E-Mail and the Attorney-Client Privilege: Simple E-Mail in Confidence

Ben Delsa
I. INTRODUCTION

Modern technology allows for the reproduction and transmission of information better, faster, and more efficient than ever before. It is now just as easy to communicate with someone on the other side of the planet as it is with someone across town. A message sent by electronic mail, commonly referred to as e-mail, enables a sender to transmit anything on a computer to anywhere in the world with a simple click of the mouse. No longer is it necessary to go through the time consuming motions of drafting a letter, mailing it, and waiting days for a reply.

E-mail has become a fixture in homes and offices all over the world. By the year 2000, it is estimated that forty million e-mail users will be sending sixty billion messages each year. Attorneys are among the growing number of people who have switched from the more traditional forms of communication to e-mail. E-mail is a commonplace means of communication among different branches of the same law firm or company, as well as between lawyers and their clients.

The popularity of e-mail can be attributed to its unique advantages over other forms of communication. E-mail documents cost less to store, can be edited and efficiently searched, and can disseminate information to several destinations at once. Unlike telephone calls, e-mail creates written records of communications, and allows users to send large documents and images by attaching them to the e-mail message. E-mail avoids "telephone tag," allowing people to respond to the e-mail when received rather than constantly trying to catch each other on the telephone. In contrast to facsimile transmission, e-mail can send information directly from a computer in a form that the recipient can
edit and return. "E-mail also costs less than a fax, especially when used for interstate or international communication."

Legal concepts must evolve to keep pace with new trends in technology. The traditional approaches courts have taken in the past must be rethought in light of new forms of communication. With the advent of this new technology comes new risks. Many attorneys use e-mail to communicate with clients without realizing the possible legal consequences. Once an e-mail message is sent over the Internet, "it can be read by people whose identities may never be known to the sender or receiver." And, for all practical purposes, the sender has lost all control over an e-mail message once it is sent.

The purpose of this comment is to analyze the possibility of waiver of the attorney-client privilege through the use of e-mail. It examines the different manners of e-mail transmission, the risks associated with each, and what happens when an e-mail message ends up in the hands of an unintended recipient. It also discusses possible precautions that attorneys should take so that their e-mail communications with their clients remain confidential. In considering whether the attorney-client privilege is compromised through the use of e-mail, the courts should look to the circumstances surrounding the transmission of the e-mail document, more specifically, what mode was used to transmit the e-mail and what measures were taken to ensure its security, both while in transit and in storage.

II. THE ATTORNEY-CLIENT PRIVILEGE

A. In General

The attorney-client privilege is the oldest of the common law privileges for confidential communications. The United States Supreme Court recognized

10. It should also be noted that the same rules applicable in this comment to the attorney-client privilege apply to the work product exception. Heidelberg Harris, Inc. v. Mitsubishi Heavy Indus., Ltd., No. 95 C 0673, 1996 WL 732522, at *1 (N.D. Ill. Dec. 18, 1996); see Hickman v. Taylor, 329 U.S. 495, 508, 67 S. Ct. 385, 392 (1947); Fed. R. Civ. P. 26(b)(3) (1970) (The work product immunity protects from discovery an attorney's thoughts, strategies, mental processes and opinions prepared in anticipation of litigation.); United States Fidelity and Guar. Co. v. Canady, Jr., 460 S.E.2d 677, 684 (W. Va. 1995) (Both protect litigants during discovery. The claimant bears the burden of proving the requisite elements for both the privilege or exception including "a showing that the communication originated in confidence, that it would not be disclosed, that it was made by an attorney acting in his or her legal capacity for the purpose of advising a client, and that it remained confidential.").
11. See 8 John H. Wigmore, Wigmore on Evidence § 2290, at 542 (McNaughton rev. ed. 1961) (The history of the privilege goes back to the reign of Elizabeth I when the privilege was for the consideration for the oath and the honor of the attorney rather than for the apprehensions of the
the need for the privilege as early as 1888.12 The “privilege protects the client from compelled disclosure of communications with his or her professional legal advisor made in confidence, unless the client has waived the privilege.”13 In Upjohn Co. v. United States, the Supreme Court recognized that the purpose of the privilege “was to encourage full and frank communications between the attorneys and their clients and thereby promote broader public interests in the observance of the law and administration of justice.”14

The privilege enables clients to “make full disclosure to their attorneys” of past wrongdoings,15 so that the client may obtain “the aid of persons having knowledge of the law and skilled in its practice.”16 Full disclosure and free and open communication helps to provide all the information necessary for the attorney to represent the client fully.17 The privilege also recognizes that sound legal advice does not “spring from lawyers’ heads as Athena did from the brow of Zeus,” but instead depends “upon the lawyer’s being fully informed by the client.”18 The privilege allows attorneys to assure clients that any confidential information given to their attorneys will remain confidential.19

Despite the gravity of the privilege, its use “obstructs the search for truth” and its “benefits are at best indirect and speculative.”20 In United States Fidelity and Guaranty Company v. Canady, the court noted that:

[T]he privilege is an exception to the general duty to disclose. Its benefits are all indirect and speculative; its obstruction is plain and concrete. . . . It is worth preserving for the sake of a general policy,

---

13. See Flaming, supra note 6.

A lawyer should be fully informed of all the facts of the matter he is handling in order for his client to obtain the full advantage of our legal system. It is for the lawyer in the exercise of his independent professional judgment to separate the relevant and important from the irrelevant and unimportant. The observance of the ethical obligation of a lawyer to hold inviolate the confidences and secrets of his client not only facilitates the full development of facts essential to proper representation of the client but also encourages laymen to seek early legal assistance.
but it is nonetheless an obstacle to the investigation of the truth. It ought to be strictly confined within the logic of its principle. We recognize the fundamental principle that "the public... has a right to every man's evidence."21 "[E]xceptions to the demand for every man's evidence are not lightly created nor expansively construed, for they are in derogation of the search for truth."22

Still, "courts sustain the privilege in individual cases to accomplish its larger systematic benefits—the greater law compliance and fairer judicial proceedings resulting from the 'sound legal advice [and] advocacy' the privilege promotes."23

