REPORT OF THE COMMITTEE ON ETHICS*

In response to the growing use of electronic mail (e-mail) by attorneys to communicate with clients and co-counsel, the American Bar Association (ABA), as well as several state bar associations, have recently addressed whether transmission of confidential information by unencrypted e-mail violates the confidentiality rules of the legal profession. The position of the ABA and most state bars that have considered the question is that unencrypted e-mail communications generally do not violate the confidentiality rules, but that additional safeguards may be required for particularly sensitive information. A few state bar associations, however, have concluded that attorneys must either: (1) encrypt their e-mail messages; or (2) inform their clients of the disclosure risks and obtain client consent. Because this is a new and developing area of ethics law, attorneys should consult the ethics rules, opinions, and relevant statutes in the jurisdiction(s) in which they practice.

I. BACKGROUND

E-mail encompasses a variety of technologies that allow computer users to communicate with one another. There are essentially four types of e-mail, each of which presents slightly different concerns with respect to the confidentiality of the communications. First, "direct" e-mail involves sending a message from one computer to another. The sender's modem converts the message into digital information that is sent over the telephone lines to the recipient's modem, where it is reassembled. This process is nearly identical to sending a fax. Second, "private system" e-mail allows multiple users to send messages directly to each other—this is the system employed in most internal corporate e-mail systems. The messages are sent over telephone lines and do not go through any publicly accessible network. Third, on-line services providers (OSPs), such as America Online, are third-party commercial services that operate a network and provide subscribers with password-protected mailboxes from which they may send and receive e-mail. Fourth, Internet e-mail allows messages to be sent over the Internet without the involvement of OSPs. Such messages typically travel over the phone lines and pass through several Internet service providers (ISPs) who use computers to send the messages to their next destination.

II. THE ABA POSITION

In ABA Formal Opinion 99-413, the ABA Standing Committee on Ethics and Professional Responsibility (the ABA Committee) addressed the obligations of attorneys under the Model Rules of Professional Conduct when using e-mail to communicate with clients or third parties about client matters.[1] The ABA Committee opined that the applicable ethics rule is Model Rule 1.6(a), which prohibits disclosure of confidential client information absent client consent.[2]

---

* The Committee gratefully acknowledges the assistance of Jacqueline Gerson Cooper, Esq. of Sidley & Austin in the preparation of this report.

1. ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413 (1999). In this opinion, the ABA Committee declined to take a position regarding the use of cellular or cordless telephones to communicate confidential client information.

2. Model Rule 1.6 provides:

(a) 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

The ABA Committee stated that the duty under Model Rule 1.6(a) to protect client confidences requires that an attorney choose methods of communication in which the attorney has a reasonable expectation of privacy. The expectation of privacy need not be absolute—just reasonable.

Applying this "reasonable expectation of privacy" test, the ABA Committee concluded that, in most circumstances, communication by e-mail affords a reasonable expectation of privacy from a technological and legal standpoint. In reaching this conclusion, the ABA Committee compared e-mail to other methods of communication that attorneys commonly use, such as United States mail, commercial mail, telephone, and fax. All of these traditional methods of communication involve some risk of interception or unauthorized disclosure. United States and commercial mail, for example, can be lost or stolen. Additionally, mail services often reserve the right to open and inspect the contents of letters and packages. Similarly, telephone calls are subject to eavesdropping and wiretapping. Phone companies can also monitor phone calls in certain circumstances. Faxes, of course, can be misdirected and are often accessible to people other than the intended recipient, such as secretaries and mail room employees. The ABA Committee noted, however, that it is uniformly accepted that these traditional methods of communication do not violate the duty of confidentiality because they afford a reasonable expectation of privacy.

Although e-mail presents some unique risks of disclosure and interception, the ABA Committee concluded that these risks are no greater than with traditional methods of communication. For example, direct e-mail can be "tapped," because it is transmitted over the phone lines. This risk is less than with telephone calls, however, because the information travels in digital form, and requires greater effort and technical expertise to perform an effective "tap." Private system e-mail can be misdirected within a law firm or organization, but this risk to confidentiality is essentially no greater than with faxes.

E-mail that is sent via the Internet or third-party services presents additional security issues for two reasons: (1) the messages can be inspected by OSP and ISP administrators; and (2) there is some risk that unauthorized "hackers" or dishonest OSP and ISP employees can intercept the messages. The ABA Committee concluded that these risks do not render the expectation of privacy less reasonable. As a practical matter, unauthorized interception of these types of e-mail requires a much greater degree of technical sophistication than a wire tap. This is particularly true of Internet e-mail messages, which ordinarily are split into several "packets" of information and travel complex routes through many phone

---

representation, and except as stated in paragraph (b).

(b) A lawyer may reveal such information to the extent the lawyer reasonably believes necessary:

(1) to prevent the client from committing a criminal act that the lawyer believes is likely to result in imminent death or substantial bodily harm; or

(2) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client.

