ADVISORY ETHICS OPINION 97-05

SYNOPSIS:

A lawyer does not violate DR 4-l0l by communicating with a client by e-mail, including the Internet, without encryption.

The use of an Internet web site to communicate with clients and prospective clients requires compliance with DR 2-103 and DR 2-104 relating to advertising and solicitation.

FACTS:

The inquiring lawyer poses several questions regarding ethical issues generated by the use of electronic methods of communication, including e-mail and the Internet.

Specifically, the lawyer asks (l) whether an unencrypted e-mail can be used to communicate with existing clients in view of the requirement of the Disciplinary Rules to maintain the confidentiality of client information, and (2) whether the use of a "web site" to advertise or otherwise facilitate contact with prospective clients requires compliance with DR 2-l03 concerning advertising and DR 2-l04 concerning direct contact with prospective clients.

Definitions

Because of the highly technical material which must considered, the Committee on Professional Responsibility of the Vermont Bar Association will first set out commonly accepted definitions of terms used herein.

l. "Electronic mail" (e-mail) is a message sent from one user's computer to another user's computer via a host computer on a network, or via a private or local area network (which we define to mean a network wholly owned by one company or person which is available only to those persons employed by the owners or to whom the owner has granted legal access) or via an electronic mail service such as America Online (a "public network"), via the Internet, or by a combination of these methods.

2. "Encrypted e-mail" is e-mail that has been electronically locked to prevent anyone but the intended recipient from reading it using a "lock and key" technology. The most common approach to encryption is "public-key" encryption. In public-key encryption two different electronic keys are used. One key is used by the sender to encrypt the message and another is used by the recipient to unencrypt or decrypt it. The decryption key is kept secret by the person who owns it and is called the "private key". The encryption key is made public, and is known as the "public key". To send an encrypted message, the sender finds the recipient's public key, uses it to encrypt the message, and then sends the encrypted message to the recipient. The recipient is the only person able to decrypt the message by using the private key. The public key may be posted on the Internet or distributed to the person who intends to send the owner e-mail, usually by diskettes or e-mail. Simply stated, such messages are "locked" by the sender, making them unreadable except by the intended recipient, who has a "key" in the form of an electronic password to decode the message.

3. The "internet" is a world wide super network of computers consisting of individual computers and private and public networks owned by various persons and entities including business, schools, governments, and non-secure military computers. Individual users connect to the Internet through a local "host" computer. The local host computer communicates with other computers throughout the world over the phone lines or privately owned high-speed fiberoptic lines using a collection of well-defined common protocols.

4. A "bulletin board" service is a privately owned and operated computer system, which is usually accessible by a direct telephone line, but may well be connected to the Internet, where electronic messages can be posted and browsed or delivered to e-mail boxes.

5. The "World Wide Web" ("WWW") is the common name applied to one of the protocols used to publish information on the Internet. The WWW consists of a vast collection of information organized in the form of pages of text, graphic images and programs, and stored on millions of computers around the world.

6. A "home page" is a computer file which may contain both text, graphics and programs stored in a special format which can be obtained via the WWW. The home page may have links to other subsidiary pages or to other web sites using an easy to use "point and click" interface.

7. A "web site" is a group of computer files containing text and graphics organized around a central home page.

8. The Electronic Communications Privacy Act (as amended) (the "ECPA") includes the Federal codification (l8 USC §25l0, et seq.) of the common law tort of the invasion of privacy as applied to electronic communication.

DISCUSSION - E-MAIL QUESTION:

These issues have produced opposing conclusions, with the Iowa Supreme Court Board of Professional Ethics and Conduct and the Ethics Advisory Committee of the South Carolina Bar opting to deny the use of e-mail without encryption except with express client approval, while the Illinois State Bar Association determined that lawyers may use e-mail, including the Internet without encryption unless "unusual circumstances" demand enhanced security methods.

The first issue presented, whether a lawyer may use e-mail, including the Internet, to communicate with clients, is entwined in the duty to protect confidential information received from the client. DR 4-l0l applies this requirement to information protected by client privilege (a "secret") and to information "gained in" the professional relationship that "the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client (a "confidence")". EC 4-4 adds that the duty differs from the evidentiary privilege, existing "without regard to the nature or source of information or the fact that others share the same knowledge". The information that a lawyer must protect includes both confidences and secrets.

The duty to maintain client confidentiality mandates the use of communication methods providing reasonable assurance that the message be and remain confidential. The Iowa (95-30) and South Carolina (94-27) opinions concluded that a particular means of communication includes the possibility of interception, use of that means of communication requires encryption or client consent after disclosure of the risk. The Illinois opinion (96-l0) disagreed, based on the conclusion that electronic communications are no more susceptible to interception than ordinary phone calls, and with the added factor that interception is illegal under the ECPA.

Moreover, all three types of electronic messages (local network, public network, or Internet) appear no less secure than the ordinary fax or telephone communication. For example, e-mail on a local or public network can be accessed only from within the group which owns the network.

E-mail sent by America Online, CompuServe, or MCI Mail (all of which are public networks) travels from a sender's computer to a computer "mail box" maintained by the public network over a reserved phone network. Access to the public networks is password protected. Undeniably, e-mail sent over public networks and BBS's is potentially less secure than mail sent over a private network because the employees of the public network or an outside person who "cracks" or breaks into the system could intercept the message, but any phone call can be tapped, legally or otherwise, and the mails and faxes can be intercepted and read. Since this possibility of interception also exists for fax transmission and regular mail, no reason exists to treat e-mail differently.

