Richmond Journal of Law and Technology

Volume 7 | Issue 3 Article 6

2001

United States v. Keystone Sanitation Company: E-mail and the Attorney-Client Privilege

Karen M. Coon
University of Richmond

Volume VII, Issue 3,
Winter 2001

United States v. Keystone Sanitation Company: E-mail and the Attorney-Client Privilege

by: Karen M. Coon(*)

Cite As: Karen M. Coon, Note, *United States v. Keystone Sanitation Company: E-mail and the Attorney-Client Privilege*, 7 RICH. J.L. & TECH. 30 (Winter 2001), *at* http://www.richmond.edu/jolt/v7i3/article4.html.

TABLE OF CONTENTS

I. INTRODUCTION

{1}The rapid growth and sophistication of technology have changed the way people communicate. E-mail and the Internet have begun to affect the way attorneys communicate with their clients. E-mail is fast and convenient, but it is not without risks. The risk of illegal interception and the risk of inadvertent disclosure are serious issues that attorneys need to be aware of and try to prevent so that the attorney-client privilege is protected as much as possible. Although communicating with a client by e-mail may be risky, the risks posed by e-mail are no different from those posed by communicating by postal mail, telephone, or fax machine.

{2}In an attempt to regulate telephonic communications, Congress passed the Federal Communications Act of 1934 ("FCA").[1] With the development of the Internet and e-mail, new risks arose, and it became necessary to regulate electronic communications. As a response, Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA").[2] Although the district court in *United States v. Keystone Sanitation Company*[3] encountered e-mail and the attorney-client privilege, the court failed to explain fully and adequately the implications and effects of e-mail on the attorney-client privilege.

{3}This note explores the implications of e-mail for the attorney-client privilege. Part II presents the basic elements of the attorney-client privilege and explains why the privilege is important. Part III introduces the ECPA, and Part IV gives a brief background on the development of the Internet and e-mail, explains the different types of e-mail systems, compares and contrasts e-mail with other forms of communication, and discusses the benefits of e-mail. In addition, Part V presents the history and issues involved in *United States v. Keystone Sanitation Company*. Finally, Part VI examines the current state of the law regarding e-mail and the attorney-client privilege, and provides a summary and conclusion of the main points of this note.

II. THE ATTORNEY-CLIENT PRIVILEGE

{4}The conversations shared, information exchanged, and advice offered between an attorney and his client generally fall under the attorney-client privilege. Information considered privileged need not be disclosed to an opposing party during the discovery process. According to the Federal Rules of Civil Procedure, "[p]arties may obtain discovery regarding any matter not privileged, which is relevant to the subject matter involved in the pending action ..."[4] In addition, the American Bar Association's Model Rules of Professional Conduct indicate that an attorney may not disclose any information concerning a client's case, unless the client has authorized disclosure or disclosure is necessary to represent the client.[5] Generally,

> [t]he attorney-client privilege arises (1) [w]here legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in

> confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[6]

However, because the privilege is in opposition to the notion that all evidence should be available so that the investigation for truth is successful, the privilege "ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle."[7]

{5}The purpose of the attorney-client privilege, which is the oldest confidential communications privilege recognized by the common law,[8] is to promote open and honest communications between attorneys and clients.[9] In order to give clients complete and accurate information and advice, attorneys must be fully informed.[10] Knowing that communications are privileged may encourage clients to divulge pertinent information that they may be unwilling or afraid to share absent the privilege. Since disclosure undermines the confidentiality of the communication, the privilege is usually waived if the information is disclosed to a third party.[11]

III. ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)

{6}Prior to Congress passing the ECPA[12] in 1986, the FCA prohibited unauthorized publication or use of radio or telephone communications.[13] The development of the Internet and e-mail made it necessary to pass the ECPA so that electronic communications would also be protected. The ECPA prohibits the interception and disclosure of wire, oral, or electronic communications.[14] Specifically prohibited acts include: "intentionally intercept[ing], endeavor[ing] to intercept, or procur[ing] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[15] The ECPA expressly states that "no otherwise privileged wire, oral, or electronic communication intercepted ... shall lose its privileged character."[16]

IV. ELECTRONIC MAIL

A. *Brief Overview of the Internet and E-mail*

{7}The Internet grew out of a U.S. Department of Defense project. Originally called the "ARPANET," the Internet was developed starting in 1969 by the Advanced Research Project Agency. It was designed to ease the sharing of information between researchers at various universities and in the military. Additionally, the Internet was also meant to assure that communication could continue during a nuclear attack.[17] The Internet is a vast network connecting many different "host" computers, each having their own address for sending and receiving e-mail.[18]

{8}E-mail is "a document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message."[19] When e-mail messages are sent, they travel through various routes and are broken up into separate segments, called "packets," before arriving in the recipient's e-mail mailbox.[20] There are four different types of e-mail systems: direct e-mail, private e-mail, on-line service provider, and Internet access provider. Each system requires users to have a username and a password in order to access their individual e-mail accounts and to receive and send messages.

B. *Types of E-mail Systems*

1. Direct E-mail

{9}Direct e-mail requires that the sender directly dial the receiver's modem. The modem puts the e-mail

message into digital form before transferring the message through phone lines to the receiver's modem. The receiver's modem then translates the digital information back into language format so that it is readable by the receiver.[21] The information is in digital form as it travels through the phone lines, so intercepting and reading information on direct e-mail systems is more difficult than intercepting other types of communication.[22]

2. Private E-mail

{10}There are two types of private e-mail systems: internal corporate e-mail systems and "extranet" networks. Internal corporate e-mail systems permit only internal access. "Extranet" networks involve one private network directly dialing another private network.[23] The attorney-client privilege may arise in the context of private e-mail systems when an attorney discusses a client's case over e-mail with another attorney who is internally connected to the same private system, or when a corporation's in-house counsel communicates by e-mail with a member of the corporation who is the client.[24] The American Bar Association ("ABA") and various state bar associations all indicate that private e-mail systems maintain confidentiality since the messages travel directly from one computer on a private network to another computer on the same private network. Additionally, even if a message on a private network is intercepted or inadvertently received by an unintended party, all attorneys and/or employees with access to the network are obligated to maintain confidentiality for all of the firm's clients.[25]

3. On-line Service Provider

{11}On-line service providers issue passwords to users who then access e-mail accounts from which the users can send and receive messages. User mailboxes are maintained by the on-line service provider in a public forum, although each individual mailbox is protected by password. Thus, even though individuals have private mailboxes accessible only by password, messages could inadvertently be delivered to the mailbox of another user.[26]

{12}Unlike private in-house e-mail systems, in which all users owe a duty of confidentiality, most people who utilize on-line service providers owe no duty of confidentiality to other users of the on-line service provider.[27] In addition, the policy of the individual on-line service provider affects how secure the system is. Depending on its policy, the on-line service provider's system administrator may be permitted to access and examine certain e-mail messages.[28] Such inspection is regulated and restricted by federal law.[29]

