Confidentiality of Email – The Changing Consensus

By Ronald Chichester

Sixteen years ago, the American Bar Association ("ABA") issued its first Formal Opinion about email,[1] which approved the use of unencrypted email for the transmission of client confidences. The only caveat mentioned by the ABA was that, under circumstances where the information to be communicated is highly sensitive, the lawyer should forego email, just as s/he would from making a phone call or sending a fax, and consult with the client about the best way to transmit the information.

In the 1990's, the legal profession was adopting email rapidly as the standard means of communications with clients. At that time, the first ABA opinion merely echoed a string of state bar opinions concerning the privacy of email.[2] These opinions tended to rely on the fact that the United States Congress had, in 1986, enacted the Electronic Communications Privacy Act[3] that prohibited access to stored electronic communications, which suggested a reasonable expectation of privacy. Most attorneys, however, began to add caveats to their emails, specific to the legal profession, claiming that the email transmission was an attorney work product, a privileged communication and/or otherwise considered to be confidential as that term is 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, however, cautioned their attorneys to look at all the factors

---

[1] Number 99-413, which is available at: http://www.americanbar.org/tools/digitalassetabstract.html/content/dam/aba/migrated/cpr/mo/premium-cp/99_413.pdf

[2] See, e.g., Illinois State Bar Association Opinion 96-10, South Carolina Bar Opinion 97-08, Pennsylvania Bar Association Opinion 97-130 and Vermont Bar Association Opinion 97-5 (all four issued in 1997); Kentucky Bar Association Opinion E-403 (1998); and Minnesota Opinion 19 (1999).

[3] 18 U.S.C. § 2510 et seq., better known as the ECPA.

[4] Some state bars went so far as to suggest that attorneys add a clause to their emails. For example, 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").

[5] See, e.g. State Bar of Arizona Opinion 97-04, suggesting that while routine communications via unencrypted email was allowed, attorneys should preferably 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. In Missouri, Opinion 970161 went so far as to put an extra duty on the attorney. That opinion required the lawyer to warn the client of the lack of secure and confidential

(particularly the sensitivity of data and the downsides associated with compromise) before electing to use email at all.

Since the 1990's, The ABA and other states have addressed email communications, most notably in the ABA Ethics 2000 Commission[6] ("E2K") and the Ethics 20/20 Commission.[7] The latter commission went so far as requiring the lawyer to understand and appreciate the technology behind email so that they could make an informed judgment themselves and provide reasonable guidance to clients about email communications.[8]

When the opinions identified above were promulgated (in the 1990's and early 2000's), the implicit assumption was that the attorney and client would send and receive emails from their respective offices. With the advent of laptops, cell phones and cloud computing in general – not to mention the use of unsecured networks at coffee shops and similar public places offering free wifi – the assumptions taken in earlier opinions began to be considered outdated. Consequently, various states (including Texas) and the ABA are taking a fresh look at email confidentiality. This year, the State Bar of Texas issued Opinion 648, which concerns the use of email.[9] That opinion 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;

---

communication if the email communications was not secured through an encryption program in *both* directions.

[6] Available at: http://www.americanbar.org/groups/professional_responsibility/policy/ethics_2000_commission.html

[7] Available at: http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html

[8] See specifically Rule 1.6, available at: http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

[9] Available at: http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx

4. sending an email from a public computer or a borrowed computer or under circumstances in which 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 by third persons without authority to access the emails 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.[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 via 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 communications should start learning now how to master the technical basics of that technology in order to communicate ethically.

About the Author

Ron 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 & Technology Section of the Texas Bar, and is currently the Immediate 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 (an intellectual property/e-commerce survey course) and Computer Crime. Ron holds a B.S. and an M.S. (both in aerospace engineering) from the University of Michigan and a J.D. from the University of Houston Law Center.

[10] Ibid.