she shares a similar background.

"There's an immediate relaxing," Recalma said. "When I first meet an Indigenous client, I ask, 'Where are you from?' Our identity is very much connected to where we're from. When they learn where I am from there is just a moment of recognition that we have a common, or shared history."

"One stereotype is that Indigenous people are silent, or that we don't express ourselves well because we do not understand an issue. Well, that's not the case. We are articulate and have a clear understanding of our own situations and certainly strong opinions on how best to move forward. Although I agree that there can sometimes be a hesitance when expressing opinions while navigating the justice system, I believe that hesitance is rooted in a lack of trust with an institution that's generally been used as a tool against us."

Hilland hopes the program can help increase the number of Aboriginal lawyers in the province, thereby serving smaller communities outside the Metro Vancouver where there is a greater proportion of Indigenous populations.

"Canadian law is for all of us, but there are some unique aspects of our laws that apply directly and specifically in connection with Aboriginal peoples. I am not just referring to the large basket of 'Aboriginal law,' constitutional rights-based issues, but to other areas of law as well, such as criminal, family, administrative, elder, child welfare, and so on, that also require the Aboriginal perspective."

– Tina Dion

"A lot of Aboriginal lawyers from smaller communities feel connected to communities and generally feel inclined to work there," Hilland said. "Aboriginal lawyers have a propensity to serve Aboriginal people."

And, while the Aboriginal Lawyers Mentorship Program provides an obvious benefit to Aboriginal lawyers and Aboriginal people in the province, the mentors have found that fostering junior lawyers by providing cultural or career guidance can be extremely rewarding.

"If offering my time, experience and advice will assist an Aboriginal student or new call get into, and not only remain, but advance within the profession, then I am happy to do so because their participation enhances the diversity necessary in our profession," Dion said.

"Ultimately, it is about feeling like we belong in this profession – because we do."❖

Some of the mentors who participated in the first year of the program (left to right): Andrea Hilland, Anja Brown, Cheryl Sharvit, Tina Dion and Maria Morellato, QC.

PRACTICE TIPS, by Dave Bilinsky, Practice Management Advisor

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) are 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.

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 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," 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 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 …❖

Services for lawyers

Practice and ethics advisors

Practice management advice – Contact **David J. (Dave) Bilinsky** to discuss practice management issues, with an emphasis on technology, strategic planning, finance, productivity and career satisfaction.
email: daveb@lsbc.org tel: 604.605.5331 or 1.800.903.5300.

Practice and ethics advice – Contact **Barbara Buchanan**, **Lenore Rowntree** or **Warren Wilson**, QC to discuss ethical issues, interpretation of the *Code of Professional Conduct for British Columbia* or matters for referral to the Ethics Committee.
Call Barbara about client identification and verification, scams, client relationships and lawyer/lawyer relationships.
Contact Barbara at: tel: 604.697.5816 or 1.800.903.5300 email: bbuchanan@lsbc.org.
Contact Lenore at: tel: 604.697.5811 or 1.800.903.5300 email: lrowntree@lsbc.org.
Contact Warren at: tel. 604.697.5857 or 1.800.903.5300 email: wwilson@lsbc.org.

All communications with Law Society practice and ethics advisors are strictly confidential, except in cases of trust fund shortages.

◆

Optum Health Services (Canada) Ltd. – Confidential counselling and referral services by professional counsellors on a wide range of personal, family and work-related concerns. Services are funded by, but completely independent of, the Law Society and provided at no cost to individual BC lawyers and articled students and their immediate families. tel: 604.431.8200 or 1.800.663.9099.

◆

Lawyers Assistance Program (LAP) – Confidential peer support, counselling, referrals and interventions for lawyers, their families, support staff and articled students suffering from alcohol or chemical dependencies, stress, depression or other personal problems. Based on the concept of "lawyers helping lawyers," LAP's services are funded by, but completely independent of, the Law Society and provided at no additional cost to lawyers. tel: 604.685.2171 or 1.888.685.2171.

◆

Equity Ombudsperson – Confidential assistance with the resolution of harassment and discrimination concerns of lawyers, articled students, articling applicants and staff in law firms or other legal workplaces. Contact Equity Ombudsperson, **Anne Bhanu Chopra**: tel: 604.687.2344 email: achopra1@novuscom.net.

Ethics Committee opinions

THE ETHICS COMMITTEE has approved these opinions for publication as guidance for the profession.