4. Internet Access Provider

{13}E-mail can also be sent over the Internet without utilizing an on-line service provider. Instead, Internet access providers are used to get messages to their destinations.[30] Each user has a local Internet access provider. The local Internet access provider "connects with a larger Internet provider ... [and] [t]hat provider may, in turn, connect to an even larger provider."[31] Like on-line service providers, Internet access providers may reserve the right to inspect e-mail and may also randomly monitor messages.[32]

C. *E-mail Compared and Contrasted with Other Methods of Communication*

{14}Attorneys have a duty to protect the confidentiality of client information and to protect confidential information from being misused or inadvertently disclosed. Confidential client information must be "acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality."[33] Therefore, in order to protect the attorney-client privilege, attorneys are required to use methods of communication through which they can "reasonably" expect confidentiality to be maintained.[34]

1. U.S. Postal Mail

{15}The U.S. Postal Service is considered "reasonably" secure, and is therefore a common and acceptable method of attorney-client communications.[35] In many ways, sending e-mail is like sending a letter through the U.S. Postal Service. Letters, which are addressed to specific recipients, pass through various hands in many different places before arriving at their destination. It is possible that someone other than the intended recipient could open the letter and read the information. It is also possible that the letter could be inadvertently delivered to the wrong person. Similarly, e-mail messages pass through many different routes before reaching their destination, and it is possible that e-mails may be intercepted or retrieved by someone other than the intended recipient.

{16}Despite the similarities between letters sent via the U.S. Postal Service and messages sent via e-mail, letters are generally considered more secure than e-mail messages since letters are sealed.[36] On the other hand, both the U.S. Post Office and many on-line service providers reserve the right to inspect the letters or messages sent through their service. Thus, neither postal mail nor e-mail guarantee absolute privacy.

{17}In addition, unlike letters that are sent as one complete document, e-mail messages are generally transmitted to the recipient in "packets." The "packets" are then put together to form the message once they reach their destination.[37] Since e-mail messages are not sent as single, complete documents, it is very difficult to intercept all the "packets" and put them all together to from the actual message.[38] In contrast, letters, which are sent as single documents, allow an interceptor access to the complete document.

2. Telephones

{18}The American Bar Association has specifically stated that "a lawyer has a reasonable expectation of privacy in the use of a telephone."[39] Using a telephone to communicate with a client does not breach the attorney-client privilege. Intercepting and reading information on e-mail systems (especially on direct e-mail systems) is generally more difficult than intercepting and eavesdropping on telephone conversations because, unlike phone conversations, the information in e-mail messages is in digital form as it travels through the phone lines. Decoding this digital message requires more skill than would be required to intercept a phone call.

3. Fax Machines

{19}A fax machine is considered a "reasonably" secure method of communication.[40] The process of sending information by e-mail is practically indistinguishable from the process of sending a fax.[41] Since e-mail uses the same type of digital transmitting system as fax machines use, and since faxes are protected by the attorney-client privilege, e-mails should also be protected by the attorney-client privilege.[42]

{20}Despite the similarities in the process of sending an e-mail message and sending a fax, differences do exist. One difference is that e-mail messages are stored during transmission.[43] An e-mail is stored by the private network, the on-line service provider, or the Internet access provider. Additionally, once the e-mail reaches its destination, it is saved on the recipient's network. Deleting the message from the recipient's e-mail mailbox does not necessarily mean that the message is completely erased from the network. Since many law firms periodically "back-up" the information on their networks, information that is deleted from individual mailboxes and from the network may still be found on a "back-up" disk.[44] Unlike e-mail messages, faxes are not stored or saved; they are printed out as soon as they travel through the phone line to their destination.

{21}Another difference between e-mails and faxes is that inadvertently sending information to an unintended recipient is generally much easier to do when using a fax machine. Sending a fax requires entering a seven-digit number. Just as entering one incorrect digit will result in calling someone different on the telephone, entering one incorrect digit will result in the fax printing out on an unintended recipient's fax machine.[45]

{22}On the other hand, each e-mail user has a specific address. Without the exact e-mail address, information cannot be transmitted by e-mail.[46] Interchanging letters or numbers that comprise the e-mail address, or entering an incorrect letter or number into the address is more likely to result in the message being returned to the user because it was undeliverable. Finally, e-mail addresses often contain the name of the recipient. This makes it less likely that the intended recipient's e-mail address will be accidentally confused with a different recipient's e-mail address.[47] In contrast, fax numbers do not contain the intended recipient's name and could be easily confused with an unintended recipient's fax number.

D. *Benefits of E-mail*

{23}E-mail has become very popular partly because of the advantages it offers over other methods of communication. One advantage is convenience. The sender can type an e-mail message and send it at any time, regardless of whether the intended recipient is also using e-mail at the same time or is available at that time. The message will be sent and stored until the recipient retrieves it. In contrast, using the telephone or a fax machine may result in receiving a busy signal and being unable to contact the recipient.

{24}Another advantage is that e-mail allows the sender to sit at his desk and transmit information to anyone in the world in a short amount of time.[48] E-mail also allows the user to correct and edit outgoing documents quickly and easily. Faxes, on the other hand, require retyping the entire document in order to make corrections. E-mail also provides the benefit of easy access of stored material. Storing paper documents takes up more room than storing the same documents on a hard drive or a disk. Finally, e-mail is generally more inexpensive and cost-effective than other forms of communication. Sending a one-page fax can cost as much as sending one page by first class mail. However, for the same price a person could send about 100 pages over e-mail.[49]

V. *UNITED STATES V. KEYSTONE SANITATION COMPANY*

A. *Background*

1. *Keystone I*

{25}In *Keystone I*,[50] the United States filed suit against the Keystone Sanitation Company and ten other defendants to recover money spent by the Environmental Protection Agency ("EPA") for cleaning up a contaminated landfill site pursuant to the Comprehensive Environmental Response Compensation and Liability Act ("CERCLA").[51] In particular, the Keystone I court dealt with the United States' motion to dismiss the defendants' counterclaims. The court ultimately granted the motion to dismiss some of the counterclaims, but denied the motion for other counterclaims.[52]

2. *Keystone II*

{26}In *Keystone II*,[53] the court examined the claims of the other defendants who were also held responsible for clean up costs. The other defendants claimed that Keystone distributed and disposed of its assets in order to avoid paying its share of the CERCLA liability.[54] To establish that Keystone transferred assets in order to avoid CERCLA liability, the other defendants requested production of all documents related to the transfer of assets since the time the EPA began investigating Keystone. In particular, the other defendants requested attorneys' billing statements dealing with the transfer of Keystone assets.[55]

{27}Keystone produced printouts of e-mail messages containing attorneys' billing statements and e-mail printouts indicating that Keystone's attorneys were giving Keystone legal advice about how to transfer assets out of the corporation.[56] Keystone claimed that the documents were protected by the attorney-client

privilege. The other defendants claimed that since Keystone included printouts of the e-mail messages when they produced prior documents, the attorney-client privilege was waived.[57] Keystone insisted that the privilege was not waived since the disclosure was inadvertent.[58]

