OLIFF & BERRIDGE, PLC
ATTORNEYS AT LAW
SPECIAL
REPORT

PRIVILEGED COMMUNICATIONS AND THE INTERNET

December 1997

An emerging trend appears to be that the mere fact of using the Internet to send a privileged communication or confidential information will not be deemed a waiver of privilege or confidentiality. However, the law in this area is still in a state of flux. The only issue on which there currently appears to be a consensus is that the waiver issue is mooted if the communications over the Internet are sent in (a reasonably secure) encrypted form.

Consequently, until the law becomes more settled and uniform, we recommend not using the Internet to send sensitive communications and information, whether privileged or confidential, unless the communications and information are encrypted. Encryption technology has advanced to the point that there are several methods that are available for international use, easy to implement and use, and provide a very substantial measure of protection. To avoid any potential disputes later, we further recommend that, before an attorney or other legal representative starts using the Internet to communicate with a client, the parties have a written agreement confirming the client's authorization of such Internet communications.

A brief summary of the relevant law in the United States follows:

Case Law

No court has found a privilege waived because information was sent via e-mail. In two cases, courts found that the work product or attorney-client privilege attached specifically to e-mail communications between client and counsel. *International Marine Carriers, Inc. v. USA,* LEXIS 4155 (S.D.N.Y. Apr. 3, 1997); *National Employment Ins., Corp. v. Liberty Mutual Ins. Co.,* No. 93-2528-g (Mass. Supp. Ct. Dec. 21, 1994) (Lawyers Weekly No. 12-42094). In a similar manner, two other courts implicitly found that the attorney-client privilege attaches to e-mail communications between client and counsel. *USA v. Keystone Sanitation Co.,* 899 F. Supp. 206 (M.D. Pa. 1995); *Stopka v. Alliance of American Assurers,* LEXIS 5466 (N.D. Ill. Apr. 25, 1996). However, none of these courts specifically dealt with the question of e-mail sent via the Internet. As discussed below, one element of both privilege and confidentiality is maintaining the privacy of the communications and information that are to be protected as privileged and/or confidential. The current debate over using the Internet centers on whether there is a reasonable expectation of privacy when using the Internet.

State Bar Advisory Opinions

Attorneys in the United States are subject to codes of professional conduct, which regulate their dealings with their clients, each other, the courts and other governmental agencies and the public. Each state, and many administrative agencies, have their own codes of professional conduct. The state codes of conduct are administered by state bar associations, which typically have special ethics committees that render formal advisory opinions concerning the interpretation of their states' code of professional conduct and the application of the code to particular fact situations.

Three state ethics committees have issued advisory opinions concerning the confidentiality of e-mail sent via the Internet. Both the Ethics Advisory Committee of the South Carolina bar and the Iowa Supreme Court Board of Professional Ethics and Conduct rendered opinions advising attorneys that sending e-mail via the Internet without the consent of their client violates the attorney's ethical obligation to keep a client's confidences secret. South Carolina Bar *Advisory Opinion 94-27* (January 1995); Iowa Supreme Court Board of Professional Ethics and Conduct *Opinion 96-1* (August 29, 1996). While these opinions do not address specifically the attorney-client privilege, they do express a belief that e-mail sent via the Internet carries a low expectation of privacy.

Ethics boards in other states appear to be headed in the same direction. North Carolina has a proposed rule and Arizona a non-binding informal statement which both recommend the use of encryption when sending messages

via the Internet to avoid any breach of confidentiality under the rules of ethics.

In contrast, the Illinois State Bar Association (ISBA) rendered an opinion affirming the confidentiality of communications sent via the Internet. This opinion focused on the difficulty of intercepting specific e-mail transmissions and the 1986 amendments to the Electronics Communication Privacy Act (ECPA), which demonstrate "that Congress intended that Internet messages should be considered privileged communications just as ordinary telephone calls."[1] Illinois State Bar Association, *Advisory Opinion 96-10* (May 16, 1997). The ISBA concluded that "because (1) the expectation of privacy for electronic mail is no less reasonable than the expectation of privacy for ordinary telephone calls, and (2) the unauthorized interception of an electronic message subject to the ECPA is illegal, a lawyer does not" commit an ethical violation by communicating with a client using electronic mail, including the Internet, without encryption. *Id.* Following suit, the New York State Bar Association approved an amendment to the state's evidence code that would preserve the privileged character of communications made via the Internet.[2]

Current Commentary

Commentators on this subject are divided into primarily two camps, conveniently referred to as the "postcard" and the "metal-box" commentators. The postcard commentators assert that sending a plain text e-mail through the Internet is analogous to sending a postcard through the postal service. This form of communication carries a low expectation of privacy, which is inconsistent with the attorney-client privilege. In contrast, the metal-box commentators feel that sending a plain text e-mail via the Internet is analogous to sending the communication in a metal box with a lock that few criminals are competent to open. Because this type of communication carries a high expectation of privacy, the metal-box commentators argue that plain-text Internet communications are consistent with the attorney-client privilege.