Internet e-mail travels to its destination differently. E-mail sent over the Internet does not go directly from the sender's computer over a land-based line to a password-protected "mail box". The message is broken into two or more "packets" of information by the sending computer or host computer, which are then sent individually over the lines and ultimately reassembled back into the complete message, at the recipient's "mail box". The mail boxes may exist on the recipient's computer or may exist on the host computer the recipient uses to connect to the internet. These information packets must pass through and be temporarily stored in other computers called "routers", operated by different firms known as "internet service providers" which assist in distributing e-mail over the internet. To intercept an internet transmission in transit would constitute an illegal wire tap.

DISCUSSION - WEB PAGE QUESTION:

Web pages may be compared to advertisements in the telephone yellow pages or magazine articles. All of them are indirect means of communicating with existing or potential clients about an attorney, the attorney's services, and the law in general. As presently designed, the author/publisher of the web page prepares the information and makes it available to the world. There are a number of companies who provide indexes to web pages (www.yahoo.com, www.altavista.digital.com, www.excite.com). The potential client seeks out information, as in the yellow pages, and chooses whether or not to read and/or act on the available information. The attorney has no choice as to who sees or reads the information posted.

The Illinois opinion also ruled that the creation and use of an Internet "web site" containing information about the lawyer's services which can be accessed over the Internet by anyone, including prospective clients, is not "communication directed to a specific recipient" within the meaning of the Rules and, consequently, only the general rules governing communications concerning a lawyer's services and advertising apply to a lawyer's "web site" on the Internet.

This opinion may change if the newly developed "push" technology become as popular as the WWW. In a push technology environment, the lawyer publishes the information on an "information channel" which is directed to the subscribers, in the manner of a cable television channel. Under that scenario the lawyer has more of an opportunity to select who will see the information provided by the attorney. Then, the issues entwined in solicitation and direct mail will arise. The day to determine those questions has not yet arisen, as push technology is relatively new and not yet widely available.

As long as the Web Page is equivalent to a "yellow page" advertisement or a magazine article, the general rules of truth in advertising and limitations on indirect solution should apply to a lawyer's use of Web Pages.

CONCLUSION:

The Committee does not respond to the unstated question as to whether inadvertent or intentional interception of confidential e-mail triggers malpractice liability. We note that the Attorneys' Liability Assurance Society (ALAS), a captive insurance company which insures lawyers against malpractice claims, advises its members that encryption is not necessary on the internet except for items so sensitive as to require avoidance of any threat of interception.

For the reasons stated, we concur with the Illinois opinion, whose reasoning and sources we adopt. The Committee believes that any lawyer may use e-mail and the internet while complying with the Code of Professional Responsibility.

With regard to the first issue presented, the Committee decides that since (a) e-mail privacy is no less to be expected than in ordinary phone calls, and (b) unauthorized interception is illegal, a lawyer does not violate DR 4-101by communicating with a client by e-mail, including the internet, without encryption. In various instances of a very sensitive nature, encryption might be prudent, in which case ordinary phone calls would obviously be deemed inadequate.

With regard to the second issue presented, concerning use of an internet web site to communicate with clients and prospective clients, the Committee concludes that the Code of Professional Responsibility's Disciplinary Rules governing advertising and solicitation provides sufficient guidance. An internet "home page" is similar to the phone book's "yellow pages" and law firm brochures and is not "directed to a specific recipient".1

MATTERS NOT ADDRESSED:

This opinion does not address the rules that may apply to participation in "newsgroups" or discussion groups that deal with legal or other subjects, "chat rooms" and other potentially interactive means of communicating with one or more existing or prospective clients. These forms of communication are different and the rules that apply to private e-mail and the traditional Web Page do not apply to these more interactive means of communication.

* * *

The Committee recommends several articles concerning a lawyer's use of electronic mail.

l. ABA/BNA Lawyers' Manual on Professional Conduct Practice Guide Dealing With Electronic Communications, under the heading "Confidentiality", No. l70.

2. ABA/BNA Lawyers' Manual on Professional Conduct, Current Reports, March 6, l996, an article by Joan C. Rogers, Staff Editor, entitled "Ethics Malpractice Concerns Closed E-Mail, On-Line Advice".

3. The ethics article entitled "The Perils of Office Tech" by Joanne Pitulla, Assistant Ethics Counsel, in the October l99l issue of the "ABA Journal"

4. "Confidentiality and Privilege In High-Tech Communications" by David Hricick appearing in the February l997 issue of the "Professional Lawyer".

5. The l996 Symposium issue of the "Professional Lawyer" comprised of papers presented at the 22nd National Conference on Professional Responsibility, which took place in Chicago. Several articles dealing with the subject matter are printed in this Symposium issue including "High Tech Ethics and Malpractice Issues", "Spinning an Ethical Web: Rules of Lawyer Marketing in the Computer Age", and "Can the Decrepit Encrypt: Do We Need the Cone of Silence, or Is 'Pretty Good' Good Enough?".

1 See DR 2-l03 and DR 2-l04.

6. An article by Kevin J. Connolly in "The National Law Journal", Monday, June 9, l997, entitled "Cryptography Can Ensure E-Mail Confidentiality". Mr. Connolly notes that New York State is considering an amendment to its Civil Practice Law and Rules, sep. 4547, which would provide that "[n]o communication otherwise privileged under this article shall lose its privileged character for the sole reason that it is communicated by a electronic means or because persons necessary for the delivery or facilitation of electronic communication may have access to the content of the communication."

7. An article by Janlori Goldman in the June l997 issue of TRIAL entitled "Privacy on the Internet". Ms. Goldman is Deputy Director and Co-Founder of the Center for Democracy and Technology (CDT).