{28}The *Keystone II* court explained that attorney billing statements "are protected by the attorney-client privilege only to the extent that they reveal litigation strategy and/or the nature of services performed."[59] Since the Keystone billing statements contain information about the nature of services performed, the court indicated that the documents would be "protected by the attorney-client privilege, absent a waiver."[60] Ultimately, the court held that Keystone waived the attorney-client privilege by providing the documents at a previous time. Keystone, therefore, had to produce all attorney billing statements related to the distribution of assets.[61]

{29}The court used the following factors to reach its conclusion that the documents lost their privilege through inadvertent disclosure:

> (1) the reasonableness of the precautions taken to prevent inadvertent disclosure in view of the extent of the document production; (2) the number of inadvertent disclosures; (3) the extent of the disclosure; (4) any delay and measure taken to rectify the disclosure; and (5) whether the overriding interests of justice would or would not be served by relieving a party of its error.[62]

The court concluded that the "balance of these factors weighs in favor of holding that ... Keystone ...waived any privilege that may have protected their attorneys' billing statements from disclosure."[63]

{30}As to the first factor, the court explained that Keystone's precautions were not reasonable since Keystone did not assert any privilege before it began producing documents.[64] Furthermore, according to the court, the second and third factors, which looked at the number and extent of disclosures, also support waiver. Although only two documents were actually in question, "the extent of the disclosure in these documents is complete."[65] Both documents contain the exact type of information that the other defendants were trying to get through their request for attorney billing statements. Therefore, despite the small number of documents, the extent of disclosure in those documents supports waiving the attorney-client privilege.

{31}The fourth factor, delay or measures taken to rectify disclosure, is not "significantly implicated" since the parties began arguing about waiver soon after the court ordered document production.[66] Finally, the fifth factor, which involved the interests of justice, also supports the conclusion that the Keystone documents lost their privilege through inadvertent disclosure. The goal of CERCLA is to make liable parties accountable for their share of cleanup costs. Discovery of evidence indicating that a party has dissipated assets in an attempt to avoid liability is contrary to that goal. Thus, the interests of justice require that Keystone's attorney-client privilege be waived for information regarding attorneys' billing statements that have been inadvertently disclosed.[67]

{32}The court concluded that the balance of the five factors resulted in a waiver of the attorney-client privilege for attorneys' billing statements in this case. Even though the privilege would normally have protected Keystone's documents, the inadvertent disclosure caused a waiver of the privilege.[68]

3. *Keystone III*

{33}In *Keystone III*[69] the court explained and clarified the *Keystone II* judgment. *Keystone III* reiterated that attorney billing statements are privileged if they reveal litigation strategy or the nature of the services performed. However, the *Keystone III* court explained that "it is the actual content of the document, rather than the type of document, that is privileged."[70]

{34}Since Keystone had revealed, albeit inadvertently, a category of information concerning Keystone's attorney communications, the attorney-client privilege was deemed waived regarding that particular category

of information.[71] *Keystone III* [72] reviewed the factors for waiver of the privilege through inadvertent disclosure, and affirmed the decision of *Keystone II*.[73]

4. *Keystone IV* and *Keystone V*

{35}In *Keystone IV*[74] the court used the printed e-mail messages as part of the evidence showing that Keystone was disposing of assets in an attempt to avoid paying its share of the CERCLA liability. [75] Finally, in *Keystone V*,[76] the court granted the defendants' cross-motions for summary judgment on the issue of whether the company who purchased Keystone Sanitation Company is liable for Keystone's CERCLA cleanup costs.[77]

B. *Evaluation*

1. Treat E-mail The Same As Other Documents

{36}*Keystone* is significant since it treats e-mail just like any other document, at least for purposes of the attorney-client privilege. The *Keystone* court allowed discovery of e-mail messages that were printed. Additionally, the court stated that the e-mail printouts would be protected by the attorney-client privilege, absent a waiver. Thus, according to *Keystone*, e-mail messages that have been printed out should be treated like any other document that contains information encompassed by the attorney-client privilege.

2. Unanswered Questions

{37}Although *Keystone* indicates that, at least in certain circumstances, e-mail messages will be treated like other documents for purposes of the attorney-client privilege, *Keystone* does not address whether e-mail is an acceptable means of communicating confidential information.

{38}The question never arose since the e-mails between Keystone Sanitation Company and its attorneys had been inadvertently disclosed as printouts rather than as electronic documents. Even though *Keystone* indicates that it is the information itself rather than the type of document that matters for purposes of the attorney-client privilege, the type of e-mail system used may affect whether e-mail is considered an acceptable method for communicating attorney-client information. Since *Keystone* dealt with printed e-mail messages, the type of e-mail system used was irrelevant because a printed e-mail message is just like any other document printed out on paper. E-mails that are still in electronic form, however, are not all the same. The security of e-mail often depends on the type of system used.[78]

{39}Regardless of the type of system, the safeguards and precautions utilized may also affect whether e-mail is considered an acceptable method of communication. *Keystone* does not address whether additional safeguards and precautions, such as encryption of e-mail messages, are required in order to protect confidential information sent by e-mail.

{40}Since the *Keystone* court treats e-mail the same as other documents for purposes of the attorney-client privilege, it may be inferred that the court considers e-mail a reasonable and acceptable method of communication between attorneys and clients. The e-mail messages dealt with in *Keystone,* however, had previously been printed and the printouts were inadvertently disclosed to third parties. Consider a situation in which a confidential e-mail message has not been printed out, but instead has been inadvertently disclosed to a third party while still in electronic form. It is not certain that *Keystone* would apply.

{41}*Keystone* did not involve, and the court did not address, the above situation in which an e-mail containing confidential information remains in electronic form and is inadvertently sent to a third party. However, the fact that an e-mail is still in electronic form should not prevent that e-mail from being

treated like any other document. According to *Keystone*, it is the content of the document, not the type of document, that is privileged.[79] E-mail messages that have been inadvertently disclosed while in electronic form should be evaluated using the same process the *Keystone* court used for the e-mail printouts: Is the information of a type that is protected by the attorney-client privilege? If so, do the five factors for waiver through inadvertent disclosure weigh in favor of waiving the privilege?[80]

{42}Ultimately, though *Keystone* treated the e-mail printouts like any other document for purposes of the attorney-client privilege, the case leaves many questions unanswered. *Keystone* does provide some support for the proposition that e-mail should be treated like conventional forms of communication. However, *Keystone* does not explain whether e-mail should be treated like other methods of communication in all situations, or only where the e-mail has been printed out. *Keystone*, therefore, clarifies only one aspect of the implications of e-mail for the attorney-client privilege. The other aspects must be derived from other sources, such as ABA opinions, state bar association opinions, the ECPA, and the limited number of other cases that have dealt with e-mail.

VI. THE CURRENT STATE OF THE LAW

A. *Case Law and the ECPA*

{43}The exact implications of e-mail for the attorney-client privilege are not completely clear. To the extent that the courts have dealt with e-mail, they often treat it in the same way that they treat other documents. The *Keystone* court treated e-mail printouts just like other documents for purposes of determining whether the attorney-client privilege was waived through inadvertent disclosure to a third party. Other courts have conducted *in camera* inspection of various documents, including e-mail messages, and have decided which documents were protected by the privilege and did not have to be disclosed.[81] This indicates that courts are treating e-mail messages like conventional documents when determining whether the documents are protected by the attorney-client privilege.

