 (observing Internet is world's largest computer network).

See Hricik, supra note 46, at 112. (commenting e-mail sent in direct computer communication goes directly from sender's computer to password protected mailbox of recipient).

See id. (discussing how Internet e-mail travels from senders host, to router, then to recipient's host). Routing e-mail through the Internet is accomplished by directing e-mail on the most direct course from the sender to the receiver, effectively avoiding any problems that may arise. See Matthews, supra note 15, at 278 (stating routers find closest routers to direct their e-mail).

See Hricik, supra note 46, at 114 (noting Internet e-mail messages may go through a dozen or more intermediate computers); Lapidus, supra note 4, at 39 (explaining Internet e-mail may pass over dozens of intermediate computers owned by disparate public and private entities).

Internet e-mail messages are susceptible to interception when stored in intermediate computers. See Jarvis, supra note 36, at 479-80 (tracing path of
When an Internet user sends someone e-mail, the original e-mail is not sent to the hosts or routers. 98 "A copy of the original e-mail is sent and the original is stored on the user's computer." 99 In fact, "every time the e-mail passes through a host or router, another copy is made." 100 The host or router, who may lawfully use or disclose the e-mail sent through the system "to the extent necessary to render the service or protect its rights," may intercept the copies. 101 Any employee of the router or host can monitor e-mail transmissions that are otherwise confidential. 102

E-mail communications are vulnerable to various other security risks that jeopardize privacy on the Internet. 103 Hackers utilize pro-

---

98 See Olmsted, supra note 2, at 524 (illustrating how e-mail messages created and stored).
99 Id.
100 Id. E-mail may exist long after one party deletes the message because it is only removed from their computer system, and then only when the computer needs the available space. See Charles A. Lovell, Danger's of E-mail Underline Need for Policies, MASS. LAW. WKLY. B4 (April 1996) (describing e-mail user's perception of e-mail as ephemeral); see also Charles A. Lovell & Roger W. Holmes, The Dangers of E-mail: The Need for Electronic Data Retention Policies, R.I. B.J. 7, 7 (Dec. 1995) (describing plaintiffs' attorneys as "smoking gun" evidence that is discoverable resulting from e-mail communications). Deletion of e-mail is a formidable task because of storage and copies of messages that are routinely saved. See Aaron Grossman, Is Opposing Counsel Reading Your E-mail?, MASS. LAW. WKLY. B4 (Nov. 1996) (stating e-mail may be harder to get rid of than nuclear waste because of intermediate computers back-up system).
101 Hricik, supra note 46, at 114.
102 See id. (stating Internet e-mail is subject to review by host and router employees as part of ordinary monitoring or maintenance).
103 On-line networks use firewalls, specialized gateway computers that insulate the inside network from the outside world, but hackers are still able to
grams called "sniffers" to search for key words in unencrypted e-mail as it travels through hosts and routers. Hackers also use another type of program called "spoofing." Spoofers configure an intermediate computer to resemble the recipient host, effectively intercepting the e-mail message. While interception of e-mail by sniffers or spoofing is a felony, sniffing and spoofing are still very real risks to confidentiality and privacy.

V. ANALYSIS: INTERNET E-MAIL AND THE ATTORNEY-CLIENT PRIVILEGE

The attorney-client privilege may not currently protect Internet e-mail communications because the medium is commonly perceived to lack privacy. Commentators and ethics advisory committees corrupt the network. See Merrill, supra note 1, at 15 (discussing sophisticated security precautions that are susceptible to hackers).

Encryption is electronic "lock and key" technology. Id. Encryption "scrambles a message so that...the messages are unreadable to anyone except the intended recipient of the message." Lapidus, supra note 4, at 40.

See Grossman, supra note 100, at B4 (explaining sniffers search for sender's or recipient's address, then store information on hacker's computer). Sniffers access information that is received by hosts and routers. See Hricik, supra note 46, at 115 (stating sniffers capture information on intermediate computers using software to detect unencrypted e-mail messages).

See Grossman, supra note 100, at B4 (observing that spoofers intercept e-mail messages and can alter or destroy message).

See Hricik, supra note 46, at 115 (explaining spoofer intercepts recipients e-mail sending message back to sender stating message received). Unlike sniffers, the intended recipient never receives the spoofed message. Id.


