The Supreme Court of Ohio

BOARD OF COMMISSIONERS ON GRIEVANCES AND DISCIPLINE

41 SOUTH HIGH STREET-SUITE 3370, COLUMBUS, OH 43215-6105
(614) 644-5800 FAX: (614) 644-5804

OFFICE OF SECRETARY

OPINION 99-2

Issued April 9, 1999

[CPR Opinion-provides advice under the Ohio Code of Professional Responsibility which is superseded by the Ohio Rules of Professional Conduct, eff. 2/1/2007.]

SYLLABUS: A lawyer does not violate the duty to preserve confidences and secrets under DR 4-101 of the Ohio Code of Professional Responsibility by communicating with clients through electronic mail without encryption. An attorney must use his or her professional judgment in choosing the appropriate method of each attorney-client communication.

OPINION: This opinion addresses whether it is ethically proper under the Ohio Code of Professional Conduct for a lawyer to communicate with clients through electronic mail without encryption.

> Does a lawyer violate the duty to preserve confidences and secrets under DR 4-101 of the Ohio Code of Professional Responsibility by communicating with clients through electronic mail without encryption?

Electronic mail communication is referred to as e-mail. Electronic mail communication has established a presence in the practice of law. A survey by the Legal Technology Resource Center of the American Bar Association reports that 52.7% of responding small law firms use the Internet or an online service to communicate with colleagues and 53.6% use the Internet or an online service to communicate with clients. The survey also reports that 83.7% of responding large law firms use the Internet or an online service to communicate with colleagues and 93.5% use the Internet or an online service to communicate with clients. *See* American Bar Association, Legal Technology Resource Center, 1998 Small Firm Technology Survey, 1998 Large Firm Technology Survey.

The widespread use of electronic mail communication is accompanied by uncertainties regarding the implications of this new technology on the practice of law. Will an attorney's use of electronic mail communication

preserve client confidences and secrets, protect the attorney-client privilege, and meet the standards of practice within the legal profession? Or, will an attorney who communicates with or about clients by electronic mail violate confidences under the ethics rules, cause a waiver of the attorney-client privilege, or incur malpractice liability?

These issues generate great interest among the bar. A resolution, drafted by the Young Lawyers Division of the American Bar Association and approved by the ABA delegates on August 4, 1998, calls upon courts of all jurisdictions to accord lawyer-client electronic mail communications the same expectations of privacy and confidentiality as lawyer-client communications by mail, telephone, and other traditional methods of communication.

Yet, these issues cannot all be resolved within this opinion. Courts and legislators will guide and determine attorney-client privilege issues and attorney malpractice liability issues. For discussion of attorney-client privilege and malpractice issues see David Hricik, *Confidentiality and Privilege in High-Tech Communications*, 8 The Professional Lawyer 1, 17-27 (1997); David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, XI Geo. J. Legal Ethics, 459, (1998); Kurt X. Metzmeier and Shaun Esposito, *How to Avoid Losing Your License on the Information Superhighway: Ethical Issues Raised by the Use of the Internet in The Practice of Law*, Kentucky Bar Association Bench & Bar, Spring 1998, at 14; Joan C. Rogers, *Ethics, Malpractice Concerns Cloud E-Mail, On-Line Advice*, 12 Current Reports, Laws. Man. on Prof. Conduct (ABA/BNA), 59 March 6, 1996; *Electronic Communications*, Laws. Man. on Prof. Conduct (ABA/BNA), 55:401 (Oct. 30, 1996).

This opinion advises solely upon the ethical concern of whether an attorney violates his or her duty to preserve confidences and secrets under DR 4-101 of the Ohio Code of Professional Responsibility by communicating with clients through electronic mail without encryption. The opinion is limited in this manner because the Board's authority under Gov. Bar R. V §2(C) is to advise upon the application of the Code of Professional Responsibility.