{44}The ECPA currently protects intercepted e-mail messages. The ECPA was passed to protect electronic communications.[82] Based on the ECPA, e-mail communications remain privileged even if those communications are illegally intercepted.[83] Since intercepting e-mail is illegal, and since intercepting e-mail does not result in the e-mail losing its privileged status, intercepted e-mail messages remain privileged despite the fact that a third party read them.

{45}Furthermore, since interception of electronic communications is prohibited under the ECPA, e-mail communications between attorneys and clients should be considered "reasonably" secure for purposes of the attorney-client privilege. Although the ECPA does not eliminate the possibility of illegal interception, it does make interception a crime.[84] Therefore, since criminal penalties ensue if messages are illegally intercepted, a person using e-mail should be able to rely on e-mail to provide a reasonable expectation of privacy. Simply because it is possible to illegally intercept communications, such as e-mail messages or telephone calls, does not mean that those methods of communication are automatically not acceptable for protection of the attorney-client privilege.[85]

B. *Ethical and Professional Responsibilities*

{46}The consensus among state bar associations is that e-mail is a reasonable and acceptable means of communication between attorneys and clients.[86] Even though the ABA and many state bar associations consider e-mail a reasonable and acceptable means of attorney-client communication, and even if courts treat e-mail messages just like other documents that may be protected by the attorney-client privilege, attorneys need to be aware of their ethical and professional responsibilities in relation to e-mail. An awareness of those responsibilities allows attorneys to make decisions that afford maximum protection of confidential information and communications.

1. Duty to Protect Confidential Information

{47}ABA Model Rule of Professional Conduct 1.6(a) states that "a lawyer shall not reveal information relating to representation of a client unless a client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation . . ."[87] Attorneys, therefore, have a duty to protect client information and to prevent confidential information from being revealed.[88]

2. Duty to Obtain Client Consent

{48}All attorneys have a duty to obtain client consent before revealing any confidential client information, regardless of the method of communication used.[89] Additionally, some state bar associations recommend that attorneys get client consent before sending confidential information by e-mail.[90] Not only is client consent one way to reduce the risk of malpractice liability,[91] obtaining client consent reduces the possibility of sacrificing the attorney-client privilege.[92] In order to obtain the client's consent, the attorney should discuss the attorney-client privilege with the client, explain the various methods of communication available, identify the risks associated with each method of communication, and determine if the client wishes to communicate by e-mail.[93]

3. Duty to Abide by the Client's Decision

{49}After discussing the attorney-client privilege with the client and obtaining the client's consent for specific methods of transmission, the attorney has a duty to follow the client's decision as to what methods of transmission may be used.[94] If a client wants to limit the type and/or amount of information transmitted by e-mail, for instance, the attorney must abide by those limitations.

4. Duty to Use Communication Methods that Afford a Reasonable Expectation of Privacy

{50}In addition to protecting confidential information, obtaining client consent prior to revealing confidential client information, and abiding by the client's decision, attorneys also have a duty to use methods of communication that afford a "reasonable expectation of privacy."[95] Thus, if the attorney is not sure of the privacy afforded by a particular e-mail system, he may be better off using a different method to transmit the information.[96] However, even though an e-mail system may not be absolutely secure,[97] it may still be used. As long as the system is deemed reasonably secure, it is an acceptable method of communicating client information.[98]

C. Safeguards

{51}Many state bar association opinions and bar journal articles indicate that e-mail is a reasonable and acceptable means of communication.[99] Still, until the courts declare e-mail a reasonable and acceptable method of communication, attorneys in all states must be aware of the safeguards that may be necessary in order to protect the attorney-client privilege.

1. Encryption

{52}Encryption involves using mathematical functions to code an e-mail message. The mathematical functions are then interpreted using a "key." The key ensures that the message is decoded only by the sender and the intended recipient. Unencrypted e-mail messages look like regular, readable text. By encrypting the e-mail and thereby putting it into a code, the message cannot be read unless the key is used to interpret the

code.[100]

{53}Although encryption will protect against inadvertent disclosure, encryption has some drawbacks. First, the sender and all receiving parties must utilize the same software.[101] Second, the keys must be programmed correctly in the sender's computer as well as in all recipients' computers in order for the encrypted message to be decoded and read.[102] Third, encryption programs take up a large amount of computer memory. Thus, a law firm with a number of attorneys using encryption on the same system may experience a network overload.[103] Fourth, since encryption programs tend to be expensive, clients and even some law firms may not be able to afford it.[104] Finally, even if all four of the previously discussed drawbacks are overcome, encryption still may not guarantee privacy since even the best available encryption systems can be "defeated."[105]

2. Disclaimer

{54}Including a disclaimer with each e-mail message may also protect the attorney-client privilege. A disclaimer lets the recipient know that the e-mail message contains confidential information and that if the e-mail is inadvertently sent to an unintended recipient, the e-mail should not be read, copied or forwarded.[106]

3. Digital Signature

{55}Digital signatures are another available option for protecting the attorney-client privilege. Digital signatures "authenticate the identity of senders and receivers; ... protect the integrity of the documents, insuring that [the] content has not been changed; and ... provide for encryption of documents and communications."[107]

4. Password

{56}Making attached documents accessible only through use of a password is another safeguard for protecting privileged documents.[108] The password prevents the document from being opened unless the recipient enters the correct password.

5. Common Sense

{57}Although encryption, disclaimers, and passwords may help protect confidential information sent by e-mail, attorneys should still use common sense when deciding whether to use e-mail to transmit information. "A profession that prides itself on confidentiality should be careful about utilizing modes of communication where the risk is difficult to assess."[109] If the attorney or client has any doubts about the security of the e-mail system used, it may be best to transmit the information through some method other than e-mail. Generally, the more confidential and sensitive the information is, the more protection it should be afforded. Until the courts set definitive guidelines for using e-mail to transmit confidential information, attorneys and clients may want to use a method other than e-mail to transmit highly confidential or highly sensitive information.[110]

{58}Attorneys should also take a few moments before sending an e-mail to double check the address to ensure that the message is going to the correct person.[111] Another precaution is to re-read the e-mail and think about what was written. E-mail should be treated like a letter or a memo. This means that attorneys should not allow the "informality" and "instantaneous nature" of e-mail to prompt them to express thoughts, opinions, or insights that they would not express in a letter or memo.[112]

D. *Conclusion*

{59}Although the law is not completely clear on exactly how to handle the attorney-client privilege within the context of e-mail messages, courts will be forced to address this issue in the future as it is likely that e-mail will continue to be used in the practice of law. The novelty and uncertainty surrounding the Internet may make electronic communications seem more risky than other forms of communication, such as telephones and faxes, that have been used in the past and are more commonplace. Since the risks are essentially the same, however, e-mail should not be treated any differently than postal mail, telephones, and faxes for purposes of the attorney-client privilege.