Both sides agree that messages sent via the Internet are vulnerable to hacker[3] threats to confidentiality: snooping, sniffing and spoofing. A snooper uses software to examine e-mail as it passes through his or her computer on its way to its destination. A sniffer uses software to search for key words in any communication passing through his or her computer. A spoofer impersonates a person's e-mail name and sends and receives e-mail as an impostor.[4] Commentators analyze these threats to confidential information and generally come to two very different conclusions.

The postcard commentators point out that hacker software is readily available, which means that communications sent via the Internet are insecure. In addition, they point out that network administrators have access to e-mail as it passes through their hub on the Internet. In light of these threats to confidentiality, the postcard commentators assert that sending e-mail via the Internet is inconsistent with maintaining the attorney-client privilege. Further, the postcard commentators argue that the availability of very good and easy to use encryption software makes its non-use imprudent, and perhaps unethical, as it may waive any claim to the attorney-client privilege.[5]

The metal-box commentators argue that, even though hacker software is readily available, it remains extremely difficult to intercept the e-mail of a particular party. E-mail on the Internet does not travel on a set route but varies its path based on traffic and other factors. In addition, information sent via the Internet is often broken into packets which travel different routes and regroup at their

---

[1] "No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or, in violation of, the provisions of this chapter shall lose its privileged character." 18 U.S.C. §2517(4).

[2] "The proposed CPLR §4547, as approved by the New York State Bar Association, states that '*[n]o communication otherwise privileged under this article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication.*'" *Memoirs From the Corner Suite: An Update on Security and the Internet,* Samuel Lewis, (March 24, 1997). This article may be found on the Internet at <<www.colegehill.com/ilp-news/lewis2.html>>.

[3] The term "hacker" describes a person using her computer to intercept e-mail, break into computer systems or to perform any of a variety of other confidentiality threatening activities using a computer.

[4] Another very real threat to confidentiality, that does not involve communications, is the threat that a hacker will enter a corporate computer network via a modem connected to the Internet and explore confidential files.

[5] This reasoning indicates that even the postcard commentators at least implicitly recognize some expectation of privacy for encrypted communications.

common destination. While it may be possible for a hacker to intercept random e-mail, it is virtually impossible to intercept the e-mail of a particular party without a wire tap or some other form of surveillance. Further, as the ISBA notes, the EPCA makes the interception of e-mail a felony and further specifically preserves the privileged character of intercepted communications. 18 U.S.C. §2511 (1997). Finally, just as networks have administrators, so do phone systems, and both types of administrators have the ability to monitor communications. In fact, the EPCA specifically allows for administrators to monitor communications while still preserving their privileged character. 18 U.S.C. §§251(2)(a)(i) and 2517(4). Considering these facts, the metal-box commentators conclude that sending a message via the Internet is no more insecure or imprudent than talking on the phone without a scrambler.

One developing trend among Internet service providers (ISPs) clouds the analogy to the conventional telephone system. Some of the largest ISPs in the United States are currently placing non-confidentiality provisions in their service contracts with end-user subscribers. These provisions require that the subscribers give up their rights to the privacy of their e-mail communications and permit the ISPs to reveal the contents of the subscribers' e-mail to third parties. It is unclear how the courts and the state bars will react to these contract waivers of confidentiality.

* * *

Oliff & Berridge, PLC is a full-service Intellectual Property law firm based in historic Alexandria, Virginia. The firm specializes in patent, copyright, trademark, and antitrust law and litigation, and represents a large and diverse group of domestic and international clients, including individual entrepreneurs, major universities, and businesses ranging from small privately owned companies to large multinational corporations.

This Special Report is intended to provide information about legal issues of current interest. It is not intended as legal advice and does not constitute an opinion of Oliff & Berridge, PLC. Readers should seek the advice of professional counsel before acting upon any of the information contained herein.

For further information, please contact our office by telephone at (703) 836-6400, facsimile at (703) 836-2787, or mail at 700 South Washington Street, Alexandria, Virginia 22314.