Column | Ethics

A Reasonable Expectation of Privacy for Client Information?

BY KATHERINE C. HALL

Texas Professional Ethics Committee Opinion 648 (April 2015) has now addressed whether lawyers may communicate confidential information by email. Lawyers used to send most written communications via the U.S. Postal Service or by fax. Many now use web-based email, such as unencrypted Gmail. How can we discharge our duties to protect information in the current environment?

As a general rule, lawyers must protect confidential client information. Tex. Disciplinary Rules Prof'l Conduct R. 1.05. reprinted in Tex. Gov't Code Ann., tit. 2, subtit. G, app. A (West 2005)(Tex. State Bar R. art. X, § 9). We must safeguard privileged and unprivileged client information, both of which might be transmitted by email. Rule 1.05(b) provides (except as otherwise specified under paragraphs (b) - (f)):

"a lawyer shall not knowingly . . .[r]eveal confidential information of a client or a former client to (i) a person that the client has instructed is not to receive the information; or (ii) anyone else, other than the client, the client's representatives, or the members, associates, or employees of the lawyer's law firm."

Using email creates a risk that unauthorized persons might get confidential information. Organizations previously considering the problem, such as the American Bar Association and other states' legal committees, often raise two points:

- All delivery systems present an inherent risk that an unauthorized person will gain access to confidential information, and
- Email users have a reasonable expectation of privacy under statutes that criminalize email interception, like the Electronic Communications Privacy Act, 18 U.S.C. § 2510 et seq. (1986).

Also instructive, Texas Professional Ethics Committee Opinion 572 (June 2006) determined that a lawyer could disclose privileged items when he reasonably expected a copy service to respect the confidential nature of the information. Following analysis of these precedents, Opinion 648 announced:

"In general, considering the present state of technology and email usage, a lawyer may communicate confidential information by email. In some circumstances, however, a lawyer should consider whether the confidentiality of the information will be protected if communicated by email and whether it is prudent to use encrypted email or another form of communication."

Of course, lawyers should exercise caution when handling communications of "highly sensitive or confidential information." They should also consider whether to use encrypted email or other forms of communication when dealing with situations in which:

- a client has a shared email account,
- a third party (spouse or co-worker) has obtained an account password,
- a lawyer or client is using a public or borrowed computer,
- a recipient checks email on an unprotected cellphone or other device, or
- a lawyer is concerned that a law enforcement agency may read email communications "with or without a warrant."

After the Opinion was released, a well-known security technologist blogged that attackers could read and modify encrypted data over certain connections. Schneier on Security, The Logjam (and Another) Vulnerability against Diffie-Hellman Key Exchange (May 21, 2015), https://www.schneier.com. Computer security breaches are often in the news. Last year, for example, hackers launched a cyber-attack against a major bank, compromising account security for an estimated 76 million households and 7 million small businesses. Despite the bank's annual $250 million computer-security budget, overseas hackers accessed sensitive, personal data, including names, addresses and emails of account holders. Russian hackers are said to be reading President Obama's unclassified email. And the NSA reportedly collects Gmail user data.

Ethical lawyers might not knowingly reveal confidential information. Most would lack "knowledge," as did JPMorgan Chase and the White House. Is lack of knowledge—which is virtually certain—sufficient? Encryption software written years ago—with known vulnerabilities—though reportedly patched in the last few weeks, is used by many websites and email providers, and is now in question. Because it is not clear that state or federal statutes provide a "reasonable expectation of privacy" for anyone, what can we do? The Opinion suggests that we:

- advise and caution clients about the dangers inherent in sending or accessing emails,
- obtain clients' informed consent to use email, including unencrypted email, and
- maintain ongoing evaluation of technology and email practices.

The Opinion's analysis of the Texas Disciplinary Rules of Professional Conduct, which does not include fiduciary obligations or best practices, notes that "there may be changes in the risk of interception of email communications over time that would indicate that certain or perhaps all communications should be sent by other means." HN

Katherine C. Hall is a Dallas-based lawyer. She can be reached at khall.atty@sbcglobal.net.