To Encrypt or Not to Encrypt?

The changing consensus on email confidentiality.

BY RONALD CHICHESTER

More than 16 years ago, the American Bar Association issued its first formal opinion on email,[1] approving the use of unencrypted messages for the transmission of client confidences. The only caveat mentioned by the ABA was that when the information is highly sensitive, the lawyer should forego email, just as he or she would abstain from making a phone call, and consult with the client in person about the best way to discuss the information.

In the 1990s, the legal profession was rapidly adopting email as the standard means of communication with clients. At that time, the first ABA opinion merely echoed a string of various state bar opinions concerning the privacy of email.[2] These tended to rely on the fact that the U.S. Congress had enacted the Electronic Communications Privacy Act[3] of 1986 that prohibited access to stored electronic communications, which suggested a reasonable expectation of privacy. Most attorneys, however, began to add legal-specific caveats to their emails, claiming that the email transmission was an attorney work product, a privileged communication, or otherwise considered to be confidential as defined under rules of professional conduct.[4] While many states and the ABA found unencrypted email acceptable, some states—notably Arizona and Missouri—encouraged the use of encryption.[5] Most states, though, cautioned their attorneys to look at all the factors, particularly the sensitivity of data and the downsides associated with potential compromise, before electing to use email at all.

Since then, the ABA and other states have further addressed email communications, most notably in the ABA Ethics 2000 Commission[6] and the ABA Commission on Ethics 20/20.[7] The latter commission went so far as to require that lawyers understand and appreciate the technology behind email so they could make informed judgments themselves and provide reasonable guidance to clients about email.[8]

The implicit assumption of the opinions promulgated in the 1990s and early 2000s was that the attorney and client would send and receive emails from their respective offices. But with the advent of laptops, cellphones, and cloud computing—not to mention the use of free, unsecured Wi-Fi networks at coffee shops and other public places—these earlier opinions became outdated. Consequently, various states, including Texas, and the ABA are taking a fresh look at email confidentiality. Last year, the Professional Ethics Committee for the State Bar of Texas issued Opinion 648,[9] which identified several instances where encryption or some other security method 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 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 account, or sending an email to a client's work email account, especially if the email relates to a dispute with the client's employer.
4. Sending an email from a public or borrowed computer or under circumstances in which the lawyer knows that the sent emails are being read on a public or borrowed computer or on an unsecure network.
5. Sending an email if the lawyer knows that the recipient is accessing the email on devices that are potentially accessible by third persons without authority to access the emails or are not protected by a password.
6. Sending an email if the lawyer is concerned that the National Security Agency or other law enforcement agency may read the lawyer's email communication, with or without a warrant.[10]

Conclusions

While state bars and the ABA may not have settled opinions regarding the scope of a lawyer's ethical responsibility in the context of transmitting a client's privileged or confidential information through email, the trend is clear—email communications are coming under increasing scrutiny, and attorneys may well be called upon to encrypt email exchanges with their clients. Consequently, those of us who do not already know how to encrypt email should start learning now how to master the technical basics of the technology in order to communicate ethically. TBJ

Notes

1. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).
2. *See, e.g.*, Ill. SBA Comm. on Prof'l Conduct, Op. 96-10 (1996); S.C. Bar Ethics Advisory Comm. Op. 97-08 (1997); Pa. BA Legal Ethics & Prof'l Responsibility Comm. Op. 97-130 (1997); Vt. BA Prof'l Responsibility Comm., Op. 97-05 (1997); Ky. BA Ethics Comm, Op. E-403 (1998); Minn. Lawyers Prof'l Responsibility Board, Op. 19 (1999).
3. 18 U.S.C. § 2510 et seq., (1986).
4. Some state bars suggested that attorneys add a cautionary statement to their emails indicating the message is confidential. *See, e.g.*, SB Ariz. Comm. on Rules of Prof'l Conduct, Op. 97-04 (1997).
5. *See, e.g.*, SB Ariz. Comm. on Rules of Prof'l Conduct, Op. 97-04 (1997) (suggesting that while routine communications via unencrypted email was allowed, attorneys should preferably protect the communications through encryption software or encrypting with a password known only to the lawyer and the client); Mo. Bar Legal Ethics Counsel, Op. 970161 (required the lawyer to warn the client of the lack of secure and confidential communication if the email was not encrypted).
6. ABA Ethics 2000 Commission, http://www.americanbar.org/groups/professional_responsibility/policy/ethics_2000_commission.html (last visited Apr. 20, 2016).
7. ABA Commission on Ethics 20/20, http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html (last visited Apr. 20, 2016).
8. Model Rules of Prof'l Conduct R. 1.6.
9. Tex. Comm. on Prof'l Ethics, Op. 648 (2015).
10. *Ibid.*

This article was previously published in Circuits. *Reprinted with permission.*

RONALD CHICHESTER

practices in the Houston area and specializes in technology-related law, particularly intellectual property, electronic discovery, cybersecurity/cybercrimes/cybertorts, electronic commerce, and technology licensing. He is a past chair of the Computer and Technology Section of the State Bar of Texas and past chair of the Business Law Section. He is also an adjunct professor at the University of Houston, where he teaches classes on digital transactions and computer crime. Chichester holds bachelor's and master's degrees in aerospace engineering from the University of Michigan and a J.D. from the University of Houston Law Center.