B. Elements of the Attorney-Client Privilege

The party asserting the privilege has the full burden of establishing the existence of the privilege.24 The essential common law elements of the attorney-client privilege are:

(1) Where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at this instant permanently protected (7) from the disclosure by himself or by the legal adviser, (8) unless the protection be waived.25

Although the privilege originated in the common law, many jurisdictions have codified the privilege.26 For example, Louisiana's statutory privilege is comparable to the privilege at common-law. Under Louisiana Code of Evidence article 506, the privilege attaches when there is (1) the existence of a "confidential" communication, (2) made for the purpose of facilitating the rendition of legal services, and (3) the communication is between the client and his lawyer.27

25. See Admiral Ins. Co. v. United States District Court of Arizona, 881 F.2d 1486, 1492 (9th Cir. 1989) (citing Wigmore, supra note 11, § 2292 (These factors are widely-accepted. However, courts may vary in their treatment of elements of the privilege.)).
26. See 8 Wigmore, supra note 11, § 2292, at 555.
27. La. Code Evid. art. 506.
Two elements relating to the loss of the privilege, confidentiality and waiver, have been the source of frequent litigation. These two elements are of particular importance in the context of e-mail and the risk of waiver of the attorney-client privilege.

1. The Confidentiality Requirement

The privilege protects only those communications made between an attorney and client that are confidential. It is essential that communications are maintained in confidence. The privilege protects not only communications made by the client to his attorney but also those communications from the attorney to his client which would disclose the client's confidential communications. The mere showing of a communication between client and attorney is insufficient to prove the confidential nature of a communication and the existence of an attorney-client relationship by itself does not create a presumption of confidentiality. “It is of the essence of the privilege that it is limited to those communications which the client either expressly made confidential or which he could reasonably assume under the circumstances would be understood by the attorney as so intended.”

Three generally accepted criteria must be met to establish confidentiality: (1) “the client must intend his communications with his attorney to be confidential, (2) the client’s subjective intention of confidentiality must be reasonable under the circumstances, and (3) the confidentiality must have been subsequently maintained. A subjective expectation of privacy can sometimes be ascertained from the client’s express intentions”; however, those intentions often must be determined from the circumstances surrounding the communication. Thus, the courts use both subjective and objective tests in discerning confidentiality. When considering whether the privilege has been breached, courts focus on the precautions taken to preserve the confidentiality as well as the parties' reasonable expectation of privacy. This reasonable expectation of privacy can

be ascertained "by the form of the document as well as the circumstances and nature of the exchange."\textsuperscript{36}

One of the circumstances which indicates a lack of confidentiality is the presence of a third person who is not the agent of either the client or the attorney.\textsuperscript{37} A communication disclosed to third persons in furtherance of the rendition of professional legal services to the client or those reasonably necessary for the transmission of the communication is not indicative of a lack of confidentiality.\textsuperscript{38} For example, in \textit{Brown v. State}, the court held that statements made by the defendant to a polygraph examiner hired by defendant's attorney were privileged.\textsuperscript{39} The court reasoned that "the attorney-client privilege is recognized as attaching to communications between the agent of an attorney and the client, provided the communication is made to the agent upon the same subject matter about which the attorney was consulted and the agent was retained for the purpose of assisting him and rendering legal advice to or conducting litigation on behalf of the client."\textsuperscript{40}

2. \textit{Waiver of the Privilege}

The attorney-client privilege exists only if it has not been waived. The privilege is the client's alone, but his attorney or an agent acting with the client's authority may waive it.\textsuperscript{41} In a corporation, the corporation's management, i.e., the officers and directors, possess the power to waive the corporate attorney-client privilege.\textsuperscript{42} The privilege may be waived expressly if the "holder of the privilege voluntarily discloses or consents to disclosure of the matter or communication" or implicitly through circumstances which are inconsistent with a reasonable claim of

\begin{footnotes}
\textsuperscript{37} 8 Wigmore, supra note 11, § 2312, at 604 (The presence of a third person (other than the agent of either) is obviously unnecessary for communications to the attorney as such, however useful it may be for communications in negotiation with the third person.).
\textsuperscript{38} David J. Haydon, \textit{Identifying and Preserving the Attorney-Client Privilege in Various Business Transactions}, 61-OCT J. Kan. B.A. 24, 26; see also McCormick, supra note 33, § 91 ("In cases where the client has one of his agents attend the conference, or the lawyer calls in his clerk or confidential secretary, the presence of these intermediaries will be assumed not to militate against the confidential nature of the consultation, and presumably this would not be made to depend upon whether the presence of the agent, clerk or secretary was in the particular instance reasonably necessary to the matter in hand.").
\textsuperscript{39} 448 N.E.2d 10, 14 (Ind. 1983).
\textsuperscript{40} Id.
\textsuperscript{41} Hebert v. Anderson, 681 So. 2d 29, 32 (La. App. 4th Cir.), \textit{writ denied}, 684 So. 2d 936 (1996); see McCormick, supra note 33, § 91.
\end{footnotes}
confidentiality. A voluntary disclosure which is inconsistent with the confidential nature of the attorney-client relationship waives the privilege. Revealing a privileged communication to a third person generally destroys the privilege. For example, in United States v. Hamilton, the United States Seventh Circuit Court of Appeals found that the party waived any privilege when he voluntarily disclosed confidential information to his cellmate. On the other hand, the privilege remains intact "if the third party shares a community of interest with the privilege holder." "A community of interest arises when two parties have an identical legal interest with respect to the subject matter of a communication between an attorney and a client regarding legal advice."54

A party asserting claims or defenses that put his attorney's advice at issue may also waive the privilege. This is exemplified when an attorney is sued by a client for malpractice or a defendant asserts reliance on the legal advice of an attorney.55

III. ELECTRONIC MAIL GENERALLY

"[E]-mail is a means of transmitting messages or computer files between computers."51 It is essentially the electronic equivalent of mailing a letter.52 E-mail, like postal mail, has a facility, known as a "mailbox", that stores messages until the user recipient can read them.53 Each user has a unique "address" to send and receive messages so that messages are not received by the wrong person.54 Only the owner of the mailbox, or someone who has the password to the mailbox, can access what has been sent.

