What Does Email Surveillance Mean for Attorneys' Ethical Duties?

Steven Thomas, Texas Lawyer

March 17, 2014

Edward Snowden's leaked documents have brought a lot of surprises. But the news hit a little close to home for lawyers on Feb. 15 when The New York Times reported that communications between an American law firm and its foreign-government client had been intercepted in early 2013 and possibly disclosed to the functional equivalent of the opposing party.

The article, "Spying by N.S.A. Ally Entangled U.S. Law Firm," said that a top-secret National Security Agency bulletin from February 2013 showed that the Australian Signals Directorate (the NSA's Australian counterpart) monitored communications between Indonesian officials and their American law firm (believed to be Mayer Brown, which was representing the Indonesian government in trade disputes with the United States). The Australians then offered to share the captured communications with the NSA, even though "information covered by the attorney-client privilege may be included." The NSA "declined to answer" whether any information was handed off to U.S. trade officials or negotiators, according to the article.

This news further exposes broad-based surveillance by United States and other intelligence-gathering governments in the so-called "Five Eyes Alliance" (Canada, Australia, Britain and New Zealand). A June 25, 2013, article in The Atlantic, "Is 'The Five Eyes Alliance' Conspiring to Spy on You?" described the scope of that surveillance as involving the interception of "vast quantities of communications between entirely innocent people, as well as targeted suspects," including "recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites."

But this isn't the only form of monitoring of concern to attorneys. Google has asserted in court filings that users of its Gmail online email service have no expectation of privacy. This led Consumer Watchdog to warn against using the Gmail service and gave Microsoft an opening to launch its "Scroogled" campaign.

Privacy

When it comes to using unencrypted email for communicating with clients, the reasonable expectation of privacy is crucial for attorneys. As email became popular, ethics committees in states such as South Carolina and Iowa warned that using unencrypted email might violate an attorney's ethical obligation to preserve client confidences.

But in 1999, the American Bar Association's Standing Committee on Ethics and Professional Responsibility gave a green light to attorneys using unencrypted email in its Formal Opinion No. 99-413. That opinion analyzed the obligations of lawyers regarding email communication under the Model Rules of Professional Conduct, and it concluded that lawyers had "a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail sent on the Internet, despite some risk of interception and disclosure."

The ABA Professional Ethics Commission bolstered that conclusion in 2008 with its Opinion No. 195: "The Commission concludes that, as a general matter and subject to appropriate safeguards, an attorney may utilize unencrypted e-mail without violating the attorney's ethical obligation to maintain client confidentiality."

But attorneys still must use caution. The commission went on to warn attorneys that they still have a duty to use good judgment according to the circumstances.

It said that before using email, lawyers "should consider both the content of the communication as well as the security of the email address to which it is being sent." For example, when representing a client in a divorce, it might not be a good idea to send sensitive advice to the client's home email address if the couple has not yet separated. And sometimes it's apparent that others might have access to a client's email address, such as corporate environments where employers frequently monitor employee emails.

The commission concluded by saying, "since email interception, though unlikely, is a possibility, attorneys should employ reasonable judgment in selecting a means of communication other than the Internet when the information is of such a highly confidential nature that disclosure would result in significant damage to the client's interests."

Then, in 2011, the ABA Ethics Committee issued its Formal Opinion 11-459, reminding attorneys of their duty to use caution when communicating by unencrypted email or other electronic means, such as text messaging. Although the opinion primarily focuses on concerns involving communications with employees who have a dispute with their employer, it concludes with a more general warning: "Whenever a lawyer communicates with a client by email, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client."

The Professional Ethics Committee for the State Bar of Texas has not specifically addressed the issue of unencrypted email. But Texas Disciplinary Rule of Professional Conduct 1.05(b)(1)(ii) prohibits attorneys from knowingly revealing "confidential information of a client or a former client to . . . anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law

firm." ABA Model Rule 1.6(a) relating to confidentiality of information also uses the verb "reveal" to describe the prohibited conduct.

So, if lawyers know that the governments of five countries are capturing, scanning and sharing our emails, does using an unencrypted email service for transmitting client information constitute "revealing" that information to third parties? What about using a service such as Gmail that affirmatively disclaims a reasonable expectation of privacy?

For now, lawyers might need to inform their clients of the risks and discuss possible alternatives to unencrypted email for particularly sensitive communications. But until courts, ethics commissions or the ABA opine further on the subject, lawyers at least need to be wary of electronic methods they use to communicate client confidences.

Steve Thomas is a shareholder in McGuire, Craddock & Strother in Dallas where he serves on the firm's technology committee. His practice includes commercial litigation in state and federal courts and administrative agencies on behalf of communications and technology companies. His email address is sthomas@mcslaw.com.