{60}Ultimately, no method of communication guarantees absolute confidentiality. E-mail, postal mail, telephone, and fax communications are not completely secure; each of them may be lost, intercepted, or inadvertently disclosed to an unintended third party. The security of e-mail messages largely depends on the type of system used [113] and on how careful the sender is about checking to make sure the address is correct.[114] The risk that information may be intercepted does not mean that e-mail messages should not be privileged. Postal mail, telephone conversations, and faxes are also susceptible to interception, but they remain privileged. E-mail should be treated the same way.[115]

{61}Courts may be wary of e-mail and the new technology involved with it. However, "[e]ach time new technology is introduced, the courts have been wary. Six hundred years ago, paper was rejected as a means of commerce, although it eventually replaced parchment for legal use."[116] Until the courts indicate acceptance of e-mail and declare it a "reasonably" secure method of communication for the protection of confidentiality, attorneys and clients should take precautions when using e-mail for confidential communications.

ENDNOTES

[*] Karen M. Coon earned a B.A. in English in 1999 from Indiana University of Pennsylvania, and will receive her J.D. in May 2002 from the University of Richmond School of Law. She is currently a Senior Staff Member of the Richmond Journal of Law and Technology. Ms. Coon would like to thank the Journal of Law and Technology staff members and Professor Deborah Tussey for providing editorial and critical reviews of her work.

[1]. 47 U.S.C. § 605 (1994).

[2]. 18 U.S.C. §§ 2510 - 2522 (1994).

[3]. United States v. Keystone Sanitation Co., 867 F. Supp. 275 (M.D. Pa. 1994) (hereinafter "*Keystone I*"); United States v. Keystone Sanitation Co., 885 F. Supp. 672 (M.D. Pa. 1994) (hereinafter "*Keystone II*"); United States v. Keystone Sanitation Co., 899 F. Supp. 206 (M.D. Pa. 1995) (hereinafter "*Keystone III*"); United States v. Keystone Sanitation Co., 903 F. Supp. 803 (M.D. Pa. 1995) (hereinafter "*Keystone IV*"); United States v. Keystone Sanitation Co., 1996 U.S. Dist. LEXIS 13651 (M.D. Pa. 1996) (hereinafter "*Keystone V*").

[4]. FED. R. CIV. P. 26(b)(1). *See also* FED. R. EVID. 501.

[5]. MODEL RULES OF PROF'L CONDUCT Rule 1.6(a) (1998). Rule 1.6(a) states, "a lawyer shall not reveal information relating to representation of a client unless a client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation."

[6]. David Hricik, *Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 470-71 (1998) (citing 8 WIGMORE ON EVIDENCE § 2292 at 554 (McNaughton rev. 1961)); *see also* Joshua M. Masur, Comment, *Safety in Numbers: Revisiting the Risks to Client*

Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail, 14 BERKELEY TECH. L.J. 1117, 1121 (1999) (quoting Wigmore). *Compare* Wigmore's statement of the elements of the attorney-client privilege, *with* Masur's statement of the elements of the attorney-client privilege, at 1121-22 (outlining the elements for the attorney-client privilege as articulated in Upjohn Co. v. United States, 449 U.S. 383, 394-395 (1981)), *and* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 118 (1998).

[7]. *In re* Horowitz, 482 F.2d 72, 81 (1973) (citing 8 WIGMORE ON EVIDENCE sec. 2291, *supra* note 6, at 554). *See also* State v. Canady, 460 S.E. 2d 677, 684 (W. Va. 1995) (stating that two policies are in conflict: "protect[ing] the integrity and fairness of the factfinding process by requiring full disclosure of all relevant facts connected with the impending litigation,....[and] promot[ing] full and frank consultation between a client and a legal advisor by removing the fear of compelled disclosure of information").

[8]. *See Upjohn*, 449 U.S. at 389 (citing 8 WIGMORE ON EVIDENCE sec. 2290, *supra* note 6, at 542); *see also* Heidelberg Harris, Inc. v. Mitsubishi Heavy Indus., No. 95-C0673, 1996 U.S. Dist. LEXIS 19274, at *27 (N.D. Ill. Dec. 18, 1996), United States v. Fisher, 692 F. Supp. 488, 490 (E.D. Pa. 1988), *In re* Grand Jury Investigation, 599 F.2d 1224, 1235 (3rd Cir. 1979).

[9]. *Upjohn*, 449 U.S. at 389. *See also* Gordon v. Newspaper Assoc. of Am., 51 Va. Cir. 183, 186 (2000) (explaining that the "privilege extends only to communications and not to facts" and a client "may not refuse to disclose any relevant fact within his knowledge merely because he incorporated a statement of fact into his communications to his attorney").

[10]. *Upjohn*, 449 U.S. at 390-91 (quoting ABA Code of Professional Responsibility, Ethical Consideration 4-1). *See also* Hickman v. Taylor, 329 U.S. 495, 511 (1947) (indicating that an attorney needs to have all relevant information in order to properly prepare the client's case).

[11]. *Upjohn*, 449 U.S. at 389 (quoting 8 WIGMORE ON EVIDENCE sec. 2290, *supra* note 6). Detailed discussion about waiver is beyond the scope of this note. For additional information and discussion about waiving the attorney-client privilege, see Amy M. Fulmer Stevenson, Comment, *Making a Wrong Turn on the Information Superhighway: Electronic Mail, the Attorney-Client Privilege and Inadvertent Disclosure*, 26 CAP. U.L. REV. 347, 359 (1997).

[12]. 18 U.S.C. §§ 2510- 2522 (1994).

[13]. 47 U.S.C. § 605 (1994).

[14]. 18 U.S.C. § 2511 (1994 & Supp. 1998).

[15]. 18 U.S.C. § 2511(1)(a) (1994).

[16]. 18 U.S.C. § 2517(4) (1994).

[17]. *See* Robert A. Pikowsky, *Privilege and Confidentiality of Attorney-Client Communications via E-mail*, 51 BAYLOR L. REV. 483, 485 (1999) (explaining that "the Internet is a 'network of networks'").

[18]. Hricik, *supra* note 6, at 465-66.

[19]. Electronic Records Management, 36 C.F.R. § 1234.2 (2000).

[20]. *See generally* Hricik, *supra* note 6, at 462-69 (discussing the history of the Internet, overview of programs usable over the Internet, and how the Internet transfers e-mail); *see generally* Craig D. Tindall, *E-mail Ethics*: *Privileged and Confidential Internet Communications*, 36 ARIZ. ATT'Y 10, 34 (Mar. 2000)

(explaining what "packets" are and how they are transmitted).

[21]. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 ¶ 18 (1999) (hereinafter "*ABA Formal Op. 99-413*"), *available at* http://www.abanet.org/cpr/fo99-413.html. *But cf.* Toby Brown, *Confidentiality on the Internet*, 12 S.C. LAW. 28 (arguing that the Internet does not afford a reasonable expectation of privacy); Masur, *supra* note 6, at 1119-20 (contending that the ABA's Formal Op. 99-413 is problematic because it "betray[s] the long-standing mandate that the attorney-client privilege ought to be treated as the exception to the general rule that all testimony should be admitted as evidence before the court," and because the Committee failed to base its conclusions on sound technological support).