44. Alldread v. City of Grenada, 988 F.2d 1425 (5th Cir. 1993).
45. 19 F.3d 350, 353 (7th Cir. 1994).
49. Id.; see also 8 Wigmore, supra note 11, § 2327, at 638.
50. 460 S.E. 2d at 688; Hunt v. Blackburn, 128 U.S. 464, 470, 9 S. Ct. 125, 127 (1888) (client waived privilege when she alleged as a defense that she was misled by counsel); Chevron v. Pennzoil Co., 974 F.2d 1156, 1162 (9th Cir. 1992) (party's claim that its tax position was reasonable because it was based on advice of counsel puts advice at issue and waives privilege).
52. Grady, supra note 17, at 529.
53. Mathews, supra note 34, at 274.
54. Id.
The e-mail process is quite simple. When a user sends an e-mail message, the user’s computer stores the original document and produces a copy which it sends to a file server. The file server stores the copy and produces another copy which it sends to another file server. "Depending on the computer network structure, the e-mail message may go through two or more servers, with each storing its own copy and making new copies to forward to the intended recipient." Since each file server stores a copy of the original, deleting the original user’s copy only “deletes” that copy; “other copies of the document will reside with other recipients and file servers.” These other copies may stay in these file servers for days or possibly even months.

The fact that the file server keeps a duplicate copy of the e-mail message makes communicating by e-mail distinguishable from other forms of communication. Communicating by telephone merely requires only recorded disclosure of the source and destination. Communicating by postal mail only requires disclosure of the destination of a communication.

In addition, “unlike postal mail, simple e-mail generally is not ‘sealed’ or secured, and can be accessed or viewed on intermediate computers between the sender and recipient.” Thus, sending e-mail is more like sending a post card rather than a sealed envelope through the postal system. However, an e-mail message may not be accessed or viewed by these intermediary computers if it is encrypted.

“Encryption is the process of converting data (stored in digital form as a series of 1s and 0s) into an incomprehensible code through the use of an algorithm.” Only users with the proper key can read the encrypted message. By encrypting an e-mail document, unintended recipients cannot read the message.

56. Id.
57. Id.
58. Id. at 525 (“E-mail messages . . . are never actually ‘deleted.’ The delete command does not actually remove the message from the computer; it only . . . marks the file as reusable. The e-mail message is still there and will remain unchanged until the message is written over or until someone knowledgeable about computers runs a software program to clear old messages.”).
59. Id.
60. Id.
63. ACLU, 929 F. Supp. at 834.
65. Id.
66. See Agin, supra note 8.
E-mail may be transmitted by several different means. E-mail messages may be sent through a private or local area network (LAN), through semi-private networks or commercial services, or through any combination of these methods. Another method of transmission is the Internet. The Internet is the most widely used mode for the transmission of e-mail between attorneys and clients. Since the security of an e-mail message is related to the manner chosen to send the e-mail, each means of transmission must be analyzed separately.

IV. ANALYSIS OF E-MAIL AND THE ATTORNEY-CLIENT PRIVILEGE

A. E-mail Sent Through a Private or Local Area Network

Private networks and local area networks operate on a system accessible only by other computers on the same system (e.g., within the same office, firm, or organization). It is a closed system and e-mail messages sent from one computer to another computer go directly with no intermediary stops. Therefore, the electronic messages may only be accessed from within the organization owning the network. Such communication should be deemed sufficiently confidential provided that there are adequate procedures in place to ensure that unauthorized employees do not have access to the e-mail systems. In United States v. Keystone Sanitation Co., the court held that e-mail messages between attorneys of the same law firm maintained a reasonable expectation of privacy.

B. E-mail Sent Through a Commercial Provider

Semi-private or commercial services operate by providing e-mail access to anyone who pays a fee. Messages are sent from one computer to the commercial network where they are stored and subsequently accessed by another member of the service using a password. These commercial providers can guarantee system security for messages and files sent and received within the respective individual service. However, this security ends when messages are transferred to the Internet because these commercial providers have no authority to trace e-mail sent outside their systems. These commercial providers do not

---

67. A LAN is a group of computers connected together so that information can be sent between computers.
68. See Rose, supra note 51, at 196.
69. Id.
70. See Cook, supra note 3.
72. Commercial providers include MCI Mail, CompuServe, America Online and Prodigy.
73. See Cook, supra note 3.
74. See Rose, supra note 51, at 210.
75. Id. at 198.
know through which intermediary computers the e-mail message has or will pass in the chain of transmission—e-mail messages attach the route that they have been through so the file servers will appear on the message. Thus both the client and the attorney must be members of the same service to be protected by the security of the commercial provider.

When an attorney and client communicate via e-mail, the client should be aware that the communication will be disclosed to his e-mail provider for transmission.\(^7\) It is irrelevant whether the message is first conveyed from the attorney to the client. It is the client’s knowledge that determines the effect of the disclosure, and the client should be aware that the message will pass through his commercial provider whether the message is sent first from the attorney or the client. However, is this disclosure to the commercial provider enough to destroy the client’s intention of confidentiality?

Although the e-mail message is technically “disclosed” to the e-mail provider and arguably destroys any confidentiality, better reasoning would hold that this is not indicative of a lack of confidentiality. This disclosure is not a revealing of the contents of the message as is the case when the client or the attorney normally disclosed to a third party the contents of the message. The disclosure of the e-mail message to these intermediary computers is necessary for the transmission of the communication. “Rather than being accidental or distinctly separate from the process of communication between the client and the lawyer,” the disclosure is an integral part of the communication.\(^7\)

In addition, although system administrators generally have easy access to all communications transmitted through their computer networks,\(^7\) they are only allowed to read e-mail messages as necessary incident to the rendering of their services or, if necessary, to protect their property.\(^7\) This access should not destroy the privilege since the access by system administrators is severely limited. In comparison to another common form of communication, “lawyers routinely make use of the convenience of overnight delivery without fear that any privilege is waived or secret improperly revealed, even though the back of the airbill makes it clear that the carrier has an unconditional right to open any envelope or package for any reason or for no

\(^{76}\) See Benkler, supra note 61.

