YOUR ABA
e-news for members

Encryption conniption

July 2015 | Eye on Ethics

by Peter Geraghty, director, ETHICSearch; and, Susan Michmerhuizen, ETHICSearch counsel, ABA Center for Professional Responsibility

In 1999, ABA Formal Opinion 99-413 approved the use of unencrypted email for the transmission of confidential information with the caveat that under circumstances where the information to be communicated is highly sensitive the lawyer should forgo email, just as he would from making a phone call or sending a fax, and consult with the client about the best way to transmit the information.

This opinion followed a line of state and local bar ethics opinions that addressed the question during the time in the mid-to-late 1990s when email use was just becoming the norm for lawyer-client communications and for most other communications as well. Most of the opinions from this era took the view that email is appropriate for lawyer/client communication, since it is just as illegal to intercept an email as it is to tap a phone call. Email communication was soon seen as equivalent to other means since a person who uses email has a reasonable expectation of privacy. See, e.g., Illinois State Bar Association Opinion 96-10 (1997) Kentucky Bar Association Opinion E-403 (1998) Minnesota Opinion 19 (1999) Pennsylvania Bar Association Opinion 97-130 (1997) South Carolina Bar Opinion 97-08 (1007) and Vermont Bar Association Opinion 97-5 (undated). It was during this growing acceptance of email use by lawyers that the privacy statement or confidentiality/privilege disclaimer entered common use. See State Bar of Arizona Opinion 97-04 (1997) (email transmissions to clients should include a cautionary statement either in the "re" line or at the beginning of the message, indicating that the transmission is "confidential" or "attorney-client privileged").

Other ethics committees did not grant an unequivocal blessing to

FIRST FOCUS

Need a change? Take a break from law, follow your bliss

EYE ON ETHICS

Encryption conniption

TECH TRANSLATORS

Law office technology for everyone

AROUND THE ABA

ABA summit offers innovative ideas on closing justice gap

Reimagining the future of the legal profession

Making alternative fee arrangements work for any size law firm

Drones: Coming not-so-soon to a business near you

Want to grow your practice? Try an online client portal

Finding – and refining – your voice as a new lawyer in the courtroom

unencrypted email but warned that the decision should consider other factors such as the sensitivity of the information and the likelihood of loss of privacy when deciding how to communicate. See State Bar of Arizona

Opinion 97-04, which advised that although a lawyer may communicate with a client via unencrypted email, it is preferable to protect the attorney-client communications through the use of encryption software or by having the email encrypted with a password known only to the lawyer and the client, and Missouri Opinion 970161 (undated) directing that if email communications are not secured through an encryption program in both directions, the lawyer must advise clients and potential clients that communication by email is not necessarily secure and confidential.

E2K and Ethics 20/20

Both the ABA Ethics 2000 Commission (E2K) and the Ethics 20/20 Commission developed this theme, advising in paragraphs 18 and 19 of the Comment to Rule 1.6 *Confidentiality of Information* that in effect, the more sensitive the nature of the information that is to be transmitted, the more the lawyer should consider whether it is appropriate to consult with the client about the extent to which additional safeguards should be employed.

An Ethics 20/20 inspired amendment to Rule 1.1 *Competence* requires lawyers to have a basic understanding of the technology that they use so that they can advise their clients as to the risks and advantages of different means of communication. For further information on the competence requirement, *see* the May 2014 Eye on Ethics column, *Competence: Acquire it or Hire it!*

Moving Target

The ever-developing nature of technology presents a moving target for those charged with setting ethics standards of competence and confidentiality. Changes in the form and manner of transmission of electronic communications force constant re-evaluation of the security of the exchange. Shared email accounts, shared passwords, shared computers, email accounts associated with an employer where the employee has no expectation of privacy *see*, e.g., ABA Formal Opinion 11-459 (2011), public computers, the idea of cloud computing, the prevalence of wi-fi connections at coffee shops and other public locations and the subsequent use of unsecured networks, the increase in hacking of institutions and individuals and information harvesting by government agencies such as the NSA all suggest that the expectation of privacy is open to question.

Shift in consensus?

The potential for unauthorized receipt of electronic data has caused some experts to revisit the topic and issue opinions

suggesting that in some circumstances, encryption or other safeguards for certain email communications may be required. A discussion on recent developments in confidentiality at this year's ABA Center for Professional Responsibility's National Conference on Professional Responsibility featured one speaker who highlighted a pendulum-swinging trend among ethics committees that are revisiting the question of whether lawyers should be required to use encryption when emailing clients. As reported in the *Lawyers' Manual*:

> …University of Georgia law professor Lonnie T. Brown said the consensus on communicating with clients through unencrypted email—driven by a 1999 ABA ethics opinion that approved the practice—may be giving way as authorities reconsider the risks of email interception.
>
> Speaking at a session on developments in confidentiality, Brown said "we have come a long way in [the] 16 years" since the ABA opinion was issued, and that a number of state ethics panels have shown a willingness to impose more onerous security requirements on lawyers. - *31 Law. Man. Prof. Conduct 320* (2015).

In 2010 after the panoply of incursions into online privacy had gained momentum, the State Bar of California Opinion 2010-179 weighed in on the issue. A digest of the opinion as it appears in the *ABA/BNA Lawyers' Manual on Professional Conduct* states as follows:

> Because the protection of confidentiality is an element of competent lawyering, a lawyer should not use any particular mode of technology to store or transmit confidential information before considering how secure it is and whether reasonable precautions such as firewalls, encryption or password-protection could make it more secure. The lawyer should also consider the sensitivity of the information, the urgency of the situation, the possible effect of an inadvertent disclosure or an unauthorized interception, and the client's instructions and circumstances, e.g., can others access the client's devices. A lawyer may use a laptop computer at home for client matters and email if the lawyer's personal wireless system has been configured with appropriate security features. However, if using a public wireless connection—for example in a coffee shop—the lawyer may need to add safeguards such as encryption and firewalls.

In 2011 Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility issued Formal Opinion 2011-200 that states as follows:

> …Compounding the general security concerns for email is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

Recently the State Bar of Texas has addressed the issue squarely and provided specific guidance. Opinion 648 (2015) identified several instances where encryption or some other method of security may be appropriate, including:

1. communicating highly sensitive or confidential information via email or unencrypted email connections;

2. sending an email to or from an account that the email sender or recipient shares with others;

3. sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client's work email account, especially if the email relates to a client's employment dispute with his employer (see ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 11-459 (2011));

4. sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;

5. sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or

6. sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer's email communication, with or without a warrant.

The question of when email should be encrypted is coming under increased scrutiny. The shift in focus is the nature of the confidential information and the surrounding technological developments that may heighten the need for protections. Heightened attention to your own firm practices and a greater awareness of the risks of regular email will be useful. As always, for further information on this issue, check the local rules, ethics opinions and court decisions of the jurisdiction. Your state or

local bar association may also be able to help.