DELAWARE STATE BAR ASSOCIATION
COMMITTEE ON PROFESSIONAL ETHICS

Opinion 2001-2

This opinion is merely advisory and is not binding on the inquiring attorney or the Courts or any other tribunal.

I. Introduction

A member of the Delaware Bar (the "inquiring attorney") has requested an opinion from the Committee regarding the ethical propriety of an attorney transmitting confidential client information via e-mail and mobile (or cell) phone.

II. Summary of Background Facts

Attorneys, paralegals and support staff of the inquiring firm have access to and use e-mail communications using an Internet-based system. This communication system allows for the electronic transfer of information both as message text and in the form of attachments. The firm has three offices in Delaware. Some of the firm's employees are case handlers and are supervised by personnel located in a different office, and thus they communicate at times by e-mail. Also, some employees have occasion to work from home and send confidential work product through the Internet-based e-mail system to an e-mail account supplied by the firm. In addition, several firm employees own mobile telephones or cell phones (of either the analog or digital variety) and find use of those devices for conversations with or about clients to be convenient and efficient.

It appears that the inquiring attorney(s) operate much like many attorneys throughout Delaware and the nation in the use of e-mail correspondence and cell phones. E-mail provides a quick and efficient means of communicating both messages and documents, and finds routine use throughout the Delaware legal community. Similarly, with the proliferation of cell phones, it is now commonplace for attorneys to engage in wireless telephonic conversations, often involving client confidences.

III. Issues Presented

Does the transmission of confidential client information over an Internet-based e-mail system violate the obligation to maintain the confidentiality of such information under Rule 1.6?

Does the transmission of confidential client information using a mobile (or cell) phone violate the obligation to maintain the confidentiality of such information under Rule 1.6?

IV. Conclusion of Opinion

The transmission of confidential information by way of e-mail or mobile (or cell) phone, absent extraordinary circumstances, does not violate Rule 1.6. Extraordinary circumstances include circumstances in which the lawyer should reasonably anticipate the possibility that his or her communication could be intercepted and confidences disclosed, such as the client's sharing an e-mail account with others.

V. Discussion

The ethical obligation to maintain the confidentiality of client information is set forth in Rule of Professional Conduct 1.6(a), which provides in part that: "A lawyer shall not reveal information relating to the representation of a client unless the client consents after consultation, except for disclosures that are impliedly authorized in order to carry out the representation …." It is appropriate to consider, therefore, whether communication by e-mail and mobile phone presents a significant risk of inadvertent disclosure of confidential information. By evaluating this risk, one can come to a reasoned conclusion about the lawyer's expectation of privacy and hence the ethical propriety of transmitting client information through these modes.[1]

A. E-mail

Although there appears to be no Delaware decisional authority addressing the issue, the American Bar Association (ABA) and several states have issued opinions concerning whether it

---

[1] Relatedly, the privilege that may otherwise apply to a communication between a lawyer and a client may be waived by the inadvertent disclosure of the communication. See DEL. R. EVID. 502. Thus, the failure of a lawyer to exercise reasonable precautions to ensure confidentiality may result in such a waiver. See Monsanto Co. v. Aetna Casualty & Surety Co., C.A. No. 88C-JA-118, 1994 Del. Super LEXIS 261 (Del. Super., May 31, 1994) (evaluating the precautions taken to prevent disclosure when determining whether a privileged document retains its privilege).

is ethical to transmit information relating to the representation of a client by e-mail sent over the Internet.[2] In Formal Opinion No. 99-413, the ABA Standing Committee on Ethics and Professional Responsibility (the "ABA Committee") concluded that a lawyer may transmit protected client information by e-mail over the Internet without violating Model Rule 1.6, which is identical to its Delaware counterpart.

The ABA Opinion recognizes that there are several forms of e-mail, including the Internet-based e-mail system in issue here. In an Internet-based e-mail system, messages are sent through land-based phone lines by intermediate Internet service providers (ISPs) whose software routes the message through third-party routers, hubs and fiber-optic cable, to the recipient's ISP, then to the recipient's address. The ABA Committee recognized that this system presents some risk of disclosure to unintended recipients; the ISPs, for example, have a qualified right to monitor e-mail passing through their networks, and "hackers" may intercept messages. Counterbalancing this risk of disclosure are federal laws imposing limits on the ability of ISPs to inspect user e-mail[3] and hackers face the threat of criminal and civil liability.[4] The ABA Committee observed, moreover, that "[b]ecause the specific route taken by each e-mail message through the labyrinth of phone lines and ISPs is random, it would be very difficult consistently to intercept more than a segment of a message by the same author."[5] Perhaps most significantly, the ABA Committee Opinion recognizes that while e-mail transmissions are subject to interception, so too are more traditional modes of communication, such as land-line telephones and the U.S.