\(^{77}\) Id.

\(^{78}\) Id.


It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.
Moreover, the e-mail provider is essentially serving as an agent of either the client or the attorney, similar to the role of secretaries, who have not threatened the privilege in the past.81

E-mail on a commercial network has been held to be subject to a reasonable expectation of privacy. The court, in United States v. Maxwell, addressed the issue of privacy in e-mail messages waiting to be retrieved from the online computer service America Online.82 The court found that such users have an objective expectation of privacy, both as senders and recipients, in e-mail messages waiting to be retrieved by or from specific individuals. The court focused upon the passwords assigned to the network subscribers, holding that there was virtually no risk that the e-mail messages would be received by anyone other than the intended recipients. "The appellant clearly has an objective expectation of privacy in those messages stored in computers which he alone could retrieve through the use of his own assigned password," and he likewise "had an objective expectation of privacy with regard to the messages he transmitted electronically to other subscribers of the service who also had individually assigned passwords."83 The court even made a comparison of e-mail to the telephone, noting how communication by e-mail is "extraordinarily analogous" to a telephone conversation because it is "transmitted from one computer to another via telephone communication, either hard line or satellite."84

However, the decision may not extend to e-mail sent over the Internet. There is a crucial difference between the e-mail transmissions in Maxwell and Internet e-mail. The e-mail massages sent in Maxwell were wholly within America Online's system, i.e., the e-mail was sent to and stored only in computers owned by AOL. The court noted that e-mail messages sent over AOL are "afforded more privacy than similar messages sent over the Internet because they are privately stored for retrieval on AOL's centralized and privately-owned computer bank."85 AOL had a policy "not to read or disclose subscribers' e-mail to anyone except authorized users . . . offering its own contractual privacy protection in addition to federal statutory protections."86 In comparison, "the Internet has a less secure e-mail system, in which messages must pass through a series of computers in order to reach the intended recipient."87

84. Maxwell, 45 M.J. at 417.
85. Id.
86. Id.
87. Id.
C. E-Mail Sent Over the Internet

The biggest concern over waiver of the attorney-client privilege in connection with e-mail arises when an e-mail document is transmitted over the Internet. The Internet is the most widely used manner of transmitting e-mail. Even if a firm’s e-mail system uses a commercial provider such as America Online or MCI Mail, an e-mail message will pass over the Internet for at least part of its destination if the communication is to a person using the Internet for e-mail.88

1. The Internet Generally

The Internet is a series of interconnected networks of computers connected and accessed through the telecommunications infrastructure,89 that is, the phone lines and exchanges90 throughout the world connect the Internet.91 E-mail messages sent over the Internet may pass over dozens of computers, "owned and operated by disparate public and private entities92 on its way to its final destination."93 The result is a "decentralized, global medium of communications" which is not administered by a single entity.94 Intermediary computers, called "routers",95 copy each message and send it to the next one until it reaches

89. American Civil Liberties Union v. Reno, 929 F. Supp. 824, 832 (E.D. Pa. 1996) (“In terms of physical access, there are two common methods to establish an actual link to the Internet. First, one can use a computer or computer terminal that is directly (and usually permanently) connected to a computer network that is itself directly or indirectly connected to the Internet. Second, one can use a ‘personal computer’ with a ‘modem’ to connect over a telephone line to a larger computer or computer network that is itself directly or indirectly connected to the Internet.”).
90. An exchange is a central office in which telephone lines are connected to permit communication.
91. ACLU, 929 F. Supp. at 831. Internet e-mail generally travels over wire cables, much like a landline telephone call. The Internet e-mail is temporarily resident on each of those computers and could be stored in any one of those computers.
92. Id. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, non-profit organizations, and some are privately owned. 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. The network later allowed researchers across the country to access directly and to use extremely powerful supercomputers located at a few key universities and laboratories. 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 the ‘DARPA Internet’ and finally just the ‘Internet.’” Id.
93. Id. Some of the computers and computer networks that make up the Internet are owned by governmental and public institutions, non-profit organizations, and some are privately owned.
94. ACLU, 929 F. Supp. at 831.
95. Flaming, supra note 6; see also ACLU, 929 F. Supp. at 831. In 1996, there were approximately 9,400,000 routers worldwide.
its destination. A communication sent over the Internet could take any of a number of different routes to its destination. A message sent from a computer in New Orleans, Louisiana, to Los Angeles, California, might first be sent to a computer in Houston, and then to a computer in Dallas, and then to Denver, Las Vegas, and San Francisco, before finally reaching its destination in Los Angeles. “If the message could not travel along that path (because of military attack, simple technical malfunction, or other reason), the message would automatically (without human intervention or even knowledge) be re-routed” within a matter of seconds. In addition, e-mail messages sent over the Internet do not necessarily travel over the same path. “The Internet uses ‘packet switching’ communication protocols that allow individual messages to be subdivided into smaller ‘packets’ that are sent independently to the destination, and are then automatically reassembled by the receiving computer.”

2. Analysis of E-Mail Sent Over the Internet

E-mail sent via the Internet is not as secure as e-mail sent via a LAN or a commercial provider. Commercial providers can protect the confidentiality of those messages for their subscribers when the message is sent and received within their system; but once the message is conveyed over the Internet, their protection ends. Also, there is no contractual agreement between the owners of the routers and the client as compared to a commercial provider and its client. In fact, once e-mail is sent over the Internet, the sender usually has no idea “where it will go and whose computer it will pass through” on its route to the recipient. Hence, if client A, using America Online as its e-mail provider, sends a “confidential” communication to attorney B who uses an e-mail provider other than America Online, A and B should know that the message is contained within AOL’s system as well as B’s service provider. However, neither the client, the attorney nor the commercial provider knows where else this message might be stored or who has access to it.

