

Opinion #195: Client Confidences: Communications with clients by unencrypted e-mail

Issued by the Professional Ethics Commission

Date Issued: June 30, 2008

Question

Bar Counsel has requested a formal opinion on the following question:

Is it a violation of Maine Bar Rule 3.6(h) (confidentiality of information) for an attorney to communicate with clients by unencrypted e-mail.

Opinion

The Commission concludes that, as a general matter and subject to appropriate safeguards, an attorney may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain client confidentiality.

Bar Rule 3.6(h)(1) provides that “a lawyer shall not, without informed consent, knowingly disclose” confidential information “except as permitted by these rules, or when authorized in order to carry out the representation, or as required by law or by order of the court.” Whether in paper or e-mail form, much correspondence between attorneys and clients is obviously confidential under Rule 3.6(h)(1).

In 1999, the American Bar Association Standing Committee on Ethics and Professional Responsibility (ABA) issued Formal Opinion No. 99-413, providing a comprehensive analysis of the obligations of lawyers regarding e-mail communication under the Model Rules of Professional Conduct.^[1] The opinion discusses the risks of disclosure inherent in many of the forms of communication available today to attorneys and their clients, including different e-mail technologies.^[2] Internet e-mail was considered to be the least secure, although of course it is the most common method of e-mail transmission. The ABA concluded that lawyers had:

“a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure.”

In reaching this conclusion, the ABA relied on both law and science for reasons that remain relevant today. Federal law criminalizes unauthorized interception or disclosure of e-mail in transit or storage and strictly regulates the rights of internet service providers (ISPs), through whose computers internet e-mail passes, to inspect traffic.^[3] In addition, the electronic process of sending e-mail divides individual transmissions into fragments of information, each of which follows a different path through the internet before being reassembled on the receiver's computer. In view of the federal legal prohibitions and the technological difficulties of intercepting more than a fragment of any communication, the ABA concluded that there was a reasonable expectation of privacy in unencrypted e-mail.

Most other jurisdictions that have considered this question have arrived at the same conclusion.^[4] Opinions to the contrary have noted the possibility of interception despite these legal and technological safeguards and

have advised attorneys to either obtain informed consent from clients or use encryption prior to sending confidential information by e-mail. ^[5]

The Commission finds the reasoning in the ABA and majority opinions to be persuasive and hence concludes that an attorney generally may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain client confidentiality, subject to the caveats discussed below.

The Commission, however, notes that Maine Bar Rule 3.6(a) sets forth a general standard requiring lawyers to "employ reasonable care and skill and apply the lawyer's best judgment in the performance of professional services." When exercising professional judgment in choosing a particular form of communication, lawyers should consider both the content of the communication as well as the security of the email address to which it is being sent. For example, an attorney representing a client in a divorce would generally not send sensitive advice in a letter to the client's home address if the couple had not yet separated. Similarly, lawyers should be sensitive to the fact that others may have access to a client's e-mail address, especially at home. Likewise, some places of business routinely monitor their employees' e-mail and often have access to it.

Of greater concern is the prospect of misaddressed email or that which is replied "to all" in response to a broadcast email when some of the original recipients are not intended to receive the reply. ^[6] However, that potential problem must be dealt with through the routine application of diligence and is not corrected by use of encrypted email. Finally, since e-mail interception, though unlikely, is a possibility, attorneys should employ reasonable judgment in selecting a means of communication other than the internet when the information is of such a highly confidential nature that disclosure would result in significant damage to the client's interests.

While it is impractical to try to fashion precise rules concerning email conduct geared to specific circumstances and ever-changing technology, as general guidance attorneys should discuss with clients their preferred method(s) of communication and follow the client's wishes, should consider the degree of confidentiality of particular information in determining appropriate means to send it, and should take reasonable precautions to make sure that the address is correct and properly targeted. With these general cautions in mind, and noting that reasonable judgment may require additional safeguards depending upon the circumstances, an attorney may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain the confidentiality of client information. ^[7]

Footnotes

^[1] Model Rule 1.6 provides that "a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent."

^[2] The opinion discusses postal service and commercial mail systems, landline telephones, cordless and cellular phones and facsimile, in addition to e-mail.

^[3] See 18 U.S.C. §§ 2510 et. seq.

^[4] See for example Ohio Ethics Opinion No. 99-2 (April 9, 1999), Hawaii Ethics Opinion No. 40 (April 26, 2001), Utah Ethics Opinion No. 00-01 (March 9, 2000), Florida Ethics Opinion No. 00-4 (July 15, 2000), Delaware Ethics Opinion No. 2001-2 (2001), Virginia Ethics Opinion No. 1791 (December 22, 2003), and the other authorities set forth in footnote 40 of ABA Formal Opinion No. 99-413.

^[5] See Iowa Bar Ass'n. Op No. 1997-1 (1997). Missouri Bar Disciplinary Counsel requires lawyers to notify all recipients of e-mail that (1) e-mail communication is not a secure method of communication; (2) any e-mail that is sent may be copied and held by various computers it passes through; and (3) persons not participating in a communication may intercept it by improperly accessing a computer through which email has passed.

^[6] For example, if an attorney sends her client a copy of an email to opposing counsel, that client may inadvertently also receive a copy of a reply "to all" from opposing counsel. In addition to the simple miscommunication, this could implicate Bar Rule 3.6(f), which prohibits communication with a represented party.

^[7] Since non-lawyer staff may participate in client communications, attorneys should be aware of Maine Bar Rule 3.13(c) as regards training non-lawyer staff on office policies and any specific constraints relevant to a particular client. See for reference Opinion #134.