Making Your E-Communications Secure

By David J. Bilinsky

"Everyone has secrets. Don't tell anyone."
—Kpop, *Everyone Has Secrets* (2013)

With the Snowden revelations and news of continual large-scale surveillance of the Internet by the U.S., United Kingdom, Canada, Australia, and New Zealand, there is increasing interest in protecting attorney-client communications. Solo and smaller firms are now inquiring about how to exchange secure electronic communications with their clients, given concerns about the perceived lack of privacy when using traditional e-mail. There is the growing realization that ordinary e-mail may not be an ideal way to communicate with clients.

Wikipedia states:

> After 180 days in the U.S., e-mail messages stored on a third party server lose their status as a protected communication under the Electronic Communications Privacy Act, and become just another database record. After this time has passed, a government agency needs only a subpoena—instead of a warrant—in order to access e-mail from a provider.[1]

There are other reasons for sending secure communications aside from concern that various governments may be reading our e-mails. All of us, at one time or another, have sent an e-mail to the wrong person. If the communication is sensitive but not secured, then the wrong recipient can read the contents (and attachments) and could forward them to others. If the communication intended for your client was instead sent to opposing counsel, you can see how this could create ethical and legal problems for you and your client. If the communication and attachments are encrypted, however, the substance of the message is still secure.

Law Practice Solutions is a regular feature brought to you by the Practice Management Resource Center (PMRC) of the State Bar of Michigan, featuring articles on practice management for lawyers and their staff. For more resources offered by the PMRC, visit our website at http://www.michbar.org/pmrc/content.cfm or call our Helpline at (800) 341-9715 to speak with JoAnn Hathaway or Diane Ebersole, Practice Management Advisors.

Further, you or your clients may be targeted. In "Hackers linked to China sought Potash deal details: consultant," *The Globe and Mail* reported:

> At least seven law firms were targeted in attacks that Daniel Tobok, president of Toronto-based Digital Wyzdom Inc., believes are also linked to hacking that paralyzed federal government computer systems last year.
>
> Most of these attacks were decoys, he said, meant to distract anyone tracing the activity from what he believes was the hackers' real goal: Getting information about BHP Billiton Ltd.'s ultimately unsuccessful $38-billion bid for Potash Corp. in 2010.[2]

There are several ways you can make your communications more secure and protect them from spying eyes of all types.

Person-to-person

This is decidedly not high tech, but if you deliver an encrypted flash drive or CD directly to your client, you completely avoid the risks of transferring information over the Internet. Using an encrypted flash drive or CD ensures that if the device is lost or stolen in transit from your office or the client's, the information is still secure assuming you used a strong encryption method. Of course, the password or phrase to decrypt the document would have to be exchanged with your client (and not by e-mail or a similarly insecure method). However, while this method is high on the security and privacy scale, it is not terribly convenient.

Encrypted communication using ordinary e-mail

You can use ordinary e-mail to deliver a fully encrypted document as an attachment. The e-mail need only say, "Please see attached." Again, the password or phrase to decrypt the document must be exchanged securely with your client.

Encryption security is only as strong as the password protection in your application. Newer software such as Adobe Acrobat XI is better than older versions. However, your best efforts can be defeated if you use a weak password that can be hacked by any number of freely available password-cracking programs. A quick Google search, for example, turns up a host of these programs—some of which may install malware on your computer in addition to the software.

The convenience of using this method is somewhat tempered by the fact that, while the attachment is encrypted, the e-mail itself is not and its metadata can be "sniffed," revealing the sender and the recipient, the time sent, and more. Some experts claim that much information can be gleaned just by noting the volume of e-mail sent between parties. An increase in the level of e-mail, for example, could indicate something important is happening.

Individual encrypted e-mail

Here, both parties use a commercial encryption application to encrypt and decrypt messages and attachments. This is typically combined with attaching a digital signature to the e-mail. According to Wikipedia:

> A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny having sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.[3]

Encryption combined with a digital signature assures the recipient that the communication was not altered and was sent by the right person.

A good encryption program can be difficult and cumbersome to use, and both you and your client must have the program for it to work. Some systems allow you to send an encrypted message without the client having the same program installed, but the client usually cannot respond with an encrypted message.