However, does the mere fact that these messages are stored in these intermediary computers destroy any reasonable expectation of privacy? The owners of these intermediary computers are prohibited by federal law, in the

96. Flaming, supra note 6.
97. ACLU, 929 F. Supp. at 831.
98. Id. at 831-32.
99. Id. at 832.
100. Matthews, supra note 34, at 275. “A protocol is a specification of how two different systems are to communicate with each other via some kind of network. A protocol often has conversational rules, which prescribe what is sent first by one of the systems in one format and what the response can be from the other system.”
102. Rose, supra note 51.
same manner as the client's commercial provider, from monitoring e-mail messages for purposes other than assuring quality of service or maintenance. 104 In fact, this access restriction is exactly the same as that placed on "telephone companies which likewise are permitted to monitor conversations for service and maintenance of the network," 105 yet there is a reasonable expectation of privacy in telephone communications. 106 This prohibition should be enough to warrant a finding of a subjective expectation of privacy even though the e-mail message is stored in these unknown intermediary computers.

In Dunlap v. Rudder, the United States Ninth Circuit Court of Appeals found that despite a telephone line's susceptibility of monitoring, "a reasonable person could have an expectation of privacy for conversations conducted" over the monitored line. 107 In dicta, the court stated that "the capability of monitoring does not create implied consent to any monitoring that occurs. Cellular telephones and electronic mail are both technologies of questionable privacy, but we nonetheless reasonably expect privacy in our cell phone calls and email messages." 108 Likewise, monitoring by e-mail providers should not warrant an implied consent to any monitoring of e-mail messages that occurs and constitute waiver of the attorney-client privilege.

There also exists the threat of interception by hackers, both in the transmission of the message and in its storage. A hacker (technically "cracker" is the proper term) uses special software to gain access to the e-mail message. 109 Hackers use programs called "sniffers" to search for key words in mail that is coming across the Net. They can search for the sender's address or the recipient's address . . . . Once target mail is found, the message data is stored on the hacker's computer. Even though some e-mail is broken down into numerous data packets before it is sent across the Net, a sniffer program can pluck each data packet from the data stream and then reassemble the complete text . . . . Another type of program lets the hacker configure his machine to resemble the intended recipient's machine including its address. This is called "spoofing." A spoofer can intercept an e-mail message, concoct a false reply, and, if he or she wants, doctor the original message and send it on to the intended recipient. 110

106. See Katz v. United States, 389 U.S. 347 (1967) (The Supreme Court first recognized that a right to privacy in telephone communications in holding that evidence obtained by means of a listening device placed outside of a phone booth was inadmissible on Fourth Amendment grounds because the caller had a reasonable expectation of privacy.).
107. 1997 WL 414380 (9th Cir. 1997).
108. Dunlap v. County and Rudder, 1997 WL 414380, at *3 (9th Cir. 1997).
Although there exists the possibility of interception, "Internet e-mail is protected by the essential federal statutory privacy protections that apply to telephone conversations."

Title 18 makes it a federal crime to intercept "any aural, wire, or electronic communications by any person . . . [and] prohibits the use or disclosure of unlawfully intercepted communications." "Wire communications" mean any aural transfer (i.e., transfer containing a human voice) made in whole or in part through wire, cable, or other like connection between the point of origin and point of reception. "Electronic communications mean 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, photoelectric, or photooptical system." Hence, "during the period of time an Internet e-mail message is in transit from one computer to the next, the transmission is protected . . . just as if it were a normal landline telephone call." Therefore, under Title 18, "there is no greater insecurity when the Internet communication is in transit over the phone lines than there is with an ordinary phone call."

The greater risk to the unauthorized access by hackers exists in the routers which relay the message and maintain a copy of the message. Although there is potential exposure through each router, "each of these computers may handle thousands or even millions of messages per day among thousands of different persons and entities." One writer said that "the odds of finding a needle in a haystack are greater than the odds that a computer hacker would successfully locate a particular message from a lawyer to the client." However, one commentator believes that it is "cold comfort at best" to rely on the sheer volume of packets passing through these computers in defending the confidentiality of a communication. This is especially true in light of the fact that there are ways of identifying potentially interesting packets without reviewing each of them for content. Still, "because courts require lawyers to take 'reasonable precautions' to ensure that the privileged communication is made and maintained in confidence, it should be enough if the lawyer ensures that the communication

111. Slonim, supra note 83.
115. Slonim, supra note 83.
117. Lapidus, supra note 93, at 40.
119. Connolly, supra note 9.
120. Id. at B14 n.3 ("A determined snooper can use traffic analysis to restrict searches to e-mail originating at law firms, high-tech companies or particular e-mail accounts.").
is properly addressed and that the client has established procedures to ensure that the communication is received in confidence."\textsuperscript{121}

Congress, recognizing the threat of network hacking, enacted the Electronic Communication Privacy Act (ECPA) in 1986. The ECPA makes it unlawful to "intentionally access without authorization a facility through which an electronic communication service is provided."\textsuperscript{122} It also makes it unlawful to exceed an authorization to access a facility and thereby alter, obtain, or prevent "authorized access to a wire or electronic communication while it is in electronic storage."\textsuperscript{123}

There are, however, several exceptions to the ECPA which "allow a party to intercept access, or use communications."\textsuperscript{124} The government may do so for "law enforcement, administrative or national security purposes"; service providers may do so for "system maintenance or the protection of the rights or property of the provider," and a party may intercept and use an electronic communication where that "electronic communication is readily accessible to the general public."\textsuperscript{125}

The limited access by the government is so limited that it should not destroy the privilege. Likewise, as explained above, the limited access by service providers should not destroy the privilege. Under the third exception, the communication must be readily accessible to the general public. In \textit{Castano v. American Tobacco Co.}, the court found that documents available for copying from a university library, being published on the Internet, and available on CD-ROM were within the public domain.\textsuperscript{126} In contrast, e-mail documents sent over the Internet are not readily accessible to the general public. They are sent to specific individuals and can only be lawfully accessed by those individuals. The fact that there is special software which allows for hackers to intercept e-mail messages can hardly be said to be readily accessible to the general public. Also, Congress has made it clear that essentially any communication carried over a communication system provided by a telecommunications carrier is deemed not to be readily accessible to the general public.\textsuperscript{127} While there exists the possibility that e-mail messages can be intercepted, identifying one of the computers in which the message is located and subsequently locating, isolating and capturing "a particular message would take an investment in time and money—not to mention personnel who are both technically proficient and willing to violate the law."\textsuperscript{128} In addition, the privileged nature of a communication