Disciplinary Rule 4-101 of the Ohio Code of Professional Responsibility requires the preservation of client confidences and secrets. Division (A) defines confidences and secrets. Division (B) prohibits attorneys from knowingly revealing or improperly using a confidence or secret. Division (C) sets forth limited circumstances in which disclosure is permitted, one of

which is client consent. Division (D) requires reasonable care by a lawyer to prevent employees, associates, and others from disclosing or using confidences and secrets.

In all likelihood, attorney communication with clients by electronic mail was not contemplated when DR 4-101 was adopted by the Supreme Court of Ohio on October 5, 1970; nevertheless, the rule applies. The rule as written, establishes a broad duty to preserve confidences and secrets that applies to all methods of communication. The duty extends to communications by electronic methods just as it extends to other forms of communication used by an attorney.

Since DR 4-101 applies to e-mail communications, what are the attorney's obligations under the rule? Does an attorney who communicates by electronic mail to clients fulfill his or her ethical duty under DR 4-101 to preserve confidences and secrets? Or, do risks of interception make an attorney's expectations of confidentiality in e-mail communication so unreasonable that the duty to preserve confidences and secrets is violated unless messages are encrypted? (Encryption refers to the encoding of messages and is discussed infra.)

Before determining an attorney's obligations under the rule, it is first necessary to consider how e-mail is transmitted. A distinction is often made between Internet e-mail and non-Internet e-mail. Non-internet e-mail is transmitted through local area networks (such as a law firm's own internal network system) or through commercial networks referred to as online service providers (such as America Online).

A local area network is considered a private network because its use is limited to those employed by a firm or an organization. The e-mail message travels from the sender's computer to the recipient's computer over land-based telephone lines. For example, a member of a law firm may use the firm's local network to communicate with another firm member regarding a client matter. Or, an in-house counsel might use the corporation's internal network to communicate with the corporate client.

An online service provider is considered a semi-public network. Members of the public who subscribe to a service pay a fee for access to the on-line service. E-mail from one member of an on-line service to another member of the online service travels from the sender's computer across land-based telephone lines directly into the recipient's password protected mailbox. If

the sender and recipient are members of the same online service, the e-mail message does not travel over the Internet to reach its destination. But, if the sender and the recipient are members of different on-line services, the message travels out over the Internet before reaching the recipient's computer.

Internet e-mail is transmitted differently. Internet e-mail travels from a sender's host computer over the Internet through "routers" (intermediate computers owned by third parties) before reaching a recipient's mailbox. The message does not travel as a whole. The sender's computer breaks the e-mail document into small packets of data. The packets travel from computer to computer through the intervening routers depending on which computer is least busy. Each packet may travel through a different router. The message is re-assembled by the recipient's computer.

To summarize, non-internet e-mail travels from the sender's host computer to the recipient's computer over land-based telephone lines and does not travel outside the provider's network. In contrast, Internet e-mail does not go directly from a sender's computer over land-based telephone lines to a recipient's password protected mailbox. Internet e-mail travels in packets rather than as a whole across interconnected networks of computers which route the message to the recipient's computer.

There are security concerns with both Internet mail and non-Internet mail. Concerns with Internet mail are that a message may be captured as it travels over the Internet ("sniffing") or that an intermediate computer may be programmed to act as the recipient's host ("spoofing"). With both Internet e-mail and non-internet mail there are concerns that security may be compromised at either the sender's computer or at the recipient's computer. Passwords may become known to others, messages may be left in open view on the sender's or the recipient's computer screen, unauthorized access to the computer system may occur ("cracking"). There are also concerns raised regarding e-mail monitoring by network system administrators.

Yet, the degree of security risk is difficult to determine. As to Internet e-mail, the large volume of e-mail, the way in which it travels over the Internet in packets rather than in its entirety, and the dynamic routing of the packets through a variety of intermediate computers are factors contributing to difficulty of interception. The interception of both Internet and non-Internet e-mail, requires an investment of time, money, and equipment and a willingness on the part of the interceptor to engage in illegal activity.

