



Attorney-Client Email: 😊 or ☹️

By Julie R. Rubin

Can e-mail blow the lawyer's duty of confidentiality or the attorney-client privilege?
What about malpractice?

E-mail has revolutionized communication. It is faster and less expensive than facsimile and conventional mail and doesn't result in thick correspondence files that clutter an office. It ends telephone tag. No surprise, then, that e-mail is a choice method of communication between lawyer and client. Even documents are sent via e-mail. A client can open, read, redline the document and zip it back.

A lawyer exchanges e-mails with her client to arrange deposition dates of the client's former employees. Her e-mail explains the process of subpoena issuance and other benign subjects. Without the lawyer's knowledge -- and thinking reasonably enough that he was saving himself the time it would take to explain the process to the witnesses himself -- the client forwarded the e-mail to several would-be deponents. When counsel learns of this, she imagines how she will have to explain to her partner how she blew the attorney-client privilege. She envisions opposing counsel gleefully awaiting production of otherwise privileged documents.

With composure reclaimed, counsel explains to her client the relevant issues (including never, ever doing that again). But wasn't it counsel's duty to alert her client to the existence of the attorney-client privilege and how easily it can be lost?

Attorney Client Privilege

E-mail impacts two of a lawyer's obligations: the attorney-client privilege and the lawyer's broader ethical duty to keep her client's information confidential. If it is reasonable to expect that an attorney-client communication will be kept confidential and not revealed to third parties, the lawyer likely has not waived the privilege or violated the duty of confidentiality even if confidential information is somehow intercepted or sent in error to a third party.

The Electronic Communication Privacy Act of 1986 made it illegal to intercept e-mail, and provides that no "otherwise privileged" communication will lose that status if intercepted -- deliberately or inadvertently. Interception under the ECPA includes "acquisition" of an e-mail even after it has been received and stored in the intended recipient's inbox. The ECPA did not, however, change the law regarding waiver of the privilege or confidentiality, which still controls whether a communication is "otherwise privileged."

Example -- a lawyer e-mails her client about whether or not the client should sue her neighbor and the e-mail inadvertently is forwarded to the neighbor. Under the ECPA, the attorney-client privilege still attaches to that e-mail provided the state's law holds inadvertent disclosures as privileged. If the state law doesn't extend the privilege to inadvertent disclosures, the ECPA would not provide any additional protection just because that communication came in

the form of an e-mail. Regardless of the ECPA, the lawyer whose client forwarded the lawyer's e-mail about depositions is out of luck. That e-mail was not "otherwise privileged" because it was deliberately and voluntarily forwarded by the client (the holder of the privilege) to third parties.

Determining whether an electronic communication is "otherwise privileged" under the ECPA depends upon which of three theories of law on inadvertent disclosures the jurisdiction in question subscribes: 1) the traditional or strict view that once otherwise privileged information is inadvertently disclosed, the privilege is waived; 2) the lenient approach, also known as the limited waiver test, which holds that only deliberate disclosures effect a waiver, and reasons that because waiver must be intentional, an inadvertent disclosure, by definition, cannot waive the privilege; or 3) the case-by-case or intermediate approach, which assesses the particular facts surrounding the disclosure, including its extent, any remedial steps taken subsequent to the disclosure and the degree of carelessness of the party responsible for the disclosure. Under the intermediate approach (which was espoused by the Maryland Court of Special Appeals on August 29, 2002 in an opinion written by Chief Judge John Murphy in *Elkton Care Center Assoc. LP t/a Medpointe*, CSA No. 335, Sept. Term 2001), a waiver generally results only where reasonable precautions were not taken. Once it is determined that a waiver has occurred, the court must still determine its scope. Waiver of the privilege for a single document may not be so damaging, but an entire subject matter -- or even the entire privilege across the board -- is a different matter. So before you click "send," a lawyer should know the jurisdiction's law on waiver through inadvertent disclosure.