---

2 See ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413, § 4 (1999); Alaska Ethics Op. 98-2 (1998); D.C. Ethics Op. 281 (1998); KY. Ethics Op. E-403 (1998); N.Y. Ethics Op. 709 (1998); Ill. Ethics Op. 96-10 (1997); Iowa Ethics Op. 1997-1 (1997); N.D. Ethics Op. 97-09 (1997); PA. Ethics Op. 97-130 (1997); S.C. Ethics Op. No. 97-08 (1997); VT. Ethics Op. 97-5 (1997); Ariz. Ethics Op. 97-04 (1996); N.C. Ethics Op. 215 (1995).

3 18 U.S.C. §§ 2511(2)(a)(i), 2511(3)(a) (2000). Delaware law parallels this federal statute, and all sections of the Electronic Communications Privacy Act that are referred to within this opinion. Although the federal Act was not adopted verbatim into Delaware law, the two Acts are largely identical and provide the same protections. See DEL. CODE ANN. tit. 11 §§ 2401-2404, 2421-2422 (2000).

4 18 U.S.C. §§ 2511, 2701-2702 (2000).

5 ABA Comm. on Ethics and Professional Responsibility, Formal Op. 99-413, § 4 (1999).

and commercial mail, which are presumed nonetheless to afford the lawyer a reasonable expectation of privacy.

The ABA Opinion thus appears well reasoned in concluding that a lawyer does not violate his or her ethical obligations in transmitting client information by way of e-mail. The ABA Opinion is in accord with most state opinions.[6] Some states, however, have more limited or cautious views regarding e-mail communications between attorney and client than the ABA. For example, one state opinion provides that for sensitive material to be transmitted on e-mail counsel must have written acknowledgment from the client about the risk of the potential for violating the disciplinary rules requiring a lawyer to maintain the confidentiality of communications.[7] Other states have endorsed e-mail as a means of communicating client confidences, but have advised that lawyers may want to seek client consent and/or consider the use of encryption prior to its use.[8] Perhaps significantly, all of these state opinions pre-date ABA Formal Opinion No. 99-413.

---

6 See, e.g., Alaska Ethics Op. 98-2 (1998) (lawyers may communicate with clients via unencrypted e-mail; client consent is unnecessary because the expectation of privacy in e-mails is no less reasonable than that in the telephone or fax); D.C. Ethics Op. 281 (1998) (lawyers' use of unencrypted e-mail is not a violation of duty to protect client confidences under District of Columbia Rule of Professional Conduct 1.6); Ill. Ethics Op. 96-10 (1997) (lawyers may use unencrypted e-mail, including e-mail sent over the Internet, to communicate with clients without violating Rule 1.6 of the Illinois Rules of Professional Conduct; client consent is not required absent "extraordinarily sensitive" matter; expectation of privacy in an e-mail is no less reasonable than that in ordinary telephone calls); KY. Ethics Op. E-403 (1998) (absent "unusual circumstances" lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients); N.Y. Ethics Op. 709 (1998) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analog to ABA Model Rule 1.6); N.D. Ethics Op. 97-09 (1997) (lawyers may communicate with clients using unencrypted e-mail unless unusual circumstances warrant heightened security measures); S.C. Ethics Op. No. 97-08 (1997) (finding reasonable expectation of privacy when sending confidential information by e-mail to communicate client confidences does not violate South Carolina Rule of Professional Conduct 1.6); VT. Ethics Op. 97-5 (1997) (lawyers may use unencrypted Internet e-mail to transmit confidential information without breaching the duty of confidentiality under state analogue to ABA Model Rule 1.6).

7 Iowa Ethics Op. 1997-1 (1997). Significantly, the Iowa and North Carolina opinions pre-date ABA Formal Opinion 99-413.

8 Ariz. Ethics Op. 97-04 (1996) (lawyers may want to caution client about transmitting sensitive information by e-mail or consider the use of encryption); N.C. Ethics Op. 215 (1995) (cautioning lawyers to take measures that will best maintain confidentiality and if a lawyer

E-mail technology is such that while unauthorized access is possible, in any given case it is certainly not probable (or even likely) that the communication will be intercepted or misdirected. This is so because e-mail messages do not travel across the Internet in a particular route or in a complete form. Rather, every message is broken up into hundreds and in some cases thousands of individual packets of information before it is transmitted.[9] Each packet travels along its own individual and random path across the Internet highway before arriving for reassembly in the recipient's mailbox.[10] Apparently, therefore, it is difficult to intercept a specific e-mail message because there is no way to predict every path or hub an e-mail message may travel through.[11]