For discussion on the transmission of e-mail and security concerns see Kenneth E. Johnson, American Bar Association Law Practice Management Section, *The Lawyer's Quick Guide to E-mail*, 93-105 (1998); David Hricik, *Confidentiality and Privilege in High-Tech Communications*, 8 The Professional Lawyer 1, 17-27 (1997); David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, XI Geo. J. Legal Ethics, 459, (1998); Janlori Goldman, *Privacy on the Internet*, Trial, June 1997, at 20-25; Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail* (Aug. 16, 1995) <http://www.computerbar.org/netethics/bjones.htm>.

Encryption is raised in response to security concerns. Encryption refers to the encoding of e-mail messages to make the message unreadable by anyone other than the sender and the intended recipient. Encryption involves the use of a mathematical function, an algorithm, to scramble messages. Encryption software programs are commercially available. As with other technologies, techniques for encryption are evolving.

For discussion of encryption see Kenneth E. Johnson, American Bar Association Law Practice Management Section, *The Lawyer's Quick Guide to E-mail*, 93-105 (1998); David Hricik, *Lawyers Worry too Much About Transmitting Client Confidences by Internet E-mail*, XI Geo. J. Legal Ethics, 459, 493-508 (1998); Timothy Tomlinson, *Public Key Cryptography: How It Works*, Computer Law Strategist, June 1997, at 3; Charles R. Merrill, Cryptography for Attorneys-Beyond Clipper (1994) <http://www.law.vill.edu/chron/articles/merrill.html>; Kevin J. Connolly, *Cryptography Can Ensure E-Mail Technology*, The National Law Journal, Monday Jun. 9, 1997, at B13-B15.

Scholars and commentators debate whether encryption should be mandatory for attorney-client communications. Proponents view encryption as a reasonable precaution an attorney can take to maintain confidentiality and to protect attorney-client privilege and/or as a way to prevent unintentional disclosure and to eliminate arguments about waiver. *See e.g.*, Arthur L. Smith, *E-Mail and the Attorney-Client Privilege* (1995) <http://www.abelaw.com/bamsl/lpm/email.htm>; Robert L. Jones, *Client Confidentiality: A Lawyer's Duties with Regard to Internet E-Mail* (1995) <http://www.computerbar.org/netethics/bjones.htm>.

Opponents of mandatory encryption object to treating e-mail differently from other types of communication, pointing out that other forms of communications, such as phones and mail, can be intercepted. Opponents also point out that interception requires a lot of time and money to capture a particular message on the Internet when there are millions sent each day; and that it is unlawful to intercept an e-mail communication. *See e.g.*, William Freivogel, *Communicating With Or About Clients on the Internet*, XII ALAS News, (Nov. 3 1995); Peter R. Krakaur, *Treat E-mail Like Other Communications: An Argument Against Mandatory Encryption of Attorney-Client Communications* (posted Jan 1, 1998, archived Feb. 1, 1998) <http://www.llrx.com/features/e-mail.htm>.

Encryption has practical limitations. The following have been raised as examples. Both lawyer and client must use compatible encryption programs. Encryption cannot protect the identity of the sender or recipient in the header of the message since the router must know this information to deliver the message. Encryption is not free. Some foreign countries do not permit encryption messages to be transmitted. As government seeks access to decryption keys for policy, law enforcement, and security reasons, encryption may become more vulnerable. *See e.g*., David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, XI Geo. J. Legal Ethics, 459, 493-508 (1998); Jan Hemm Pritchard, *E-Mail Privacy: An Oxymoron*? J. Mo. Bar, Jul.-Aug. 1997 at 239, 243; Charles R. Merrill, Cryptography for Attorneys - Beyond Clipper (1994) <http://www.law.vill.edu/chron/articles/merrill.html>.

The trend among advisory bodies in other states (and the District of Columbia) is that electronic mail without encryption is ethically proper under most circumstances.

