Making your e-communications secure*

♫ Everyone has secrets
Don't tell anyone … ♫
Lyrics by Kim Eana, recorded by Kpop

These days, with the Snowden revelations and news of continual large-scale surveillance of the internet by the "Five Eyes" (USA, Britain, Canada, Australia and New Zealand), there is increasing interest in how to protect solicitor-client communications. Solo and smaller firms are now inquiring about how they can send and receive secure emails and documents with their clients, as they are concerned about the perceived lack of privacy when using traditional email. There is the increasing realization that ordinary email may not be a great way to communicate with your clients. Wikipedia states:

> *After 180 days in the U.S., email messages stored on a 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 email from a provider. Other countries may even lack this basic protection, and Google's databases are distributed all over the world.*

But there are other reasons for sending secure communications, aside from concern that governments may be reading our emails. All of us, at one time or another, have sent an email 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 on 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) is encrypted, however, the substance of the message is still secure.

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.*

There are several ways you can make your communications more secure and protected 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, then you have totally avoided 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 or 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 email 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 email: You can use ordinary email to deliver a fully encrypted document as an attachment. The email need only say "Please see attached." Again, the password or phrase to decrypt the document must be exchanged securely with your client.

"Making your e-communications secure" Practice tips, was written by Dave Bilinsky,
Practice Management Advisor with the Law Society of British Columbia
and published in the Law Society British Columbia BENCHERS' BULLETIN, 2014: No. 3 FALL

Encryption security is only as strong as the password protection in your application. Newer software, such as Adobe Acrobat version 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, will turn up a host of password-cracking applications– some of which may install malware on your computer in addition to the cracking software.

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

Individual encrypted email: Here, both parties use a commercial encryption application to encrypt and decrypt a message and any attachments. This is typically combined with attaching a digital signature to the email. 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.*

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 need to have the system in order for this to work. There are systems that allow you to send an encrypted message without the client having the same program installed, but the client usually cannot respond with their own encrypted message.

Some firms have installed a specific device on their network that encrypts all email without the user's intervention, such as an encryption management server, 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 would require that all important buy-in from your clients (not to mention your staff as well).

Third-party secure services: There are service providers that allow for the secure transfer of information. However, security expert Bruce Schneier warns in his blog that the NSA is actively trying to penetrate and break these services.

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

Other companies still offer secure email services, but there is always the risk 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. Kapersky Lab, the internet security company, states:

> *In a recent survey, 70% of tablet owners and 53% of smartphone / mobile phone owners stated*

"Making your e-communications secure" Practice tips, was written by Dave Bilinsky,
Practice Management Advisor with the Law Society of British Columbia
and published in the Law Society British Columbia BENCHERS' BULLETIN, 2014: No. 3 FALL

> *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.*

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," Tech Republic 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 email is to use a secure client portal. A portal is a private webpage that provides access to authenticated and authorized users only via a browser to digital files, calendars and other information. The advantage of a secure client portal is that nothing travels along the email 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.*

Conclusions: It is a matter of judgment as to the appropriate level of security to place around solicitor-client communications, knowing that ordinary email is not very secure at all. After all, everyone has secrets ...

"Making your e-communications secure" Practice tips, was written by Dave Bilinsky, Practice Management Advisor with the Law Society of British Columbia and published in the Law Society British Columbia BENCHERS' BULLETIN, 2014: No. 3 FALL