\begin{footnotes}
\footnote{121}{Smith, supra note 118.}
\footnote{122}{18 U.S.C. § 2701(a)(1) (1994).}
\footnote{123}{18 U.S.C. § 2701(a)(2) (1994).}
\footnote{124}{\textit{Id.}}
\footnote{125}{Karen L. Hagberg, \textit{Shadow Data, E-mail Play a Key Role in Discovery, Trial, N.Y.L.J.}, June 16, 1997, at 53,510.}
\footnote{126}{896 F. Supp 590, 595 (E.D. La. 1995).}
\footnote{127}{18 U.S.C. § 2518 (1994).}
\footnote{128}{Pope, supra note 4 (citing William Frievogel, \textit{Communicating with or about Clients in the}}
does not turn on whether interception of the communication is possible, but rather whether the communication was made in 'confidence' and whether any disclosure by a party to the communication is intentional or inadvertent.\textsuperscript{129} It is not required nor possible to have one hundred percent security when communicating with clients by any means of communication.\textsuperscript{130}

V. OTHER FORMS OF COMMUNICATION (RELATED TECHNOLOGIES)

The risk of interception is not unique to e-mail. Other forms of communication are equally at risk of being intercepted. It is impossible to guaranty the security of any communication. Equipment necessary to tap a regular telephone line can be purchased for less than twenty-five dollars at most local electronic stores.\textsuperscript{131} Yet, "the fact that some individuals eavesdrop on regular telephone conversations does not mean that no one has a reasonable expectation of privacy for ordinary phone calls."\textsuperscript{132} In the context of the attorney-client privilege, it is only necessary that the means of communication is reasonable, not that it is impenetrable.

E-mail is protected from interception by federal law the same way that written mail is protected by federal law from interception, "just as telephone voice messages or fax messages are protected from interception by the [Federal Wiretap] Act."\textsuperscript{133} Therefore, in light of present legislative protections, e-mail should be seen as a reasonable means of communication for transmitting confidential communications much the same way that written mail and telephone calls are.

There are no cases which directly address the issue of whether e-mail sent over the Internet is subject to a reasonable expectation of privacy. Still, the prohibition on the interception of e-mail communications and the restrictions on the e-mail providers, while not preserving the privilege, are indicative of an objective expectation of confidentiality; and therefore, the mere showing that the communication was sent by e-mail over the Internet should not destroy the attorney-client privilege.

VI. INTERCEPTED E-MAIL

Although the mere transmission of e-mail is insufficient to warrant a finding that there is no attorney-client privilege, does the interception of e-mail lead to the waiver of the privilege? Just as there is no privilege waiver when written

\textsuperscript{129} Pope, supra note 4.
\textsuperscript{130} Leibowitz, supra note 35.
\textsuperscript{131} United States v. Smith, 978 F.2d 171, 179 n.10 (5th Cir. 1992).
\textsuperscript{132} Id.
mail is stolen, the interception of e-mail by criminal conduct should not lead to the waiver of the privilege when reasonable precautions have been taken to ensure its confidentiality.

In Section 2517(4) of Title 18, Congress provided 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." Thus, the interception or access of e-mail communications while in transit or storage, assuming they meet all the other requirements of the attorney-client privilege, should not result in the loss of the privilege if they are intercepted.

In In re Dayco Corp. Derivative Securities Litigation, the court found that there was no waiver where the defendant's privileged documents, referred to as the Curry "diary" or "chronology", came into a reporter's possession and was published, all without the client's permission. The reporter indicated that he obtained a copy of the diary from an unidentified source. The court held that, "absent any indication that [the defendants] voluntarily gave the diary to the [press], publication of excerpts of [the privileged documents] should not be considered a waiver of the privilege." Likewise, if an e-mail message is intercepted and printed in the press or given to an unintended recipient, a waiver should not be found, provided that reasonable precautions were taken to ensure its confidentiality.

VII. INTERNAL SECURITY EMPLOYED BY LAWYERS AND CLIENTS

The reasonableness of e-mail as a mode of communication also depends on the policies for use, retention and destruction of e-mail implemented by both the law firm and the client. Communications which are intended to be confidential but are intercepted despite reasonable precautions remain privileged. Issues to be considered in determining whether reasonable precautions have been taken include: Who routinely has access to e-mail? Is access determined by a password? Could anyone in the company retrieve the message? Are confidential communications routinely deleted, printed in hard copy or transferred to disk?

Due to the permanent nature of e-mail documents, attorneys and clients must be wary of their system of controls over e-mail storage, use and destruction. Unlike the shredding of a paper document, the mere hitting of the delete button does not destroy the document. Even if the user's copy is successfully deleted, there are other copies which exist that will be unaffected.

135. Id. at 469.
136. Id. at 470.
137. Id.
138. Olmstead, supra note 55.
Procedures for periodic retention and destruction of electronic documents should be established, maintained and monitored. These procedures should consider all potential copies of electronic documents: backups and archival tapes; operating systems that create logs of data files; "off the end" data stored on magnetic tapes not overwritten when the tapes are reused to store other information; PCs connected in a LAN . . . that may contain independent storage capacity; laptops; and floppy diskettes containing documents not transferred to the main system.139

Attorneys should make sure that such precautions are taken and that they advise their clients to do the same to ensure that the attorney-client privilege is maintained.