See J.T. Westermeier et. al., Ethical Issues on the Internet and World Wide Web, COMPUTER LAW. 8, 11 (Mar. 1997) (indicating concern over
have reached disparate conclusions when addressing the applicability of the attorney-client privilege to Internet e-mail. Civil and criminal cases have dealt with the application of the privilege in e-mail communications sent through private and closed computer networks. Courts have yet to address the application of the attorney-client privilege to Internet e-mail communications. Internet e-mail communications are commonly perceived to be more susceptible to interception than privileged communication mediums such as landline telephone, cellular telephone, direct computer to computer and private computer networks. Potential interception by hackers or employee monitoring is the principal reason for doubting the exten-

insufficient security in Internet e-mail may fail to protect privilege); Jarvis, supra note 36, at 479 (stating privilege unclear for Internet e-mail communications because of greater interception risk).

“Contemporary ethics committees and commentators opine that because federal law now makes it a crime to intercept...e-mail, the interception of such should not result in a waiver of the attorney-client privilege.” Lapidus, supra note 4, at 40. Other commentators believe the answer to the privilege issue is dependent on whether the disclosure is intentional or inadvertent. See id. (explaining inadvertent disclosures do not destroy privilege). But see Iowa Supreme Court Board of Professional Ethics and Conduct, Formal Op. 96-1 (May 16, 1996) (requiring encryption for e-mail message to avoid ethical violation); South Carolina Ethics Advisory Committee, Ethics Advisory Op. 94-27, 11 LAW. MAN. PROF. CONDUCT 67 (1995) (finding ethical violation committed by attorney unless electronic communication guaranteed confidentiality in e-mail communication); North Carolina State Bar, Published Op. 215 (1995) (concluding precautions required when utilizing e-mail to protect client confidentiality).

See infra notes 75-82 and accompanying text (finding in National Employment and Maxwell that private network computers afforded attorney-client privilege).

See Lapidus, supra note 4, at 39 (observing no cases could be located for the article that discussed whether unauthorized interception of e-mail constitutes a waiver of the attorney-client privilege). For the purposes of this note, no cases could be located that discussed the application of the attorney-client privilege to Internet e-mail.

See supra notes 34-108 and accompanying text (discussing various modes of communication, privacy concerns and attorney-client privilege).
sion of the attorney-client privilege to Internet e-mail.\textsuperscript{114}

Intentional interception of Internet e-mail is a crime.\textsuperscript{115} The Electronic Communications Privacy Act protects privacy interests in Internet e-mail.\textsuperscript{116} Direct computer to computer communication is within the meaning of “electronic communication” under federal statute.\textsuperscript{117} Routers and hosts utilized during an Internet e-mail transmissions are protected pursuant 18 U.S.C. §§ 2510, 2701, and 2702.\textsuperscript{118} Internet e-mail communications intercepted in violation of

\textsuperscript{114} See Matthews, supra note 15, at 285 (stating focus of doubts surrounding Internet e-mail and privilege center around perceived lack of confidentiality).

\textsuperscript{115} See 18 U.S.C. § 2701(a) (1994) (stating intentional interception of Internet e-mail from intermediate computer is a felony); 18 U.S.C. § 2702(a) (1994) (stating provider of electronic communication service that discloses communication commits a felony).

\textsuperscript{116} See Matthews, supra note 15, at 288 (asserting statutory framework of federal statutes supports objective expectation of privacy with e-mail).

\textsuperscript{117} Title 18 of the United States Code provides: “‘electronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce....” 18 U.S.C. § 2510(12) (1994).

\textsuperscript{118} Section 2510 provides in pertinent part:

(14) “electronic communication system” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

(15) “electronic communication service” means any service which provides to users thereof the ability to send or receive wire or electronic communications.

18 U.S.C. § 2510 (1994). Section 2510(17) “electronic storage” provides: “(a)ny temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of any communication by an electronic communication service for purposes of backup protection of that communication...” 18 U.S.C. § 2510(17) (1994). Section 2701(a) provides:
federal law, similar to landline telephone, cellular telephone, direct computer to computer and private computer network communications, are inadmissible evidence in a legal proceeding.\textsuperscript{19} In addition, otherwise privileged communications intercepted in violation of federal law does not lose its privileged character.\textsuperscript{20} The federal statutory prohibition against interception of Internet e-mail communications justifies a reasonable expectation of privacy when using this

\textbf{Except as provided in subsection (c) of this section whoever—}

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

702(a) provides in pertinent part:

\textbf{Except as provided in subsection (b)—}

(1) a person or entity providing an electronic communication service to the public while its in electronic storage in such system shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and (2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service—(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and (B) solely for the purpose of providing computer storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of such communications for purposes of providing any services other than storage or computer processing.