Some firms install a specific device on their network—such as an encryption management server—that encrypts all e-mail without the user's intervention and forces security compliance. It also manages and stores the keys used to encrypt and decrypt messages, making the user's experience that much easier. This requires the all-important buy-in from your clients (not to mention your staff).

Third-party secure services

Although some service providers allow for the secure transfer of information, security expert Bruce Schneier warns in his blog that the National Security Agency is actively trying to penetrate and break these services.

The notorious Edward Snowden purportedly used Lavabit, a secure e-mail service designed to protect users' privacy. However, the U.S. government served the company with a court order to turn over the private SSL key that would allow it to read all the e-mails on the service. Lavabit complied but closed soon after, citing an inability to safeguard customers' privacy. At least one other secure e-mail service company was also reported to have closed to avoid being caught in a similar situation.

Other companies still offer secure e-mail services, but the risk remains that they, too, will close and your communications may be lost.

Wi-Fi and mobile computing risks

For very good reason, most organizations have a policy that confidential information is not to be transferred through any public (i.e., unsecured) Wi-Fi network.

Kaspersky Lab, the Internet security company, states:

> In a recent survey, 70% of tablet owners and 53% of smartphone/mobile phone owners stated that they use public Wi-Fi hotspots. However, because data sent through public Wi-Fi can easily be intercepted, many mobile device and laptop users are risking the security of their personal information, digital identity, and money. Furthermore, if their device or computer is not protected by an effective security and anti-malware product...the risks are even greater.[4]

Risks of public Wi-Fi are identified in "6 wireless threats to your business," an article published on Microsoft.com. Also, in "Convenience or security: you can't have both when it comes to Wi-Fi," TechRepublic warns about the Wi-Fi Pineapple device, which captures passwords and other sign-on credentials when people use public Wi-Fi. In my view, this is enough evidence that every workplace should prohibit the exchange of client or other work-related communications via unsecured public Wi-Fi.

Secure client portals

Another alternative to e-mail is using a secure client portal. A portal is a private web page that allows only authenticated and authorized users to access digital files, calendars, and other information via a browser. The advantage is that nothing travels along the e-mail backbone of the Internet; all communications take place within the portal.

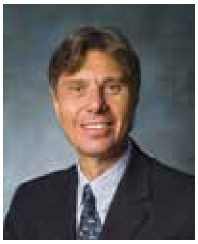
Wikipedia has this to say about lawyers and secure client portals:

> Due to the nature of the industry, law firms make up a significant amount of client portal users. This is because lawyers are constantly collaborating and interacting with clients, involving a significant amount of paperwork. In these cases the file sharing functionality is imperative.[5]

Conclusion

It is a matter of judgment as to the appropriate level of security to place on attorney-client communications, knowing that ordinary e-mail is not very secure. After all, everyone has secrets... ■

This article previously appeared in the Benchers Bulletin, *2014 No. 3 Fall, published by the Law Society of British Columbia.*



David J. Bilinsky is a practice management consultant and lawyer for the Law Society of British Columbia. He is a Fellow of the College of Law Practice Management and former editor-in-chief of the ABA's Law Practice Magazine. *He is the founder and chair of the Pacific Legal Technology Conference and a past co-chair of the American Bar Association's TECHSHOW. You can contact him at daveb@thoughtfullaw.com.*

ENDNOTES

[1] Wikipedia, *Email privacy* (last modified April 10, 2015) <http://en.wikipedia.org/wiki/Email_privacy>. All websites cited in this article were accessed April 19, 2015.

[2] Gray, *Hackers linked to China sought Potash deal details: consultant,* The Globe and Mail (November 30, 2011).

[3] Wikipedia, *Digital signature* (last modified April 7, 2015) <http://en.wikipedia.org/wiki/Digital_signature>.

[4] Kaspersky Lab, *Public Wi-Fi Security* <http://usa.kaspersky.com/internet-security-center/internet-safety/public-wifi#.VTUgsFJFBMg>.

[5] Wikipedia, *Client portal* (last modified March 20, 2015) <http://en.wikipedia.org/wiki/Client_portal>.