ADVANCING FUNDS TO A CLIENT TO COVER THE COST OF DISBURSEMENTS, MEDICAL EXPENSES OR LIVING EXPENSES

It is common practice for lawyers to pay the cost of client disbursements, particularly when clients are unable to afford them and the lawyer expects the funds to be recovered when the case is resolved. This practice is not contrary to the rules, and some court decisions have approved it: see *Franzman* v. *Munro* 2013 BCSC 1758 and *Chandi* v. *Atwell* 2013 BCSC 830 (currently on appeal). Less common, but a not infrequent practice, is when a client's financial situation compels a lawyer to advance funds to pay for the client's medical treatment or living expenses.

The *BC Code* has a number of provisions that restrict and regulate the circumstances under which lawyers can advance funds to clients. The following summary is intended to assist lawyers to stay within the rules.

When a lawyer pays the client's disbursements and charges interest on those costs, the lawyer must:

- disclose the charge in writing in a timely fashion (rule 3.6-1);
- ensure the charge is fair and reasonable (rule 3.6-1); and
- ensure the client consents to the charge (rule 3.6-1).

When a lawyer advances funds to a client to cover expenses other than disbursements (such as medical costs and living expenses), and charges interest on those costs, the lawyer must:

- disclose the charge in writing in a timely fashion (rule 3.6-1);
- ensure the charge is fair and reasonable (rule 3.6-1);
- ensure the client consents to the charge after receiving independent legal advice (rule 3.4-28); and
- be in compliance with *BC Code* rule 3.4-26.1, which prevents a lawyer from advancing funds to a client if there is a substantial risk that the lawyer's loyalty to or representation of the client would be materially and adversely affected by the lawyer's relationship with the client or interest in the client or the subject matter of the legal services. In practical terms, this means that a lawyer may not advance funds to a client if the advance would reasonably be expected to affect the lawyer's professional judgment. Depending on such matters as the size of the loan, the strength of the client's case, the client's chances of repaying the loan if the case fails and the lawyer's own financial circumstances, the loan may cause the lawyer to prefer his or her own interest in being reimbursed to that of the client's cause.

Lawyers who have questions about how these standards affect their practices may discuss the issue with a Law Society practice advisor or ask the Ethics Committee for guidance in a particular case.

JOINT RETAINER BY POLICE OFFICERS UNDER INVESTIGATION

In response to Commissions of Inquiry into police-related deaths, the BC Legislature established the Independent Investigations Office (IIO) to investigate incidents of death or serious harm involving police officers and special provincial constables in the province. The IIO opened in September 2012. Part 7.1 of the BC *Police Act* requires the IIO to investigate "incidents" in which police may have caused death or serious harm, including, but not limited to, criminal activity by the police.

All provincial police agencies have entered into a Memorandum of Understanding (MOU) with the IIO to enable the IIO to coordinate its investigations into police incidents. Section 15 of the MOU provides:

> 15.1 To prevent contamination of evidence, officers involved in or present during an incident which may fall within the jurisdiction of the IIO shall not communicate their accounts or recollections of the incident directly or indirectly to anyone other than an IIO investigator, except for communication that is necessary for:
>
> (a) public safety and obtaining medical care for injured persons;
>
> (b) the securing or identification of evidence;
>
> (c) the furtherance of concurrent investigations;
>
> (d) obtaining advice from legal counsel or a police association representative;
>
> (e) obtaining health care for an officer; or
>
> (f) any other purpose that is agreed upon by the IIO investigator and the police service liaison officer.

BC Code rules 3.4-5 to 3.4-9, which cover joint retainers, require that, before a lawyer is retained by more than one client in a matter or transaction, the lawyer must advise each of the clients that:

(a) the lawyer has been asked to act for both or all of them;

The committee has concluded that, as a general rule, a lawyer should not jointly advise or represent two or more police officers under investigation for, or witnesses to, a serious incident that arose in the course of their duties.

(b) no information received in connection with the matter from one client can be treated as confidential so far as any of the others are concerned; and

(c) if a conflict develops that cannot be resolved, the lawyer cannot continue to act for both or all of them and may have to withdraw completely.

The IIO has asked the Ethics Committee whether a lawyer may jointly advise or represent two or more police officers who are under investigation for, or witnesses to, a serious incident that arose in the course of their duties.

The committee is of the view that the MOU would place a lawyer retained to act for more than one police officer