[22]. *ABA Formal Op. 99-413*. Formal Op. 99-413 ¶ 18 explains that the process of sending e-mail is "virtually indistinguishable from the process of sending a fax," and that, as a result, intercepting faxes and e-mails requires "more effort and . . . sophistication" than eavesdropping on a telephone conversation via a telephone tap.

[23]. *ABA Formal Op. 99-413*, *supra* note 21 at ¶ 20 (explaining that the main relevant distinction between direct e-mail systems and private e-mail systems is the "greater risk of misdirected e-mails in a private system. Messages mistakenly may be sent throughout a law firm or to unintended recipients within the client's organization.").

[24]. Hricik, *supra* note 6, at 486-87. *See* State v. Canady, 460 S.E. 2d 677, 689 (W. Va. 1995) (indicating that internal e-mail messages may be privileged). *But see Keystone III*, 903 F. Supp. 803, 808 (M.D. Pa. 1995) (indicating that inadvertent disclosure does not automatically waive the attorney-client privilege) (citing *Keystone II*, 885 F. Supp. 672 (M.D. Pa. 1994)).

[25]. Hrick, *supra* note 6, at 487 (referring to Illinois State Bar Advisory Op. on Prof'l Conduct Op. No. 96-10 (May 16, 1997), and S.C. Ethics Advisory Op. 97-08 (June 1997), and pointing out that "any internal network is only as secure as the work stations having access to it."). *See also ABA Formal Op. 99-413*, *supra* note 21, at n.25 (1999).

[26]. *See* Hrick, *supra* note 6, at 487; *see also ABA Formal Op. 99-413*, *supra* note 21, at ¶ 22.

[27]. *See* Hricik, *supra* note 6, at 487.

[28].*See ABA Formal Op. 99-413*, *supra* note 21, at ¶ 24; *see also* Hricik, *supra* note 6, at 487. Even though on-line service providers are essentially public access networks that do not obligate users to maintain confidentiality, the attorney-client privilege may still protect information stored in private places, such as an e-mail mailbox. Fourth Amendment issues arise in conjunction with privately stored information. For a discussion of the relevant Fourth Amendment issues, *see* Pikowsky, *supra* note 17, at 529, and Hricik, *supra* note 6, at 478-79, 488, 490 n.172.

[29].18 U.S.C. § 2511(3)(a)-(b) provides that:

> (3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.
> (b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

18 U.S.C. § 2511(3)(a)-(b) (1994 & Supp. 1998).

[30]. *ABA Formal Op. 99-413, supra* note 21, at ¶¶ 27-33 (1999) (discussing Internet e-mail).

[31]. Lou Parker & Dave Gardner, *Technology: Using the Internet - Ethical, Privileged or Malpractice?*, 8 NEVADA LAW 20 (2000).

[32]. *See ABA Formal Op. 99-413*, *supra* note 21, at ¶ 30. For a detailed discussion of internet service providers, *see* Deborah M. McTigue, *Marginalizing Individual Privacy on the Internet*, 5 B.U.J. SCI. & TECH. L. 5 (1999).

[33]. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 112 cmt. d (Tentative Draft 1998). *See ABA Formal Op. 99-413*, *supra* note 21.

[34]. Pikowsky, *supra* note 17, at 579 (stating that "the existence of a reasonable expectation of privacy permits an attorney to discuss client confidences via e-mail without violating the ethical duty to safeguard those confidences.").

[35]. ACLU. v. Reno, 929 F. Supp. 824, 834 (E.D. Pa. 1996), *aff'd* 521 U.S. 844 (1997) ("One method of communication on the Internet is via electronic mail, or 'email,' comparable in principle to sending a first class letter. One can address and transmit a message to one or more other people. Email on the Internet is not routed through a central control point, and can take many and varying paths to the recipients. Unlike postal mail, simple email generally is not "sealed" or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)"). *See also* Hricik, *supra* note 6, at 481 (discussing e-mail and postal mail). For an in-depth discussion of ACLU. v. Reno, *see* Dharmesh S. Vashee, Note, *ACLU v. Reno: Congress Places Speed Bumps on the Information Superhighway*, 6 RICH. J.L. & TECH. 16 (1999), *at* http://www.richmond.edu/jolt/v6i3/note4.html.

[36]. ACLU v. Reno, 929 F. Supp. at 834.

[37]. *See* Craig D. Tindall, *E-mail Ethics*: *Privileged and Confidential Internet Communications*, 36 ARIZ. ATT'Y 10, 34 (Mar. 2000); Brian D. Wassom, *A Reasonable Expectation of Privacy: Can Michigan Attorneys Safely Use Unencrypted Internet E-Mail for Confidential Communications?*, 78 MICH. B.J. 590, 590 (1999).

[38]. *See* Wassom, *supra* note 37, at 590 (explaining that it is difficult for eavesdroppers to intercept e-mails since they "must know exactly what they are looking for and when it will be transmitted, and be fortunate enough to both guess the path that the messages will take and discover the packets with significant information").

[39]. *ABA Formal Op. 99-413, supra* note 21, at ¶ 10. *See also* Hricik, *supra* note 6, at 479 (stating that " [t]raditional land-line telephone conversations are confidential... because such communications are made under circumstances that reasonably ensure their confidentiality").

[40]. *See ABA Formal Op. 99-413*, *supra* note 21, at ¶ 7; s*ee also* State v. Canady, 460 S.E.2d 677, 689-90 (W. Va. 1995) (quoting *Upjohn*, 449 U.S. 383, 388 (1981), and concluding that both e-mail and fax are privileged).

[41]. *ABA Formal Op. 99-413*, *supra* note 21, at ¶ 18 (explaining that the process of sending e-mail is "virtually indistinguishable from the process of sending a fax," and that, as a result, intercepting faxes and e-mails requires "more effort and technical sophistication" than eavesdropping on a telephone conversation via a telephone tap).

[42]. Hricik, *supra* note 6, at 485 and n.154.

[43]. *See* Tindall, *supra* note 37, at 34 (explaining that e-mail messages are "most vulnerable to security breaches" right before and right after transmission since the message "resides in at least two computers" when it is sent and when it is received).

[44]. *See*, *e.g.*, Steven A. Heinrich & Roxana Dastur Malladi, *News of the Wired: Security, the Internet and the Networked OfficeBProblems for Law Offices*, 56 OR. ST. B. BULL. 15, 18 (1995) (stating that "[m]any people believe that if you 'delete' a file from a floppy disk, it is gone forever").

[45]. This is assuming that the unintended recipient has a fax machine hooked up to the phone line dialed.

[46]. For additional information about the similarities and differences between faxes and e-mails, *see ABA Formal Op. 99-413*, *supra* note 21, at ¶ 15.

[47]. Malvern U. Griffin & Aaron P. Maurer, *Netethics: Concerns Regarding E-mail and World Wide Web Use by Attorneys*, 59 ALA. LAW. 44 (1998).