Accordingly, it would appear that a lawyer reasonably could expect that the transmission of client information via e-mail will remain private and will be viewed only by the intended recipient(s). Inevitably, circumstances may arise where there is a genuine risk of unauthorized access. For example, a lawyer representing one spouse in a matrimonial proceeding might need to refrain from communicating with the client by way of e-mail if the other spouse shares access to a computer at their shared residence. For the most part, however, lawyers can communicate by way of e-mail secure in the knowledge that the communicated information will reach the intended recipient(s) without being intercepted. For these reasons, we believe that transmitting confidential client information over an Internet-based e-mail system, absent extraordinary circumstances, is not violative of Rule 1.6.

---

knows or has reason to believe that the communication may not be secure the lawyer must advise the other parties to the communication of the risks of losing confidentiality); Pa. Informal Op. 97-130 (1997) (noting that the risk of intentional or inadvertent interception may not be different than other forms of communication, but suggesting that a lawyer should advise of risks of e-mail communication and obtain consent to use e-mail communication, or even use encryption, with respect to sensitive information).

9 David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, 11 GEO. J. LEGAL ETHICS 459, 468-69 (1998).

10 Id.

11 Id.

B. Mobile Phones

Unlike e-mail messages, which are transmitted over land-based phone lines, cordless phones rely on radio waves to broadcast signals to the phones' base units. These radio waves are subject to interception by radios, baby monitors and other cordless phones.[12] Similarly, cellular phones transmit radio signals that are subject to interception. Improvements in mobile phone technology, such as digital transmissions, may lessen the risk of interception.[13]

The ABA has not yet taken a position on the ethics of mobile or cell phone use. Among the state bars that have addressed the issue[14] there is a split of authority. Generally, the state opinions fall into three categories. At one end of the spectrum, Massachusetts and New Hampshire, under the "strictest" category of opinions, advise against any use of cellular or cordless phones by attorneys to discuss client information.[15] Their thinking is premised upon the notion that clients have a right to presume that communications with their lawyer will be confidential. Hence, if a lawyer has doubts that a particular communication is secure, he or she should resolve those doubts in favor of protecting confidentiality and avoiding the use of a mobile phone.

At the other end, Arizona has concluded that an attorney's mere use of a cellular or cordless phone does not constitute an ethical breach or automatic forfeiture of the attorney-client privilege.[16] The Arizona Bar's reasoning is that any other conclusion would lead to

---

12 Id. at 483.

13 Id.

14 Arizona, Illinois, Iowa, Massachusetts, New Hampshire, New York, North Carolina, and Washington.

15 See Mass. Ethics Op. 94-5 (1994) (concluding that confidential information should not be discussed on a cellular phone if there is any non-trivial risk that such information may be overheard by a third party; and even if the attorney concludes that there is no risk, the conversations should only occur after full disclosure of the dangers involved and client consent); N.H. Ethics Op. 1991-92/6 (1991) (advising attorneys not to discuss client confidences or any other matter related to representation without client consent unless a scrambling device is used).

16 See Ariz. Ethics Op. 95-11 (1995).

unintentional waivers of privilege, and would hinder a lawyer's ability to advise clients with reasonable promptness and diligence.

The last group of states (garnering the most support) advocates a middle-ground approach. This body of opinions advises caution and disclosure. Specifically, these states advise lawyers to advise their clients that mobile phone conversations cannot be considered confidential, and to obtain the client's informed consent prior to using cellular or cordless phones to discuss client matters.[17]

Courts of law have addressed in a variety of contexts constitutional issues arising from the use of cordless and cellular phones. It does not appear, however, that a court of law has spoken definitively to the specific issue of whether or not the attorney-client privilege applies to conversations conducted on cellular phones.

Much of the authority that concluded that there could be no reasonable expectation of privacy in mobile phone conversations was addressing the issue in the context of cordless, not cellular phones. The distinction between the two types of phones was determinative in the outcome of the cases.[18] This was so because under the Electronic Communications Privacy Act (the "ECPA")[19] of 1986, cordless phone communications were specifically excluded from the legal protections granted by the Act, while cellular phone communications were not.[20] It was not until 1994 that Congress amended the ECPA to protect cordless phones. Under the 1994

---

17 See N.C. Ethics Op. 215 (1995); N.Y. City Ethics Op. 1994-11 (1994); Iowa Ethics Op. 90-44 (1991); Wash. Informal Ethics Op. 91-1 (1991); Ill. Ethics Op. 90-7 (1990).