> In the District of Columbia, "[i]n most circumstances, transmission of confidential information by unencrypted electronic mail does not *per se* violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security." District of Columbia Bar, Op. 281 (1998).
>
> In Illinois, "[l]awyers may use electronic mail services, including the Internet, without encryption to communicate with clients unless unusual circumstances require enhanced security measures." Illinois State Bar Ass'n, Op. 96-10 (1997).

> In New York, the state bar association advised that "lawyers may in ordinary circumstances utilize unencrypted Internet e-mail to transmit confidential information without breaching their duties of confidentiality under Canon 4 to their clients, as the technology is in use today. Despite this general conclusion, lawyers must always act reasonably in choosing to use e-mail for confidential communications, as with any other means of communication. Thus, in circumstances in which a lawyer is on notice for a specific reason that a particular e-mail transmission is at heightened risk of interception, or where the confidential information at issue is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted Internet e-mail." New York State Bar Ass'n, Op. 709 (1998). The city bar association advised that "[a] law firm need not encrypt all e-mail communications containing confidential client information, but should advise its clients and prospective clients communicating with the firm by e-mail that security of communications over the Internet is not as secure as other forms of communication." Ass'n of the Bar of the City of New York, Formal Op. 1998-2 (1998).
>
> In North Dakota, "Rule 1.6 of the North Dakota Rules of Professional Conduct is not violated by a lawyer who communicates routine matters with clients, and/or other lawyers jointly representing clients, via unencrypted electronic mail (e-mail) transmitted over commercial services (such as America Online or MCI Mail) or the Internet unless unusual circumstances require enhanced security measures." State Bar Ass'n of North Dakota, Op. 97-09 (1997).
>
> In Vermont, "[a] lawyer does not violate DR 4-101 by communicating with a client by e-mail, including the Internet, without encryption." Vermont Bar Ass'n, Op. 97-5.

One state is reticent in its advice regarding unencrypted electronic communication with clients.

> In Arizona, the state bar responded "Maybe" to the question "Should lawyers communicate with existing clients, via e-mail, about confidential matters?" They advised "it is not unethical to communicate with a client via e-mail even if the e-mail is not encrypted" but suggested "it is preferable to protect the attorney/client communications to the extent it is practical." The committee suggested using a password known only to the lawyer or client, using encryption software, or at a minimum using a cautionary statement such as "confidential" and "Attorney/Client Privileged" either in the "re" line or beginning the communication. An additional suggestion was to caution clients about transmitting highly sensitive information via e-mail if the e-mail is not encrypted or otherwise secure from unwanted interception. Attorneys were "reminded that e-mail records may be discoverable." State Bar of Arizona, Op. 97-04 (1997).

Several states have reconsidered their initial views on the issue.

> In South Carolina, the bar association first advised that "unless certainty can be obtained regarding the confidentiality of communications via electronic media, that representation of a client, or communication with a client, via electronic media, may violate Rule 1.6, absent an express waiver by the client." South Carolina Bar, Op. 94-27 (1995). Later, the bar advised that "[t]here [now] exists a reasonable expectation of privacy when sending confidential information through electronic mail (whether direct link, commercial service, or Internet). Use of electronic mail will not affect the confidentiality of client communications under South Carolina Rule of Professional Conduct 1.6." South Carolina Bar, Op. 97-08 (1997).
>
> In Iowa, the bar association rescinded Formal Op. 95-30 and replaced it with Formal Op. 96-1 advising that "with sensitive material to be transmitted on E-mail counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for the communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks, or it must be encrypted or protected by password/firewall or other generally accepted equivalent security system." Iowa State Bar Ass'n, Op. 96-1

> (1996). *See also* Iowa State Bar Ass'n Op. 96-33 (1997). Later, the bar association amended Opinions 96-1 and 96-33 by advising that "with sensitive material to be transmitted on e-mail counsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgement includes consent for communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks to be protected as agreed between counsel and client." Iowa Bar Ass'n, Op. 97-1 (1997)