\textsuperscript{19} See 18 U.S.C. § 2515 (1994) (stating wire or oral communications that are intercepted are inadmissible in trial, hearing, or any other proceeding).

If a court determines a user justifiably relied on the privacy of a communication medium, the attorney-client privilege attaches. Courts have held that landline telephone, direct computer to computer and private computer network communications warrant a reasonable expectation of privacy and are subject to the attorney-client privilege. Communications sent by these mediums are subject to interception, misdirection and monitoring. Internet e-mail communications have comparable security risks. These security risks should not deter a court from finding that Internet e-mail communications warrant a reasonable expectation of privacy.

---

121 See supra note 46 and accompanying text (discussing reasonable expectation of privacy justified for landline communication because of federal statutory protection).

122 See United States v. Blasco, 702 F.2d 1315, 1329 (holding communication protected if made under circumstances where reasonable expectation of privacy); Nunez, supra note 17, at 490-91 (opining expectation of privacy necessary for attorney-client privilege to exist).


124 See supra notes 34-82 and accompanying text (observing security risks in landline, direct computer and private network communications).

125 See supra notes 83-108 and accompanying text (discussing Internet e-mail and privacy risks).

126 See infra note 127 (opining Internet e-mail does not present greater security risk than communication mediums that are privileged).
Internet e-mail communications do not pose a greater risk of interception than other privileged communication mediums.\textsuperscript{127} Landline telephone communications may be intercepted by illegal wiretaps.\textsuperscript{128} Cellular communications are at risk of interception through the use of specially adapted scanners.\textsuperscript{129} Private computer network and Internet e-mail communications are vulnerable to illegal interception by hackers.\textsuperscript{130} In each instance, interception is a felony but nonetheless a very real risk.\textsuperscript{131}

Internet e-mail and landline telephone communications are susceptible to employee monitoring.\textsuperscript{132} Employees of entities owning hosts and routers may legally subject Internet e-mail to monitoring within the normal scope of business.\textsuperscript{133} Switchboard operators for landline telephone communications may legally monitor phone conversations if acting within the usual course of business.\textsuperscript{134} Employees in both situations may monitor communications and disclose

\begin{footnotes}
\footnotetext{127}{See supra notes 34-108 and accompanying text (discussing inherent security risks in communication mediums afforded attorney-client privilege and Internet e-mail communications ambiguous status).}
\footnotetext{128}{See United States v. Alter, 482 F.2d 1016 (9th Cir. 1973) (considering improper electronic surveillance of landline telephone calls and attorney-client privilege).}
\footnotetext{129}{See supra note 60 and accompanying text (explaining cellular communications are not susceptible to inadvertent interception).}
\footnotetext{130}{See United States v. Maxwell, 45 M.J. 406 (U.S.A.F. 1996) (finding interception of e-mail by hacker does not diminish privacy expectation); supra notes 105-110 (discussing Internet e-mail and hackers).}
\footnotetext{131}{See 18 U.S.C. § 2701(a) (1994) (stating intentional interception of electronic message stored in electronic storage system is a felony); 18 U.S.C. § 2702(a) (1994) (stating disclosure of electronic communication stored in or carried on a service commits a crime).}
\footnotetext{132}{See Hricik, supra note 46, at 114 (observing privilege landline telephone communications subject to switchboard operators eavesdropping).}
\footnotetext{133}{See Jarvis, supra note 36, at 480 (explaining employees may lawfully review both Internet e-mails and landline telephone communications).}
\footnotetext{134}{Id.}
\end{footnotes}
their contents to third parties. Landline telephone communications
are clearly afforded the protection of the attorney-client privilege. Employee monitoring conducted in the normal scope of business
should not diminish the reasonable expectation of privacy necessary
to sustain the application of the attorney-client privilege to Internet
e-mail communications.

The extension of the attorney-client privilege to various com-
munication mediums exemplifies the legal systems ability to adapt
rules of law to advances in technology. In 1888, the Supreme Court
of the United States recognized the attorney-client privilege to pro-
tect communications between a lawyer and client. During the
twentieth century, society experienced a communications boom that
revolutionized the way lawyers and clients communicate. In con-
sideration of new communication mediums, the legislature provided
statutory prohibitions against interception and the courts expanded
the application of the attorney-client privilege. The legislature, in
the Electronic Communications Privacy Act, made interception of
Internet e-mail a crime. This statutory prohibition against inter-
ception warrants a reasonable expectation of privacy when using

135 See Hricik, supra note 46, at 114 (finding landline telephone calls subject
to monitoring pursuant federal statute). 18 U.S.C. § 2511 provides that both
Internet e-mail and landline telephone communications are subject to monitoring
and such monitoring does not prevent a reasonable expectation of privacy for
landline communications. See id. at 115 (citing no case has held monitoring
destroys landline telephone communication privilege).