MODEL RULES OF PROFESSIONAL CONDUCT Rule 1.6 (1995).

lines and ISPs. Moreover, pursuant to the Electronic Communications Privacy Act of 1986, as amended in 1994 (the ECPA), the unauthorized interception of e-mail is a crime.[3] Similarly, while OSP and ISP administrators can lawfully inspect e-mail, this right is limited by the ECPA to purposes that are "a necessary incident to the rendition" of their services or to the protection of the "rights or property" of the service provider. Monitoring or disclosure for any other purpose is prohibited.[4] Accordingly, the ABA Committee concluded that attorneys have a reasonable expectation of privacy in communication by all forms of e-mail.

The ABA Committee cautioned, however, that an attorney still has an obligation to consider whether special measures are warranted when the confidential information is highly sensitive or the consequences of disclosure would be costly. In such circumstances, the attorney should consult with the client and follow the client's instructions as to whether another mode of delivery, such as private courier, is preferred.

III. STATE BAR OPINIONS

Most state bar opinions are in accord with the ABA opinion. Several state bars have opined that the use of unencrypted e-mail generally does not give rise to any ethical concerns, but that greater precautions may be required in certain circumstances. For example, the District of Columbia bar has held that in most circumstances, transmission of confidential information by electronic mail is acceptable and does not violate the District of Columbia's confidentiality rules, but that higher levels of security may be required for sensitive information.[5] A few state bar associations have imposed additional obligations on attorneys using e-mail. The position of the Pennsylvania bar is that attorneys should advise clients of the risks of using unencrypted e-mail and obtain the client's written or oral consent.[6] The opinion also recommends that attorneys place a notice on client e-mail warning that it is a privileged and confidential communication. Similarly, the Arizona bar suggests that attorneys encrypt e-mail communications with cli-

3. 18 U.S.C. §§ 2511, 2701-02 (1994).

4. 18 U.S.C. § 2511(2)(a)(i).

5. D.C. Bar Op. No. 281 (Feb. 18, 1998). *See also* Minnesota Lawyers Professional Responsibility Bd., Op. No. 19 (Jan. 22, 1999) (applying Minnesota confidentiality rules); Ohio Bd. of Comm'rs on Grievances and Discipline, Op. No. 99-2 (Apr. 9, 1999) (applying Ohio law); Alaska Bar Ass'n Ethics Comm., Op. No. 98-2 (Jan. 16, 1998) (applying Alaska confidentiality rules; encouraging the use of encryption software or other safeguards for sensitive information); New York State Bar Ass'n Comm. on Professional Ethics, Op. No. 709 (Sept. 16, 1998) (applying New York confidentiality rules; attorneys who use Internet e-mail should stay abreast of technological developments to assess any changes in the likelihood of interception and the availability of technologies that may reduce this risk); Kentucky Bar Ass'n Ethics Comm., Advisory Op. No. E-403 (1998) (applying Kentucky confidentiality rules); Illinois State Bar Ass'n Advisory Opinion on Professional Conduct, No. 96-10 (May 16, 1997) (applying Illinois confidentiality rules); South Carolina Bar Ethics Advisory Comm., Op. No. 97-08 (June 1997) (applying South Carolina confidentiality rules); North Dakota State Bar Ass'n Ethics Comm., Op. No. 97-09 (1997) (applying North Dakota confidentiality rules); Vermont Advisory Ethics Op. No. 97-5 (1997) (applying Vermont's confidentiality rules).

6. Pennsylvania Bar Ass'n Comm. on Legal Ethics and Professional Responsibility, Informal Op. No. 97-130 (Sept. 26, 1997).

ents and caution clients about transmitting sensitive information by e-mail.[7] The Arizona bar also concluded that e-mail transmissions should include a cautionary statement indicating that the content is "confidential" or "attorney/client privileged." The North Carolina bar also concluded that attorneys must advise clients of the risks that e-mail will be intercepted.[8] Lastly, the Iowa bar has stated that an attorney must either obtain the written consent of the client to communicate sensitive material via e-mail or ensure that the communications are encrypted or protected by an equivalent security system.[9]

IV. CONCLUSION

Although a few state bars require attorneys to obtain client consent or encrypt e-mail, the clear majority view, recently adopted by the ABA, is that attorneys can communicate by unencrypted e-mail without obtaining client consent in most circumstances. This view is based on the rationale that no means of communication, including accepted means such as the mail, telephones, and faxes, is absolutely secure and that e-mail affords a reasonable expectation of privacy because interception of e-mail is technologically difficult as well as illegal.

Attorneys, however, are ultimately responsible for assessing the risks of using e-mail in particular situations. In some situations, including situations where an attorney normally would avoid using the mail, telephones, or faxes, the prudent course of action likely would be to avoid e-mail as well.

COMMITTEE ON ETHICS

Carl W. Ulrich, Chair
Eugene R. Elrod, Vice Chair

Ann L. Fisher
James N. Horwood
Stephen E. Williams

7. State Bar of Arizona's Comm'n on the Rules of Professional Conduct, Advisory Op. No. 97-04 (Apr. 7, 1997).

8. North Carolina State Bar, Ethics Op., RPC 215 (July 21, 1995).

9. Iowa Bar Ass'n, Op. No. 96-1 (Aug. 29, 1996).