

Use of E-Mail Creates Ethical Challenges

BY ANTHONY E. DAVIS

Communications by lawyers involve two sets of legal and ethical principles — the legal and ethical obligation to protect *privileged* information, and the legal and ethical obligation to protect all other client *confidences* (or “secrets” in states like New York whose ethics code is still based on the Model Code, rather than the Model Rules). The distinction between matter which is privileged and matter which is merely confidential is based on the fact that the former enjoys a narrow protection derived from the law of evidence, while the latter earns a broad protection based on the lawyer’s fiduciary duties to the client. The evidentiary privilege relates to confidential communications directly between lawyer and client for the purpose of obtaining legal advice. The much broader obligation to maintain confidentiality relates to the lawyer’s duty to protect *all information obtained in the course of representing* a client for the client’s benefit. Privileged matter is protected from compelled disclosure in litigation; but disclosure may be compelled of matter which is merely confidential, but which falls outside the scope of the evidentiary privilege. However, the lawyer’s obligation to protect confidential information may be just as strong — up to the moment of court ordered compulsion — as the obligation to preserve privilege. The underlying principle is that the right to decide what information in the possession of the lawyer — whether privileged or merely confidential — may be disclosed to third parties is the client’s, not the lawyer’s. The second legal principle at issue is the law of waiver. What does it take to create an actual or implied waiver of confidentiality or privilege, either by the client, or by the lawyer as the client’s agent? This article focuses on how these principles apply to E-mail.

E-Mail and the Expectation of Privacy

First, two “disclaimers”: this article will not deal with (i) problems created by the use of E-Mail by employees to harass others; or (ii) problems which arise when lawyers who have been provided with E-Mail addresses by their firms do not actively use them, leaving messages unanswered (sometimes indefinitely). These real (and growing) problems apply respectively to the burgeoning field of employment practices liability, and to ordinary malpractice, but both are beyond the scope of this article. We will also not deal with the ethical issues involved in marketing by lawyers on the Internet, particularly the dangers posed by interactive “web” sites (e.g., initiating attorney-client relationships; unauthorized practice in states where the firm and its lawyers are not admitted; and violation of advertising and solicitation rules).

We focus here on the degree to which E-Mail communications give rise to a reasonable expectation of privacy. The security offered by basic E-Mail is somewhere between a land-line telephone and a cellular telephone: transmissions may be subject to interception (which would be criminal), but a fair degree of technological sophistication and deliberation are required for interception. The central problems presented by the use of E-Mail are:

Communications Are Susceptible to Interception by Third Parties. Although interception is generally a criminal offense (in the same way that any interception of telephonic communications may be criminal), it is clear that this does not necessarily prevent the actual disclosure of E-Mail communications to third parties.

Inadvertent Disclosure by the Transmitting Party: Two mirror image questions arise:

(1) when an E-Mail is misaddressed, does this constitute a waiver (albeit inadvertent) of client's confidences and privilege? and (2) what are the obligations of the recipient on receiving the misaddressed message?

The Ethics Opinions and Other Sources

There are few cases in this area, but there are many ethics opinions. These opinions differ widely as to whether E-Mail should be regarded as any less secure than regular mail (on which lawyers and clients regularly rely, notwithstanding the risk of theft of mail) or land-line telephone communications. Some argue that the chances of surreptitious interception are real and much more serious for E-Mail, and demand special precautions.

Relevant by analogy are the earlier opinions regarding cellular telephones. Generally, these assert that although eavesdropping on others' telephone conversations (or, by extension, E-Mail) is criminal, the nature of these transmissions is such that there can be *no reasonable expectation of privacy*, and that lawyers should either refrain entirely from using these technologies, or, at least, realize that they have a duty to warn clients before using them.

Inadvertent Disclosure

The Inadvertent Transmitter: State evidence law will govern cases of inadvertent transmission — and it will be impossible to know ahead of time which state's law will apply. That will be determined by where the E-Mail went, which court has jurisdiction, and whose law applies to the case. While there are no cases specifically relating to E-Mail, there is case law dealing with the parallel (and frequent) problem of misaddressed faxes. In the facsimile cases, three separate approaches are currently in use, each with its own set of built-in problems for lawyers and clients.

Some courts follow the traditional common law approach that disclosure of a privileged communication constitutes a waiver, regardless of precautions (or lack thereof), or of the "implied waiver" rule. Other courts adopt the "actual waiver" rule. This holds that there is no waiver in the absence of an actual and deliberate waiver of the privilege *by the client*.