18 Compare United States v. Smith, 978 F.2d 171 (5th Cir. 1992) (concluding that cordless phone conversations were not protected under the ECPA of 1986); McKamey v. Roach, 55 F.3d 1236 (6th Cir. 1995) (same result); Askin v. United States, 47 F.3d 100 (4th Cir. 1995) (same result), with Shubert v. Metrophone, Inc., 898 F.2d 401 (3d. Cir. 1990) (concluding that Congress clearly intended cellular phone conversations to be protected when it enacted the ECPA of 1986).

19 18 U.S.C. §§ 2510 et seq. (2000).

20 Cellular phone communications have been protected since the inception of the ECPA of 1986. See The Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 101(d)(2), 100 Stat. 1848 (1986).

Amendment, "cordless" phone conversations were given the same legal protections as land-line and cellular telephone conversations.[21] Thus, cellular, cordless, and land-line phone conversations are now protected under the Act, and any interception of such conversations may constitute a federal crime.[22]

In pertinent part the ECPA states that: "[i]nterception and disclosure of a wire, oral, or electronic communications [are] prohibited."[23] Additionally, the Act specifically preserves the privileged status of unlawfully intercepted communications;[24] prohibits any use of information that was illegally intercepted;[25] and prohibits the introduction of such information as evidence at trial even if it was not privileged to begin with.[26] Moreover, it is now a federal crime to manufacture, distribute, possess, or advertise for sale, any device that can be used to intercept cellular phone conversations.[27] Perhaps most significant is that courts have interpreted the ECPA to apply to cellular and cordless phones.[28] Consequently, attorneys may reasonably conclude that the above stated statutory provisions offer vast (if not full) protection for client communications that are conducted via cellular phones.[29]

---

21 See The Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (wherein Congress deleted previous provisions of the ECPA that limited the protections given to cordless phone communications).

22 18 U.S.C. § 2511 (2000).

23 Id.

24 Id. § 2517(4).

25 Id. § 2511(1)(b).

26 Id. § 2515.

27 Id. § 2512.

28 Bartnicki v. Vopper, 121 S. Ct. 1753, 1760 (2001) (citing Nix v. O'Malley, 160 F.3d 343, 346 (6th Cir. 1998); McKamey v. Roach, 55 F.3d 1236 (6th Cir. 1995)).

29 Practitioners should note that the Supreme Court has held that in a very limited context, i.e. where a matter of public concern has been intercepted by an unknown third party and subsequently published by the press, the ECPA may be unconstitutional. Bartnicki, 121 S. Ct. at 1765. However, the court made it very clear that the case should not be viewed as affecting

Based on the foregoing discussion, one can reasonably conclude that the major risks associated with the use of cellular phones (e.g., intentional interception; inadvertent disclosure; adverse use of disclosed or intercepted information; or admittance of disclosed or intercepted information into evidence at trial) are largely alleviated by federal statute.[30] Of course, as a practical matter, legislative protections make no inroads on the technological problems with mobile phone communications, but at least such protections make unauthorized listeners less likely to misuse the information. The ABA Opinion on e-mails relies in part on just such legislative protection. Specifically, if it is unlawful to intercept a communication, a lawyer reasonably may harbor a greater expectation of privacy. Therefore, we conclude that, absent extraordinary circumstances,[31] transmitting confidential client information using a mobile (or cell) phone is not violative of Rule 1.6.

ECPA jurisprudence outside of the context of First Amendment freedom of speech challenges dealing with matters of public concern. Id. at 1764-65.

[30] To the extent that the above-mentioned statutes do not address the risk of inadvertent disclosure or interception, ABA Formal Opinions 92-368 (1992) and 94-382 (1994) provide some guidance on the topic. In these opinions the ABA Committee addressed the propriety of a lawyer's use of information that was inadvertently received. They concluded that a lawyer in receipt of information that does not belong to him, must refrain from examining the information any more than necessary to determine that information was not intended for him and must notify the sender. Furthermore, after notification the recipient is required to dispose of the information in the manner requested by the sender.

[31] The extraordinary instances in which mobile phone communications might be electronically intercepted are far less likely than the problem presented when lawyers and clients share confidential communications on mobile phones while in public places within earshot of others. Lawyers therefore should take precautions not to discuss confidential matters with clients while in a public place, such as on a train or in an airport, if others may overhear the conversation. Likewise, lawyers should advise their clients to take similar precautions when speaking to counsel on mobile phones.