


TECHNOLOGY

BY THOMAS L. SPRAGGS,
SPRAGGS & CO.
LAW CORPORATION &
MICHAEL MCCUBBIN
SINCLARE & COMPANY

Tom runs Spraggs & Co. Law Corporation, an injury litigation boutique. He holds a Bachelor of Laws, Master of Laws, and Masters of Business Administration. His law firm has experienced significant growth over the last several years, and his lifelong passions for technology and learning have helped him develop unique approaches to collaborative work processes and practice management. Tom's work has been primarily in civil litigation, but he also has a strong interest in administrative law and governance. He has been a frequent participant in the CLEBC Solo and Small Firm Conference, sitting as 2017 Course Chair.

Michael is a Courtenay based lawyer practicing with Sinclare & Company after running his own firm in Vancouver for seven years. He has a general civil litigation practice, including professional regulation and administrative law. He also assist clients as a solicitor in corporate maintenance, commercial transactions, and risk management. Michael is the current chair of the Pacific Legal Technology Webinar series and frequently speaks on legal technology topics.

INCREASING INTERNET SECURITY WITH A VPN

"Hardware is easy to protect: lock it in a room, chain it to a desk, or buy a spare. Information poses more of a problem. It can exist in more than one place; be transported halfway across the planet in seconds, and be stolen without your knowledge."

– BRUCE SCHNEIER,
PROTECT YOUR MACINTOSH, 1994

INTRODUCTION

With more lawyers practicing on the go, connectivity to the office to retrieve email and documents is a good productivity habit. The mobile office and portability of work are easier and more cost-effective than ever before. Connections through public and private wireless hotspots and networks negotiate the delivery of this information which is often of a private and confidential nature.

Is there a chance that the information being sent and retrieved could be compromised? Is there a way to help better manage that threat? If you are interested or concerned, read on to learn about the benefits and limitations of subscribing to a service that offers a Virtual Private Network or as it is commonly known, a "VPN." If you frequently use free Wifi or connect to unsecured websites, a VPN may be an essential tool for your digital life.

THE INTERNET SECURITY LANDSCAPE

The average internet user is likely unaware of the complex technologies that allow computers to connect and what types of information is transmitted. Behind every internet connection is some form of ISP which is short for Internet Service Provider. The ISP allows you to surf the internet and connect to the increasingly popular cloud services that are now becoming necessities of business and life in general. From purchasing movie tickets with a credit card to hosted productivity applications like Microsoft Office 365 or Google's G-Suite for business, all that is required is a reasonably modern computer with an internet connection. Any work done in the cloud is a function of a connection that is originated with an ISP.

Your ISP knows a lot about what you do online. Any website that is not prefixed with HTTPS and only HTTP would allow the ISP to know usernames, passwords and payment information linked with any accounts. If the connection is secure as represented by HTTPS, the ISP will know which sites have been visited and how long a user has spent on that site but no further details. Even with an encrypted website, your ISP will have a record of the unencrypted metadata[1] that can be harvested and used to make educated assumptions about activities especially when that data is provided through the internet of things (IoT) devices like smart tvs and appliances. Even your smart thermostat is collecting and using metadata in the name of comfort and convenience.

VIRTUES OF THE VPN

A VPN is often described as a tunnel between two computers. The VPN encrypts the data between computers through the internet making hacking and intercepting communications much more difficult.[2] VPN's became popular with Canadians a few years ago when attempts to "spoof [3]"a geographic location was done so consumers of Netflix and other geographically restricted content delivery platforms could be accessed more freely. Netflix has recently deployed technology measures to combat the VPN users.

VPN's are quite easy to set up and use. They do not require any special technical skills to configure properly.

EMAIL

Electronic mail was never designed to be the centre of our digital communications. Simply put, email was not designed with any privacy and security in mind.[4]

More succinctly, your email can be read by a variety of domain administrators,[5] this is concerning from a technical perspective. One of the best ways to properly view unencrypted email is that it is akin to a postcard that can be read by the mailman or anyone who might handle it. Encrypting email sounds like a solution but is largely impractical because of the difficulties of providing everyone you email an encryption key to read and send emails. The only way encrypted email works practically is if it is to a dedicated closed group of recipients. Fortunately, most non-spam email is already encrypted by the large hosting service providers. For example, Gmail to Gmail users are encrypted within Gmail.

In those situations, there are better solutions.[6] A VPN can help mitigate email security risks as it reduces the potential for email to be intercepted as it goes from bouncing from multiple mails servers around the planet to a dedicated tunnelled connection.

COSTS AND PROVIDERS

There are a number of VPN providers offering services. Some VPN providers also offer dedicated apps for the Apple IOS and Android operating systems. These apps enable mobile phones to leverage VPN technology and with increasing volumes of data originating from handheld and tablet devices, a more secure mobile computing experience is available. The chart below outlines some popular providers and the subscription fees.

NordVPN[7]	$2.99 per month
ExpressVPN[8]	$6.67 per month
Purevpn[9]	$10.95 per month
CyberGhost VPN[10]	$12.99 per month

LIMITATIONS OF VPN'S

A VPN is not an internet connection; it is simply a more secure connection to the internet and as such has some limitations. Some VPN providers have different levels of encryption. Some encryption may slow down internet speeds. There may be a trade-off between usability and security depending on the speed of your connection. For example, while a public wifi network is risky; many users may wish to avoid VPN's as it can slow the speed of data transfer due to encryption.

VPN's may also trigger security alerts when transacting with more secure web processes such as banking. Some VPN providers also may log user information and be subject to laws and interests of foreign jurisdictions. Some low or free VPN's also likely resell the user data, largely defeating the intent of a VPN.

Researching what might be best for you and your comfort level is a must. While a VPN may be worth considering as an additional layer of security, it will not be a substitute for an enterprise-grade firewall at your main office.

CONCLUDING REMARKS

The origins of the internet were a bunch of shared computers with limited data transfer speeds and processing capabilities. Fast forward to 2019, computers and data transfer speeds have improved those processes exponentially and at reduced costs. Technology and security are a bit like opposite sides of a scale, one of the biggest challenges facing lawyers and law firms is the desire to provide fluid and accessible access to information while maintaining security. There is no single simple solution, but awareness of security can assist in achieving a balance between access to information and implementation of appropriate security standards.

The ability for your communications to be stored, intercepted and mined is now making encrypted communications the wise choice for users who care about maintaining privilege and confidentiality. A VPN, like an anti-virus, may be a good option when connecting on the road away from any trusted ISP. V

1. Metadata is often used to describe information about the content of an item. For example, an image is described in metadata by including information about the size, depth, and colour of the image. Metadata often would also include the date the image was created and accessed. https://techterms.com/definition/metadata
2. https://www.pcmag.com/article/352757/you-need-a-vpn-and-heres-why
3. Hiding or changing your location is often viewed very negatively by online content providers. https://www.comparitech.com/blog/vpn-privacy/change-location-chrome-firefox-spoof/
4. Spying on the Smart Home: Privacy Attacks and Defense on Encrypted IoT Traffic Apthorpe, N., Riesman, D., Sundaresan, S., Narayanan, A., &Feamster, N. (2017).
5. https://www.digitaltrends.com/computing/can-email-ever-be-secure/
6. Future articles will discuss electronic communications alternatives. Client communication portals are becoming increasingly useful and accessible for practitioners.
7. www.nordvp.com
8. www.expressvpn.com
9. www.purevpn.com
10. www.cyberghostvpn.com