[48]. Richard M. Georges, *The Impact of Technology on the Practice of Law - 2010*, 71 FLA. B.J. 36, 38 (1997).

[49]. Stevenson, *supra* note 11, at 350.

[50]. *Keystone I*, 867 F.Supp. 275 (M.D. Pa. 1994).

[51]. *Id*. at 279. Although there were numerous counterclaims, basically the counterclaims involved "judicial review of certain actions taken by the EPA, the [Pennsylvania Hazardous Sites Cleanup Act], and recoupment." The applicable CERCLA section can be found at 42 U.S.C. § 9607 (1994).

[52]. *Id*. at 284.

[53]. *Keystone II*, 885 F. Supp. 672 (M.D. Pa. 1994).

[54]. *Id*. at 675.

[55]. *Id*.

[56]. *Id*.

[57]. *Id*. Keystone also claimed that these documents were protected by the work-product doctrine. The work-product doctrine is beyond the scope of this case note. For information on the work-product doctrine, see Fed. R. Civ. P. 26(b)(3) and Hickman v. Taylor, 329 U.S. 495 (1947).

[58]. *Keystone II*, 885 F. Supp. at 676.

[59]. *Id*. at 675.

[60]. *Id*.

[61]. *Id*. at 676.

[62]. *Id*.

[63]. *Keystone II*, 885 F. Supp. at 676.

[64]. *Id*.

[65]. *Id*.

[66]. *Id*. The court noted that document production was ordered by the court on August 26, 1994, and that the parties began arguing about waiver in early September.

[67]. *Keystone II*, 885 F. Supp. at 676.

[68]. *Id*.

[69]. *Keystone III*, 899 F. Supp. 206 (M.D. Pa. 1995).

[70]. *Id*.

[71]. *Id*.

[72]. *Id*.

[73]. *Id*. at 208.

[74]. *Keystone IV*, 903 F. Supp. 803 (M.D. Pa. 1995).

[75]. *Id*. at 811-12.

[76]. 1996 U.S. Dist. LEXIS 13651 (M.D. Pa. 1996).

[77]. *Id*. The court explained that it will "require Keystone's assets to be looked to first to satisfy its portion of CERCLA liability." *Id*. at *44.

[78]. *See supra* Part IV.B.

[79]. *Keystone III*, 899 F. Supp. 206, 207 (M.D. Pa. 1995).

[80]. *Keystone II*, 885 F. Supp. 672, 675-76 (M.D. Pa. 1994).

[81]. Heidelberg Harris, Inc. v. Mitsubishi Heavy Indus., No. 95-C0673, 1996 U.S. Dist. LEXIS 19274, at *7 (N.D. Ill. Dec. 18, 1996).

[82].18 U.S.C. §§ 2510-2533 (1994). For a discussion of the ECPA, see *supra* Part III.

[83]. Hricik, *supra* note 6, at 471. *See* 18 U.S.C. § 2517(4) (1994) (stating that otherwise privileged communications remain privileged even if intercepted).

[84].Various states also have laws making interception a crime. *See, e.g.*, GA. CODE ANN. § 16-11-62 (1999 & Supp. 2000); UTAH CODE ANN. § 77-23a-4 (1999); Neb. Rev. Stat. § 86-702 (1999).

[85]. *ABA Formal Op. 99-413*, *supra* note 21, at ¶ 3 (stating that "[i]t is not...reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible").

[86]. *See*, *e.g.*, AK Bar Ass'n Ethics Op. 98-2 (1998) (stating that "a lawyer may ethically communicate with a client on all topics using electronic mail"); AZ Op. 97-04 (Apr. 7, 1997), *available at* http://www.legalethics.com/ethics.law?state=Arizona#opinions (allowing the use of e-mail to communicate with clients, but recommending that encryption or other precautionary measures be taken); KY Op. E-403 (July 1998), *available at* http://www.uky.edu/Law/kyethics/opinions/kba403.htm (authorizing the transmission of unencrypted e-mail); S.C. Ethics Advisory Op. 97-08 (1997), *available at* http://www.scbar.org/apps/reference/EthicsOpinions/ethicsopinion.dbm?OpinionID=97%2D08&OpinionType=ethics (concluding that the "[u]se of electronic mail will not affect the confidentiality of client communications). For links to state ethics opinions, see *LegalEthics.com: Internet Legal Services*, *at* http://www.legalethics.com/ethics.law (last visited Oct. 1, 2000). For links to all state bar associations, see *State Bar Ass'ns*, *at* http://www.bestcase.com/statebar.htm (last visited Oct. 1, 2000). For an extensive list of bar association opinions e-mail and encryption, see *ABA Formal Op. 99-413*, *supra* note 21, at n. 40.

[87]. MODEL RULES OF PROF'L CONDUCT, *supra* note 5.

[88]. "It should be noted that a lawyer's negligent use of any medium - including the telephone, mail and fax - may breach the duty of confidentiality." *ABA Formal Op. 99-413*, *supra* note 21, at n.6.

[89]. MODEL RULES OF PROF'L CONDUCT, *supra* note 5. Rule 1.6(a) states: "a lawyer shall not reveal information relating to representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation." *Id. See also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS, *supra* note 6, at § 112(1)(a) (stating that "the lawyer may not use or disclose confidential client information . . . if there is a reasonable prospect that doing so will adversely affect a material interest of the client or if the client has instructed the lawyer not to use or disclose such information").

[90]. *See* Griffin, *supra* note 47, at 47; Evan R. Shirley, *Dilbert, Supermodels & Confidentiality of E-mail Under Hawaii Law*, 3 HAWAII B.J. 6, 10-11 (1999); Wassom, *supra* note 37, at 593.

[91]. Wassom, *supra* note 37, at 593.

[92]. Griffin, *supra* note 47, at 47.

[93]. Shirley, *supra* note 90, at 11.

[94]. MODEL RULES OF PROF'L CONDUCT R. 1.2(a) (1999). *Compare* MODEL RULES OF PROF'L CONDUCT R. 1.2(a) (1999) (stating that "a lawyer shall abide by a client's decisions concerning the objectives of representation...and shall consult with the client as to the means by which they are to be pursued"), *with* Model Rules of Prof'l Conduct R. 1.2(a) (Proposed Rule 2000), *available at* http://www.abanet.org/cpr/rule12.html (stating that "a lawyer shall abide by a client's decisions concerning the objectives of representation and may take such action on behalf of the client as is impliedly authorized to carry out the representation").

[95]. *ABA Formal Op. 99-413*, *supra* note 21, at ¶ 6; *see also* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS sec. 112 cmt. d (Tentative Draft 1998) (explaining that confidential client information must be "acquired, stored, retrieved, and transmitted under systems and controls that are reasonably designed and managed to maintain confidentiality").

[96]. "Particularly strong protective measures are warranted to guard against the disclosure of highly sensitive matters. Those measures might include the avoidance of e-mail, just as they would warrant avoidance of the telephone, fax, and mail." *ABA Formal Op. 99-413*, *supra* note 21, at ¶ 5.