VIII. INADVERTENT DISCLOSURES

While it is evident that a voluntary disclosure of information which is inconsistent with the confidential nature of the attorney client relationship waives the privilege,140 there is no consensus as to the effect of an inadvertent disclosure of confidential communications.141 There are several different ways that an e-mail document may inadvertently end up in the hands of an unintended recipient. An e-mail message could be "placed in the wrong box when delivering responses to a discovery request";142 a secretary could mistakenly hit the wrong key on the keyboard, sending the e-mail document to the wrong recipient; or a privileged e-mail could be "accidentally produced when responding to a voluminous discovery request."143

Courts have used "three different tests when deciding whether the inadvertent production of a privileged document waives the attorney-client privilege."144 The three tests are: the "strict test," the "lenient test" and the "middle test."145

139. Id. at 527.
141. Allred v. City of Grenada, 988 F.2d 1425, 1434 (5th Cir. 1993).
142. Dorothea Beane, Inadvertent Disclosure of Attorney-Client Privileged Material: Putting the Horse Back in the Barn, 69 Fla. B.J. 67 (1995). Unlike paper correspondence, it is extremely easy to inadvertently misaddress an e-mail. Computer users typically address e-mail from an online directory and simply click on the wrong recipient's address.
143. Id.
144. Id. at 68.
A. The Strict Test

Some courts apply the strict test, finding that the privilege is lost once there has been a disclosure to third parties, "even if the disclosure is unintentional or inadvertent." The Fourth Circuit reasoned, in In re Sealed Case, that "the amount of care taken to ensure confidentiality to the holder of the privilege reflects the importance of that confidentiality to the holder of the privilege." Thus, a disclosure, although inadvertent, is indicative of the lack of concern over confidentiality in the message.

These courts follow a traditional view expressed by Wigmore that any disclosure of a privileged communication is a waiver, no matter what precautions were taken to avoid it: All involuntary disclosures, in particular, through the loss or theft of documents from the attorney's possession, are not protected by the privilege, on the principle . . . that, since the law has granted secrecy so far as its own process goes, it leaves to the client and attorney to take measures of caution sufficient to prevent being overheard by third persons. The risk of insufficient precautions is upon the client. This principle applies equally to documents.

This approach is disadvantageous to the client in that it takes from him the ability to control when the privilege will be waived; "the privilege for confidential communications can be lost if papers are in a car that is stolen, a briefcase that is lost, a letter that is misdelivered, or in a fascimile that is missent." It is also inconsistent with "the Supreme Court's admonition that courts should apply the privilege to ensure a client remains free from apprehension that consultations with a legal advisor will be disclosed."

B. The Lenient Test (No Waiver Rule)

Other courts apply the lenient test, or "no waiver" rule, finding that the "mere inadvertent production [of privileged documents] does not waive the [attorney-client] privilege." These courts never find a waiver of the

---

146. Allread v. City of Grenada, 988 F.2d. 1425 (5th Cir. 1993); see, e.g., In re Sealed Case, 877 F.2d 976, 980 (D.C. Cir. 1989); In re Grand Jury Proceedings, 727 F.2d 1352, 1356 (4th Cir. 1984).
147. 877 F.2d 976, 980 (D.C. Cir. 1989).
150. Id.
privilege unless there has been a deliberate disclosure. There are two reasons behind this view. First, the client is the holder of the privilege, not the attorney, so an act of the attorney cannot constitute a waiver of the privilege." Second, "a 'waiver' is by definition the intentional relinquishment of a known right, and the concept of an 'inadvertent waiver' is therefore inherently contradictory." Thus, as one court concluded, "if we are serious about the attorney-client privilege and the client's welfare, we should require more than ... negligence by counsel before the client can be deemed to have given up the privilege."

C. The Middle Test

Still, the majority of the courts have chosen to apply the middle test, opting for "an approach which takes into account the facts surrounding a particular disclosure" in determining whether the inadvertent disclosure has waived the privilege. This approach "focuses upon the reasonableness of the steps taken to preserve the confidentiality of privileged documents." The Fifth Circuit has adopted this view in discerning whether the inadvertent production of privileged documents results in a waiver of the privilege. Courts following this approach find that a disclosure resulting from gross negligence constitutes a waiver of the privilege. "Inadvertent disclosures are, by definition, unintentional acts, but disclosures may occur under circumstances of such extreme or gross negligence as to warrant deeming the act of disclosure to be intentional."

Courts that have adopted the middle test employ a multi-factor analysis when determining whether documents have lost their privilege through inadvertent disclosure. The factors they consider are: (i) precautions taken to prevent inadvertent disclosure in view of extent of document production; (ii) number of inadvertent disclosures; (iii) extent of disclosures, and delay in rectifying disclosure; and (iv) whether overriding interests of justice would be served by

156. Mendenhall, 531 F. Supp. at 955.
159. Lapidus, supra note 93.
relieving party of consequences of error.\textsuperscript{161} The presence or absence of one factor of the test is not determinative of a finding of waiver. Rather, the courts will look to all the factors in considering whether a party has undertaken reasonable precautions to avoid inadvertent disclosures of privileged documents.

IX. ENCRYPTION

Though intercepted or inadvertently sent e-mail which is not encrypted should not result in a waiver of the attorney-client privilege, the advantage inherent in the privilege can nevertheless be lost. For example, the contents of a privileged e-mail communication could end up on the front page of the newspaper or in the opposing counsel’s hands, regardless of whether the communication retains its privileged status. To safeguard against such a result, attorneys should encrypt any highly-sensitive material that they do not want to end up in the press, especially if the message will be transmitted over the Internet. With good encryption, “the only security risks come from someone stealing the private encryption keys, or someone tricking you into thinking he’s your client.”\textsuperscript{162}

There are several drawbacks to the use of encryption. Both the attorney and the client must have the encryption software.\textsuperscript{163} In addition, certain encryption technologies may not be exported outside the United States and Canada.\textsuperscript{164} “Some countries, such as France, Russia and China, prohibit use of encryption technology entirely.”\textsuperscript{165} This makes encryption programs of limited value in international communications.

The use of encryption has been suggested by some as necessary to preserve the attorney-client privilege when a document is sent by way of e-mail.\textsuperscript{166} These authors suggest that the risk of interception makes unencrypted e-mail an unreasonable mode of communication for preserving the attorney-client privilege.

Although simple e-mail, i.e., e-mail that is not encrypted, can be intercepted and read upon interception, the failure to use encryption should not indicate a party’s lack of an expectation of confidentiality. Confidentiality does not turn on whether the communication is capable of being intercepted. All that is required is that the parties reasonably expect the communication to be confidential. No communication is entirely secure, and e-mail is no exception. In light

\textsuperscript{161} See, e.g., F.D.I.C. v. Marine Midland Realty Credit Corp., 138 F.R.D. 479, 482-84 (E.D. Va. 1991) (balancing the above factors and finding the privilege waived); Golden Valley Microwave Foods, Inc. v. Weaver Popcorn Co., Inc., 132 F.R.D. 204, 209 (N.D. Ind. 1990) (finding the privilege waived due to counsel’s failures to take precautions to prevent disclosure and to rectify error); Bud Antle, Inc. v. Grow-Tech, Inc., 131 F.R.D. 179, 183-84 (N.D. Cal. 1990) (finding the privilege waived based on the above factors, especially the “overriding issue of fairness”).