In Ohio, the issue is now addressed herein. In advising upon whether unencrypted e-mail is a method of communication that fulfills an attorney's duty to preserve confidences and secrets under DR 4-101, the Board considers the following in reaching its interpretation of the ethical requirements of the rule. First, through the use of computers in the practice of law, electronic mail communication has become a popular and efficient method of communication. Second, while there are security risks that e-mail will be intercepted, the risk of interception is not singular to this one method of communication. Every method of communication carries with it a risk of interception. Mail can be intercepted. Telephone messages can also be intercepted. Land-based telephones may be wiretapped, eavesdropping may occur by listening through a receiver of a telephone extension, or too loud voices may be overhead by others. Yet, these forms of communication are considered reasonable under the rule.

Third, interception of electronic communication is a criminal activity. Interception of e-mail is illegal under both federal law and state law. Federal law prohibits interception and use of electronic communication at 18 U.S.C.A. § 2511 (West 1998). Ohio law prohibits purposeful interception of electronic communication at Ohio Rev. Code Ann. § 2933.52(A) (West 1998). Under both state and federal law the prohibition on interception and use of electronic communication does not apply to a provider of electronic service communication while engaged in any activity necessary to the rendition of the service or to the protection of the rights of the provider of the service. However, service observing or random monitoring by a provider is not permitted except for mechanical or service quality control checks. *See* Ohio Rev. Code Ann. § 2933.52(B)(2) (West 1998); 18 U.S.C.A. § 2511 (2)(a)(i) (West 1998).

Fourth, there is support in case law for the proposition that a reasonable expectation of privacy may exist even though a form of communication is

capable of being intercepted. As an issue of first impression, the Supreme Court of Ohio considered the rights of Ohio citizens to be free from unauthorized invasions of their cordless communications. In *State v. Bidnost*, 71 Ohio St. 3d 449, 461 (1994), the court held that the "provisions of R.C. 2933.52(A), prohibiting the purposeful interception of wire or oral communications through the use of an interception device, apply to cordless telephone communications that are intentionally intercepted and recorded." According to the court the terms of the Ohio statute defining "oral communications" and "wire communications" clearly encompass cordless telephone communication. *Id*. at 460-62. The court questioned the proposition that people communicating on cordless telephones have no legitimate expectation of privacy. "Fundamental rights should not be sacrificed on the altar of advancing technology." *Id*. at 462.

To summarize, additional security measures, such as scrambling devices or encoding methods, have not traditionally been required under DR 4-101 for other forms of communication frequently used by attorneys, even though the communication may be susceptible of interception. Interception is illegal. An expectation of privacy is not per se unreasonable particularly with communication methods that are illegal to intercept. For these reasons it is the Board's view that encryption of electronic messages is not mandated under the rule.

Even so, an attorney must use his or her professional judgment to determine the appropriate method of each attorney-client communication. Just as there may be some instances in which an attorney would not communicate by telephone or mail, there may be some circumstances under which an attorney would choose not to communicate by e-mail whether encrypted or not, for example, matters of extraordinary sensitivity. Likewise, there may be some circumstances under which an attorney may choose to encrypt a message. The nature of the communication will be relevant in choosing the method of communication. Client preferences will also be relevant in determining the method of communication. Evolving technology will influence communication decisions. Developing case law and statutory law will be relevant as well. Accepting responsibility for choosing the most appropriate method of communication is a duty of each member of the legal profession.

In conclusion, the Board advises that a lawyer does not violate the duty to preserve confidences and secrets under DR 4-101 of the Ohio Code of Professional Responsibility by communicating with clients through

electronic mail without encryption. An attorney must use his or her professional judgment in choosing the appropriate method of each attorney-client communication.

Advisory Opinions of the Board of Commissioners on Grievances and Discipline are informal, nonbinding opinions in response to prospective or hypothetical questions regarding the application of the Supreme Court Rules for the Government of the Bar of Ohio, the Supreme Court Rules for the Government of the Judiciary, the Code of Professional Responsibility, the Code of Judicial Conduct, and the Attorney's Oath of Office.