Lawyers and Email: Ethical and Security Considerations

By Scott Aurnou

The specter of attorney-client privilege has a long and well-respected history in litigation...but means nothing at all to a hacker. "Delete this email if you are not the intended recipient" or similar language theoretically sounds imposing, but essentially does nothing to protect firm or client data from any nefarious actors who view it (though they may get a good chuckle before reading the "forbidden" email).

In May 2014, LexisNexis published a study pertaining to law firm security awareness versus actual practices with respect to communications and file sharing with clients.[1] Almost 90% of those surveyed used email to communicate with clients and privileged third parties. The vast majority of attorneys surveyed also acknowledged the increasingly important role of various file sharing services and the inherent risk of someone other than a client or privileged third party gaining access to shared documents. Yet only 22% used encrypted email and 13% used secure file sharing sites, while 77% of firms relied upon the effectively worthless "confidentiality statements" within the body of emails to secure them.[2]

Relevant Ethical Standards

The effect of changes to the Model Rules: The ABA Model Rules of Professional Conduct were updated in 2012 specifically to address the effect of technology upon the legal profession, and a number of those changes directly pertain to the need for confidential communications.

The language in Comment 8 to Rule 1.1 (Competence) was amended to emphasize a duty for attorneys to stay up-to-date on technical matters pertaining to the practice of law, generally speaking: "[A] lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*."[3]

Paragraph (c) of Rule 1.6 (Confidentiality of Information) states:

> (c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.[4]

Comment 18 to Rule 1.6 relates to the need for a lawyer to "act competently" to prevent the disclosure of "information relating to the representation of a client." It offers a safe harbor provision and factors to determine the reasonableness of an attorney's conduct in protecting the information at issue:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[5]

In addition, Comment 19 to Rule 1.6 specifically relates to electronic communications with clients, stating, "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."[6] It also offers a safe harbor provision: "This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy."[7]

Therein lies the rub. What is reasonable, given the state of modern snooping technology? Moreover, from whom do the communications need to be kept private? Commercial competitors? Cyber criminals? Government actors? Other interested parties? Comment 19 specifically notes a pair of factors to consider when determining the reasonableness of the expectation of privacy. They are: (1) the sensitivity of the data itself, and (2) the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.[8] A client may also give informed consent to a method not otherwise permitted, though that approach may be asking for trouble if a client changes his or her mind later or disputes whether he or she was properly apprised of the relevant risks.

In addition to the Model Rules, failure to reasonably secure communications with clients can run afoul of state privacy laws[9] and potentially provide an effective basis for a colorable legal malpractice claim.

Pertinent Technology Basics

How does email actually work? By its nature, email is not a terribly secure way to share information. When you send out an email, it goes through a more powerful, centralized computer called a server on its way to a corresponding email server associated with the recipient's computer or mobile device. It passes through any number of servers along the way from sender to recipient, like a

flat stone skipping along the top of a pond. And if that email isn't encrypted, anyone with access to any one of those servers can read it.

What is encryption? Encryption is the use of an algorithm to scramble normal data into an indecipherable mishmash of letters, numbers and symbols (referred to as "ciphertext"). An encryption key (essentially a long string of characters) is used to scramble the text, pictures, videos, etc. into the ciphertext. Depending on how the encryption is set up, either the same key (symmetrical encryption) or a different key (asymmetrical encryption) is used to decrypt the data back into its original state (called "plaintext"). Under most privacy and data breach notification laws, encrypted data is considered secure and typically doesn't have to be reported as a data breach if it's lost or stolen (so long as the decryption key isn't taken as well).

A Few Methods to Secure Email

(1) Encrypted email. Properly encrypted email messages should be converted to ciphertext before leaving the sender's computer or mobile device and stay encrypted until they are delivered to the recipient (remaining indecipherable as they pass through each server along the way). This is referred to as *end-to-end encryption*.

There are plenty of encrypted email offerings from larger commercial companies, as well as a number of new and interesting email encryption services that have become available in the wake of disclosures made by Edward Snowden.[10]

When choosing one, be mindful of where the service you use is located (including where the servers handling the emails on the system actually are). Mr. Snowden used a well-regarded U.S.-based encrypted email provider called Lavabit. Not long after Mr. Snowden's revelations came to light, federal law enforcement officials forced Lavabit to secretly turn over the encryption keys safeguarding its users' private communications. Lavabit's founder tried to resist, but was overwhelmed in federal court.[11] As a result, he shut down the service. Another well-regarded service called Silent Mail followed suit shortly thereafter, as it felt it could no longer ensure its customers' privacy.[12] Both have since relocated to Switzerland and are planning to introduce a new encrypted email service called Dark Mail.[13]

Larger companies offering encrypted email services typically control the encryption keys and will decrypt data before turning it over in response to a warrant or subpoena (including one coupled with a gag order). In addition, email service providers can legally read any email using their systems under Title II of the Electronic Communications Privacy Act, referred to as the Stored Communications Act.[14] Moreover, emails remaining on a third party server for over 180 days are considered abandoned.[15] Any American law enforcement agency can gain access to them with a simple subpoena.[16]

Accordingly, if you choose to use a service based in the United States or another jurisdiction with similar privacy protections, be mindful of who controls the encryption keys.