[97].*See* Heinrich, *supra* note 44, at 16 (stating that "no system is completely impenetrable").

[98]. *See ABA Formal Op. 99-413*, *supra* note 21, at ¶ 3 (stating that "[i]t is not . . . reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible"); Shirley, *supra* note 90 (explaining that "lawyers are not obligated to use every available means of insuring that confidential communications are not intercepted"); Tindall, *supra* note 37, at 33 (noting the ABA has opined that "[m]ethods used to communicate with clients . . . need not offer absolute privacy, but only reasonable privacy").

[99]. *See State Bar Ass'n* opinions, *supra* note 85.

[100]. Stevenson, *supra* note 11, at 353-54; Pikowsky, *supra* note 17, at 564 (providing background information about encryption and how encryption works); Daniel E. Orr, *Confidentiality in an Electronic World Using Encryption in Everyday Law Practice*, ABA LAW PRACTICE TODAY, (2000), *available at* http://www.abanet.org/lpm/newsarticle11130_front.shtml (last visited October 8, 2000). For general information about encryption and about an Internet company that provides security and encryption services for attorneys and law firms, see www.jdusa.net. For more information on encryption, see Steven Levy, *Crypto: How They Beat Big Brother*, NEWSWEEK, Jan. 15, 2001, at 42.

[101]. Wassom, *supra* note 37, at 590. *See generally*, Georges, *supra* note 48, at 38 (providing information about PGP (Pretty Good Privacy), an encryption software package). For more information about PGP, *see* www.pgp.com.

[102]. Wassom, *supra* note 37, at 590.

[103]. *Id*.

[104]. *Id*.

[105]. *Id*. at 590-91.

[106]. Griffin, *supra* note 47, at 47. Griffin & Maurer provide an example of a disclaimer:

> **Notice**: This Electronic Mail (e-mail) contains confidential and privileged information that is intended only for the individual or party identified directly below, and not necessarily the addressee. Do *not* read, copy or forward this e-mail unless you are the intended recipient. If you are not the intended recipient, please call **firm name** at **phone number** and ask for **sender**. In addition please return this e-mail using a reply command and then delete all copies. Thank you.

See also Wassom, *supra* note 37, at 592-93; Tindall, *supra* note 37, at 35-36.

[107]. Toby Brown, *Confidentiality on the Internet*, 12 S.C. LAW. 28, 29 (2000).

[108]. *See* Wassom, *supra* note 37, at 593.

[109]. Brown, *supra* note 107, at 29.

[110]. *See ABA Formal Op. 99-413*, *supra* note 21 (stating that a method other than e-mail should be used "when the lawyer reasonably believes that confidential client information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted"); Tindall, *supra* note 37, at 36 (stating that "[e]-mail should not be used to convey highly sensitive information). *See also* Wassom, *supra* note 37, at 593 (exploring the importance of "heightened attorney awareness and common-sense precautions).

[111]. Wassom, *supra* note 37, at 593; Stevenson, *supra* note 11, at 373.

[112]. Shirley, *supra* note 90, at 9. *See also* Thomas R. Haggard, *Legal Writing in the Electronic Age*, 11 S.C. LAW 12 (1999) (recommending that attorneys "pretend that [e-mail messages are] still going out under the letterhead of the firm").

[113]. For further discussion of direct e-mail, private e-mail, on-line service providers, and internet e-mail systems and the risks inherent in each system, see *ABA Formal Op. 99-413,* at ¶ 17; see *supra* Part IV B.

[114]. *See* Hricik, *supra* note 6, at 496 (explaining that the "potential for misdirecting an e-mail appears no greater than that of misdirecting a fax").

[115]. *See* Peter R. Krakaur, *Treat E-mail Like Other Communications: An Argument Against Mandatory Encryption of Attorney-Client Communications* (Jan. 1, 1998), *at* http://www.llrx.com/features/e-mail.htm. *See generally ABA Formal Op. 99-413*, *supra* note 21, at ¶¶ 3, 35-36 (explaining that the possibility of interception of e-mail, does not make e-mail an unreasonable method of communication); Hricik, *supra* note 6, at 485 (arguing that using a fax machine, even though it is possible for a fax to be misdirected or intercepted, does not destroy the privilege).

[116]. Hricik, *supra* note 6, at 507.

Related Browsing

1. http://cyber.lp.findlaw.com/privacy/attorney_client.html. Findlaw, Cyberspace Law Center, Privacy, Attorney-Client Privilege. An index page that lists several articles on different aspects of attorney-client privilege in email communications. Also lists articles discussing discovery and email documents.

2. http://www5.law.com/tx/today00/ethics0920.htm. Seminar discussion among academics and practitioners discussing the practical consideration of communicating by email with clients.

3. http://www.bamsl.org/lpm/email.htm. Bar Association of Metropolitan Saint Louis, Law Practice Management Committee. Article by practicing attorney titled "Email and the Attorney-Client Privilege." The article applies traditional evidence rules to the relatively new communication form of email.

4. http://cyber.lp.findlaw.com/privacy/attorney_client.html. America's Law Links, Resource Center, Ethics and Professional Responsibility, Attorney/Client Relations. Includes a variety of articles on the attorney-client privilege in general and several articles on email and the attorney-client privilege.

5. http://www.agin.com/aigc/tic51.html. Compliance: The Attorney-Client Privilege by J. Alden Lincoln. It often becomes necessary for company officials to confide very sensitive information to legal counsel in the course of obtaining legal advice.

6. http://www.kuesterlaw.com/netethics/bjones.htm. Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail by Robert L. Jones. Article on attorney's duties to protect client disclosures in electronic media from hackers.

7. http://www.marinlaw.net/confidentiality/confidentiality.html. Cyber Security, Confidentiality & Encryption. Checklist of issues, resources, articles and tools on the issues of security and confidentiality.

8. http://albany.bcentral.com/albany/stories/1998/10/26/focus5.html. New-age Communications Can Thwart Attorney-client Privilege by Andrew C. Rose. Discusses how attorney-client privilege may be waived when information is communicated via cell phone, voice mail, e-mail and other electronic communications.

9. http://www.bamsl.org/lpm/email.htm. E-Mail and the Attorney-Client Privilege by Arhtur L. Smith. Discusses whether e-mail communications may be protected by attorney-client privilege.

10. http://www.infowar.com/law/99/law_030999a_j.shtml. E-Mail and the Attorney-Client Privilege on Infowar.com. Reviews whether e-mail is a secure enough medium to be considered for attorney client privilege protection.

11. http://www.sw.com/acpriv.htm. Internet E-Mail and the Attorney-Client Privilege by Todd H. Flaming. The author argues that even unencrypted e-mail messages between lawyers and clients should be subject to the attorney-client privilege.

12. http://www.gdf.com/online.htm. Communicating with Clients On-Line: Confidentiality, Privilege and Authenticity by Peter D. Kennedy. Discusses issues of attorney-client privilege as regards e-mail communication and offers suggestions on how to communicate with clients via e-mail without waiving the privilege status.