\textsuperscript{163} Id.

\textsuperscript{164} Id.

\textsuperscript{165} Id.

\textsuperscript{166} See Connolly, supra note 9; Agin, supra note 8.
of the legislation which makes it illegal to intercept e-mail, there should be a finding of an objective expectation of privacy even when using simple e-mail.

Although encryption should not be necessary to preserve the attorney-client privilege, attorneys should be aware of the risks involved when using simple e-mail and should advise their clients of the risks of interception. Because there is a risk of interception, highly sensitive material should either be encrypted or not sent over the Internet.\textsuperscript{167} Attorneys should also discuss the benefits of encryption with their clients. "Out of an abundance of caution, an attorney might get a written consent from the client, but the better reasoned authorities do not require client consent."\textsuperscript{168}

\section*{X. Policy Concerns}

The attorney-client privilege is designed to encourage a client to speak freely and fully with his attorney in confidence so that the attorney can fully represent him. The law should grant protection to the client for this privilege whenever it is evident that communications between attorney and client are made in confidence and that expectation of confidentiality is reasonable. The law should not put a stranglehold on the means of communication between a client and his attorney, especially where, as here, such means are reasonable in light of the surrounding circumstances.

The advantages present in e-mail communication make it a popular choice of communication in-house, among different branches of the same law firm, among different branches of the same company, and between lawyers and clients. "With increasing frequency, attorneys and their clients are turning to electronic mail to speed the flow of information and documents back and forth. No longer is it adequate to rely on the mail, or even next-day document delivery services."\textsuperscript{169} The law needs to reassure clients that confidential documents will not be disclosed simply because e-mail was used to exchange the information. If courts should step in and rule that the use of e-mail does constitute a waiver of the attorney-client privilege then the whole purpose of the privilege, to "encourage full and frank communications between the attorneys and their clients," will be frustrated.\textsuperscript{170}

\section*{XI. State Opinions}

There is no clear consensus among the states as to whether Internet e-mail is privileged. The South Carolina State Bar Association said, in September 1997, that "Internet e-mail was secure enough to raise a reasonable expectation of

\begin{thebibliography}{99}
\bibitem{167} Slonim, \textit{supra} note 83.
\bibitem{168} \textit{Id.}
\bibitem{169} Smith, \textit{supra} note 118.
\end{thebibliography}
privacy and could . . . be used by attorneys and clients to communicate.  

This determination is in line with the New York Bar Association, the Vermont Bar Association, and the Illinois State Bar Association.

The Illinois State Bar Association stated that "lawyers may use electronic mail services, including the Internet, without encryption to communicate with clients unless unusual circumstances require enhanced security measures." Such unusual circumstances would be those "involving an extraordinary sensitive matter that might require enhanced security measures like encryption, but in such situations, ordinary telephone and other normal means of communication would also be deemed inadequate." The Illinois opinion was based on the fact that "the expectation of privacy for e-mail is no less reasonable than for ordinary telephone calls" and that "the unauthorized interception of e-mail subject to ECPA is illegal." The Vermont opinion was based on the premise that since "any phone call can be tapped, legally or otherwise, and the mails and faxes can be intercepted and read . . . no reason exists to treat e-mail differently."

In contrast, authorities in Iowa and North Carolina "hold that it is unethical to use the internet unless the communications are encrypted or the client has consented." These authorities base their opinions on a concern for the security of the Internet, especially the fact that operators of the intermediary computers can read the messages and that "e-mail is susceptible to interception by anyone who has access to the computer network to which a lawyer 'logs-on' and such communications are rarely protected from interception by anything more than a simple password." In so deciding, the Iowa and North Carolina opinions overlook the "federal statutory protections afforded to e-mail and the technical difficulties attendant to interception."

**XII. CONCLUSION**

The law must evolve to meet society's needs and demands for modern technology without imposing an undue burden upon the use of such means. It should recognize that modern technology involves new risks. Old laws must be reevaluated in light of this new technology and its inherent risks, taking into account all the surrounding circumstances. To merely say that the risk of e-mail interception makes it an unreasonable means of communication is to turn a blind

171. Cook, supra note 3.
172. Slonim, supra note 83.
173. Cook, supra note 3.
174. Slonim, supra note 83.
175. Id.
176. Id.
177. Id. (citation omitted).
178. Id. (citation omitted).
179. Id.
eye towards the reality of modern society. There now exists the inherent possibility of intercepting any form of communication: facsimile, phone, mail, and even person to person conversations. There is no communication means which is risk free. If someone wants to obtain information illegally, they are going to find a way to do so, no matter how safely guarded the information. The possibility of interception is not the standard by which communication means are adjudged confidential or not. Rather, the communication must be seen as providing a reasonable expectation of privacy to its user; and e-mail by whatever means does just that.

Transmission of a communication by way of e-mail should not destroy the attorney-client privilege, whether it is sent through a LAN, by a commercial provider, or over the Internet. There is legislation already in place which should allow for a client to make an unencrypted e-mail communication with his attorney in confidence and without fear of waiving the attorney-client privilege. Still, attorneys must be wary of the risks of simple e-mail and advise their clients accordingly, especially since there are no court decisions deciding the issue with respect to the Internet. Encrypting e-mail, which makes it unreadable to an unintended recipient, can alleviate the fear of an e-mail message ending up in the hands of an unintended recipient and should be used with highly sensitive documents; but it should not be required of all confidential documents. It must ultimately be remembered that the purpose of the attorney-client privilege is “to encourage full and frank communication between attorneys and their clients.”

To lose sight of this is to forget that the privilege exists to protect the client so that he can have confidence in his attorney and in the law itself.

Ben Delsa