136 See supra notes 34-46 and accompanying text (finding attorney-client
privilege applicable to landline telephone communications).

137 See Hricik, supra note 46, at 114 (suggesting distinction between Internet
e-mail and landline telephone communications is routers); see also supra notes
98-102 and accompanying text (discussing routers and hosts).

privilege is that of clients).

139 See supra note 2 and accompanying text (discussing communication
advances and the Internet).

140 See supra notes 34-82 and accompanying text (observing communication
mediums protected under attorney-client privilege).

Internet e-mail. In addition to statutory protection, Internet e-mail is a reasonably safe mode of communication because messages are not commonly intercepted. A court addressing the application of the attorney-client privilege to Internet e-mail would be justified in holding that such communications are privileged.

142 See Lapidus, supra note 4, at 40 (observing modern ethics committees and commentators believe that because federal law make interception of Internet e-mail a felony, interception should not result in waiver of privilege). Because employee monitoring of Internet e-mail is the same as monitoring of landline telephone calls, and Internet e-mail is protected by federal statute, "there is no reasonable argument against privilege unless the presence of an eavesdropper is known or expected." Jarvis, supra note 36, at 480.

143 See id. (noting author's personal experience indicates majority of Internet e-mails not intercepted). Attorneys' Peter R. Jarvis and Bradley F. Tellam, in a discussion concerning the attorney-client privilege, state:

[O]ne might ask whether, as a matter of fact, the risk of interception via the Internet is empirically greater than the risk of a break-in to a private law office located in a high crime area or the risk that a lawyer will be mugged and robbed of his briefcase while waiting for a bus at night. If privilege is not destroyed by such risks (and it is not), it should not be destroyed by similar risks in the electronic form.

Id.; see also Hricik, supra note 46, at 114 (opining no greater security risk when Internet communication travels over phone lines than traditional phone calls); Lapidus, supra note 4, at 42 (stating the risk of interception of Internet e-mail is relatively low). Because Internet e-mail is generally transmitted in pieces rather that as an entire message, even if an interception occurs the communication may be unreadable. See supra note 100 (discussing transmission of e-mail in packets). But see Matthews, supra note 15, at 287-88 (asserting Internet e-mail not protected until reasonable expectation of privacy is reality); Gruber, supra note 6, at 655 (believing unprotected confidential e-mail sent via Internet should eliminate privilege status of communication).
VI. CONCLUSION: FUTURE OF THE ATTORNEY-CLIENT PRIVILEGE

"Unless you can modify a rule to deal with the realities of modern technology, you will have a rule that cannot be enforced." 144

A communication is protected by the attorney-client privilege provided the mode of communication utilized warrants a reasonable expectation of privacy. The courts have traditionally extended the application of the attorney-client privilege to a communication medium once it is deemed sufficiently private. Modern communication mediums protected by the attorney-client privilege do not offer an absolute guarantee that interception or inadvertent disclosures will not occur. An absolute guarantee is not necessary for the application of the attorney-client privilege.

Many legal commentators opine that communications sent by way of Internet e-mail are particularly vulnerable to interception. For this reason, communications sent by Internet e-mail may waive the client’s attorney-client privilege. It is indisputable that Internet e-mail is susceptible to interception, misdirection and monitoring. Communication mediums that are currently protected by the attorney-client privilege, however, are susceptible to the same risks. The interception of Internet e-mail requires a degree of sophistication and expertise from hackers. In short, Internet e-mail is not easily intercepted. The intentional interception of Internet e-mail, regardless of the degree of sophistication required, is a felony. Internet e-mail communications are not absolutely secure. Internet e-mail, nonetheless, offers a reasonably private mode of communication that warrants the protection of the attorney-client privilege.

As the speed of business increases, clients will demand lawyers to keep pace. Internet e-mail offers lawyers and clients a cost effective and time efficient mode of communication. A historical consideration of the attorney-client privilege illustrates its flexibility and ability to adapt to technological advances in communication. While the attorney-client privilege may not currently extend to Internet e-

144 Cohen, supra note 49, at 1 (quoting Massachusetts lawyer Mark I. Berson’s opinion of modern communications and attorney-client privilege).
mail communications, technology and necessity will demand its protection in the future.

Sean M. O'Brien