The Duty of Confidentiality

Where the broader duty of confidentiality is involved, regardless of the fact that the ECPA makes interception illegal, a lawyer should be mindful of the *ease* of interception -- particularly where the bottom line is the reasonableness of the expectation of privacy. Nonetheless, most state's ethics rules hold that there is a reasonable expectation that a communication via e-mail will be kept private, reasoning that e-mail is no different than the telephone or the fax machine. In fact, e-mail is transmitted over land-based phone lines just like an ordinary office telephone -- in contrast with cordless phones, which use common FM frequencies, and cellular phones, which can be tapped by using scanners. (Some courts have held that lawyers using cell phones do not have a reasonable expectation of privacy. It is now illegal, however, to market scanners in the United States, and in 1994 the ECPA was amended to protect cordless telephone transmissions.)

While, the law relating to waiver and the duty of confidentiality is no different when applied to e-mail than to telephone and facsimile, lawyers must keep in mind the ease and prevalence of re-distribution by an e-mail recipient -- particularly since state waiver law plays a key role where the privilege is concerned. For a fax to be distributed to an unintended third party (deliberately or inadvertently), fairly substantial steps must be taken. Plus, fax machines are a slow enough mode of communication that transmission can often be stopped before its completion. Forwarding of an e-mail requires almost no effort and the transmission of an e-mail is completed in a fraction of the time it takes to send a fax -- certainly too quick to reconsider or catch a mistake after the ill-fated click.

E-mail is also accessible to unwelcome, but lawful, monitors. Example -- the client who works in an office in which the employer retains the right to monitor employee e-mails is hardly an unusual circumstance. What happens when a lawyer sends her client an e-mail and the employer reads it? Particularly if the employer's employee manual includes a notice that e-mails are subject to monitoring, a waiver may well have occurred under applicable state law. At the very least, the client's confidentiality has been compromised (even though the lawyer may not have violated the duty of confidentiality).

Certainly, employers can also assert the right to monitor in-coming faxes, but a call alerting the client that a fax is coming through allows him to stand watch over the machine awaiting transmission of the fax. E-mail monitored by an omni-present employer affords no such privacy.

What of the third party IT vendor who maintains the Internet and e-mail system at your client's office? The vendor likely has access to the company's e-mails and to privileged and confidential communications. Does this waive the privilege? Maybe. And "maybe" isn't a comforting answer -- particularly if the laws of a jurisdiction applying the strict waiver approach are involved.

Case law on the subject is scarce and it's better to take precautions than to be sorry later.

Minimize the Risks

Take steps to minimize clients' exposure, but don't give up the convenience of e-mail. Certainly, include the now ubiquitous legend informing the recipient that "this e-mail may contain confidential or privileged information and should be destroyed if received in error" strengthens the reasonableness of the expectation. And place the legend at the beginning of the message. It does not do much good to add it as a postscript, after the confidential message has already been fully perused.

Encryption may be the surest form of protection for sensitive e-mail communications. Encryption software is simple, abundant and often free over the Internet. An effective and simple option is transmitting the communication as an attachment to the main message, which states that the attachment includes confidential and privileged content.

Consider adding the "dos and don'ts" about e-mail and attorney-client privilege to the standard engagement letter, including a provision that allows the client to opt-out of communicating by e-mail. Consider a one-time mass mailing setting forth basic guidelines and the firm's policy. Find out where clients receive e-mails and who may have access to them.

Setting aside the issues of the privilege and the duty of confidentiality, what about a lawyer's malpractice risk? Can lawyers who fail to take advantage of encryption or other risk management steps be held liable for third party interception and its aftermath -- perhaps a tanked deal or criminal charges? Some may argue that it is negligent to communicate with clients via unencrypted e-mail -- especially if the lawyer has failed to inquire whether the messages will be subject to monitoring or easily accessed by a third party.

Taking such precautions could save lawyer and client from the dreaded post-click “uh oh.”