Client Confidentiality in the Age of Surveillance

By Bob Ellis

Do you send unencrypted email to clients? Do clients send you email from their work address? Do you communicate with clients using instant messaging or texting? Do you use cloud-based storage or applications? If so, you're like most of us in the legal profession – but you should consider taking steps to make your online activity more secure.

The applicable ethics rules are simple in theory. RPC 1.6(a) says that a lawyer "shall not reveal information relating to the representation of a client, including information protected by the attorney-client privilege. . . ." Although 1.6(a) contains exceptions where the client gives "informed consent," and where the disclosure is "impliedly authorized in order to carry out the representation," those exceptions don't cover communications that are not intended to be revealed but that end up being revealed because they were not secure. Comment 16 to RPC 1.6 states that lawyers "must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure," and Comment 17 specifically states: "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients."

> If that were the complete status of ethics requirements regarding online communications, there would be little room for discussion: We all would be encrypting our communications with clients and would never even think of using non-secure means of communication (except to the extent we obtained informed consent from each client).

But the remaining part of Comment 17 clouds – as it were – the issue: "This duty [to take reasonable precautions], however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule." Comment 17 was written in the "age of innocence," when it wasn't obvious how unsecure online communications really are. The same can be said for ABA Formal Op. 99-413, still considered authoritative, which says that, given the laws protecting the confidentiality of electronic communication, it is ok for lawyers to send and receive confidential information via unencrypted e-mail: "[T]he mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint," and "the same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet email."[1]

Such a view is hard to take seriously today. The only real protection unencrypted communications have these days is "security through obscurity" – the likelihood that a particular message will not be noticed. Nonetheless, no specific guidance on such issues has yet been issued by any ethics organization in the wake of the revelations that virtually all unsecured online communications are monitored by unknown people and organizations around the world. The international law firm Meyer Brown discovered that the NSA had been monitoring its communications with foreign clients and had forwarded the content of those communications to U.S. officials conducting trade negotiations. That firm is now conducting seminars regarding "actual threats to the integrity and confidentiality of your data."

A lawyer's duty to protect client confidences goes beyond outgoing messages. "A lawyer sending or receiving substantive communications with a client via e-mail or other electronic means must ordinarily warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access. [This includes, for example,] circumstances where there is a significant risk that the communications will be read by [an] employer or another third party."[2] This is not merely a theoretical possibility; it happens frequently. If a client uses e-mail that is monitored by an employer or by a third party, the attorney-client privilege may be waived.[3]

All states now permit cloud computing, either by opinion or rule, or by lack of one.

Those states that place conditions on such permission have imposed fairly mild rules, mainly emphasizing client confidentiality and the integrity of client data. A typical example is New York, which permits cloud computing if the lawyer takes reasonable care to ensure that confidentiality is maintained. The lawyer also must keep up with technological advances to ensure that confidences remain confidential, and monitor changes in the law (and presumably provider contracts) to ensure that online data storage will not cause loss or waiver of privilege.[4]

Fifteen years ago Scott McNeely, the founder of Sun Microsystems, when told that many Internet users were worried about online privacy, famously declared, "You have zero privacy anyway. Get over it." Our ethical responsibility as lawyers – now more than ever – is to make sure that his declaration does not apply to our communications with our clients.

1. ABA Formal Op. 99-413: Protecting the Confidentiality of Unencrypted E-Mail (March 10, 1999).
2. ABA Formal Op. 11-459 (Aug. 4, 2011). See also N.C. Ethics Op. 2012-5 (Oct. 26, 2012); Wash. Advisory Op. 2216 (2012).
3. See Holmes v. Petrovich Development Co., LLC, 191 Cal. App.4th 1947 (Jan. 13, 2011); Fazio v. Temporary Excellence, Inc., 2012 WL 300634 (N.J. Super. Feb. 2, 2012). New York: U.S. v. Finazzo (Slip op.), 2013 WL 619572 (E.D.N.Y. Feb. 19, 2013) (criminal defense attorney's communication sent to his client's work email found not privileged; defendant was indicted based on the content of that communication). A ruling in favor of the employee: Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54, 973 A.2d 390 (N.J. Super 2009).
4. N.Y. State Bar Ass'n. Committee on Professional Ethics, Op. 842 (Sept. 10, 2010).

Bob Ellis
rellis@henniswhite.com