(2) Secure cloud storage. Another way to securely communicate or share files with a client or privileged third party is to place the communication and/or files in encrypted cloud storage and allow the client or third party to have password-protected access to them. Rather than a direct email with possible attachments, the client or third party would receive a link to the securely stored data. The cloud service you select should be designed for security. Before you ask, DropBox and Google Drive would not be suitable options. There are a number of services offering well-protected cloud storage and it's important to do your due diligence before selecting one. If it all seems a bit much to figure out, two services I would recommend looking into are Cubby[17] and Porticor.[18]

(3) Secure Web portal. A third approach is to place the communications and/or files in a secure portion of your firm's network that selected clients and/or privileged third parties can access. As with the secure cloud storage option noted above, the email sent to the client or third party would have a link back to the secure Web portal's log-in page. An advantage to this approach is that the communications and files do not actually leave your computer network and should be easier to protect.

An additional consideration. A government snoop or competent hacker doesn't necessarily have to target a message while it's encrypted. A message that is protected by strong encryption when it's sent or held in secure cloud storage can still be intercepted and read once it has been opened or accessed using a mobile device or computer that has been compromised. The same holds true for intercepting a message before it's encrypted initially. What steps can you take to protect them?[19] The software on any computer or other device that can potentially access confidential data should be kept as up-to-date as possible; it should be protected against possible data loss if lost or stolen; and all firm personnel should have regular security awareness training with respect to social engineering[20] and other threats.

At the end of the day, there is no single silver bullet to provide "perfect security." But there are genuinely helpful steps (including those noted above) that you can take to comply with pertinent ethical standards and better protect your electronic communications with clients and privileged third parties.

Endnotes

1. LexisNexis Software Division, *LexisNexis Survey of Law Firm File Sharing in 2014*, SLIDESHARE (May 28, 2014), http://www.slideshare.net/BusinessofLaw/lexisnexis-2014-survey-of-lfile-sharing-survey-report-final.
2. *Id.*
3. MODEL RULES OF PROF'L CONDUCT R. 1.1, cmt. 8 (2014) (emphasis added).
4. MODEL RULES OF PROF'L CONDUCT R. 1.6.
5. *Id.* at cmt. 18.
6. *Id.* at cmt. 19.
7. *Id.*
8. *Id.*
9. *See, e.g.*, MASS. GEN. LAWS, ch. 93H, § 2(a) (regulations at 201 CMR 17.00 *et seq.*) (2014); NEV. REV. STAT. § 603A.215 (2014).
10. *See, e.g.*, Richard Stiennon, *Various Email Security Solutions Post Snowden*, SECURITY CURRENT (June 25, 2014), http://www.securitycurrent.com/en/news/ac_news/various-email-security-solutions-post-snowden.
11. Ladar Levinson, *Secrets, Lies and Snowden's Email: Why I Was Forced to Shut Down Lavabit*, THE GUARDIAN (May 20, 2014), http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email.
12. Parmy Olson, *Encryption App Silent Circle Shuts Down E-Mail Service 'To Prevent Spying,'* FORBES (Aug. 9, 2013, 12:41 PM), http://www.forbes.com/sites/parmyolson/2013/08/09/encryption-app-silent-circle-shuts-down-e-mail-service-to-prevent-spying/.
13. *See* DARK MAIL TECHNICAL ALLIANCE, http://darkmail.info/ (last visited Nov. 20, 2014).
14. 18 U.S.C. § 2701(c)(1) (2014).
15. *Id.* at §§ 2701(c)(3), 2703.
16. *Id.* at § 2703(b).
17. *See* CUBBY, HTTPS://WWW.CUBBY.COM/ (last visited Nov. 20, 2014).
18. *See* PORTICOR, https://www.porticor.com/ (last visited Nov. 20, 2014).
19. *See* Scott Aurnou, *What Is Endpoint Security?*, THE SECURITY ADVOCATE (Aug. 27, 2013), http://www.thesecurityadvocate.com/2013/08/27/what-is-endpoint-security/.
20. *See* Joan Goodchild, *Social Engineering: The Basics*, CSO ONLINE (Dec. 20, 2012, 7:00 AM), http://www.csoonline.com/article/2124681/security-awareness/social-engineering-the-basics.html.

Scott Aurnou is an information security consultant, attorney and Vice-President of SOHO Solutions, an IT consulting and managed services firm based in New York City. He regularly lectures on security, computer forensics and ethics relating to security and technology (particularly for legal professionals) and maintains a website called TheSecurityAdvocate.com.

Like what you're reading? To regularly receive issues of the *NY Business Law Journal*, join NYSBA's Business Law Section (attorneys only).

NEW YORK STATE BAR ASSOCIATION

CONNECT WITH NYSBA

Visit us on the Web:
www.nysba.org

Follow us on Twitter:
www.twitter.com/nysba

Like us on Facebook:
www.facebook.com/nysba

Join the NYSBA LinkedIn group:
www.nysba.org/LinkedIn