The third, and seemingly most common approach is to undertake a factual analysis in each case to determine if the precautions taken to prevent disclosure were "reasonable." This approach will find waiver only where the precautions were inadequate, or under the "factual analysis" rule. The fundamental problem for everyone using faxes — and by extension, E-Mail — is that it is impossible to know ahead of time which rule will apply.

The Inadvertent Recipient: Two ABA ethics opinions (92-368 (1992) and 94-382 (1994)) have created an extraordinary problem for lawyers who receive faxes (or, presumably, E-Mail messages) inadvertently sent to them. In direct conflict with lawyers' normal obligations towards their clients (which, presumably,

require competent and diligent — or zealous — use of all relevant information for the client's benefit), the 1992 opinion states that when the materials appear "on their face" to be privileged, the receiving lawyer should refrain from examining the materials, notify the sending lawyer, and then follow the sending lawyer's instructions.

The problem with this approach ought to be obvious. On an E-Mail there is no equivalent of the fax cover page, and the actual document being transmitted is immediately there -to read (unless it requires separate "downloading"). How then can we determine if it is "clear on its face" that the material is privileged, or not intended for the receiving lawyer? Besides, what is the legal basis for this wholly new set of duties? The 1996 draft of the ALI Restatement of the Law Governing Lawyers asserts that the ABA view is "not supported by decisional law." The courts, state ethics opinions, and discipline authorities have not been consistent in any direction in dealing with receiving lawyers who have sought to use material or information inadvertently disclosed to them.

Managing the Risks

There is a simple solution to the issues presented by these new technologies, which relates back to the fact that *the confidences and privilege attaching to client information are rights which belong to the client*. The issue, therefore, should be "what are the client's actual needs and requirements in the preservation of its particular confidences?"

Getting Client Consent: A simple solution is available for those lawyers who have adopted a requirement of mandatory engagement letters for all clients. Firms which are using these letters can easily include an express discussion of the issues which E-Mail presents, and the appropriate warning, within the text of these letters. The warning should disclose the danger (and implications) of interception, and the various technologies available — such as encryption — to limit the dangers. Discussion of the letter with the client can actually lead the client to make decisions about the need for, and the selection of, additional security measures, such as encryption — or whether E-Mail should be used at all. In this way, it will be the client who decides what level of security is required to preserve the secrets which are likely to be communicated during these transmissions.

Clients With Sensitive Data

For clients with very sensitive data, special protections may be required. At the most extreme, some information (such as, perhaps, information relating to a client's pending public securities offering) may need to be kept secure on stand-alone computers, not attached either to a network or to a modem so that E-Mail, if used at all, cannot easily be used to transmit sensitive documents. However, the final determinant ought to be, as in each of the other areas we discuss, client consent.

Avoiding Inadvertent Transmission: Firms have fundamental choices to make in their speed of response and control over E-Mail transmissions. If a firm seeks to establish some level of control over these problems, it may wish to impose some (or all) of the following rules and procedures: (i) that no E-Mail be sent to any client without the client's express prior consent, including any security requirements he may wish to install; (ii) that no E-Mail be sent without a printout of the text, including the address of the recipient; (iii) that all E-Mail messages be saved in memory.

What is important is that every firm confront the issue, make a considered decision as to what level of risk it wishes to accept — and confirm its decision in a memorandum to all lawyers in the firm, with advice on how to deal with the wishes of clients.

Limiting Inadvertent Receipt: There is not much the recipient can do, other than to know the local law and rules (or know who in the firm is the designated expert) — and to read introductory text slowly. This should help her to identify, as soon possible, transmissions that are “clearly on their face” not intended for her. If some of the ethics opinions are to be taken at their face value, failure to take this precaution may lead to allegations of impropriety against the recipient and even, conceivably, to motions to disqualify.

Let the Client Decide

Every communications technology presents new potential problems in protecting the property which represents our clients’ ultimate trust in us as professionals — their secrets. Each new technology presents firms with the need to balance seriously conflicting goals, namely the benefits of quick response and the dangers of inadvertent disclosure. In connection with each technology, however, there are steps which can be taken so that the clients’ trust in their lawyers is maintained; ideally, the client should play the central role in determining the proper level of precautions for each technology.