THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

Technology Law

Patrick W. Stufflebeam
HeplerBroom LLC, Edwardsville

VPN and Chill

Recently, I was flying home from Chicago to St. Louis. A woman sat down next to me, and as soon as allowed, immediately got her laptop out and logged in to the in-flight Wi-Fi. A true road warrior, I thought. She was on a 50-minute flight and was not about to lose a second to knock out those last few revisions to a report. She was not working, however, she was shopping. And before long, she had her credit card out and was hitting buy.

It made me wonder if she had given any thought to typing in her credit card information over an open Wi-Fi network. I know I have written before about the use of Virtual Private Networks or VPNs, but after talking with a number of other lawyers, I was surprised how few utilize a VPN on his or her devices—even on open networks.

To be clear, open Wi-Fi networks pose a large security risk to anyone on that network. I advise everyone to avoid open Wi-Fi networks if at all possible. I also caution everyone never to transmit any private information over an open Wi-Fi connection. Software is readily available to intercept your data packets (the computer translation of what you entered) and attempt to intercept. Login usernames and passwords become very vulnerable.

There are times, however, when you have no choice but to use an open Wi-Fi connection—like on an airplane. Using your credit card with its fraud protection to purchase the latest Lebron-inspired suit-shorts from a reputable shopping website utilizing HTTPS encryption may be worth the risk to you. What if you are emailing privileged information? Or, what if your username and password have been intercepted while trying to access an unsecure cloud storage service with client documents? You may not be taking reasonable efforts to safeguard client data.

The original internet was not designed for security. In the 1960s and 1970s, the concepts and protocols that power the modern internet were just being invented. Today, the internet and ways to connect to it are continually expanding. As lawyers, we need to be aware of how we conduct our work on the internet in a secure and potentially private way.

Security and privacy are not the same. Each requires trade-offs. Security is the principle of safeguarding data. "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Ill. R. Prof'l Conduct R. 1.6. All inadvertent disclosure is not necessarily a violation of this rule. The rule requires "reasonable efforts" to prevent the disclosure. A client, however, may mandate additional efforts. Lawyers should closely examine all client guidelines and work with clients to verify any specific security requirements of the client. For example, some clients may mandate multifactor authentication when accessing client data. Clients may also mandate how its data is stored, *e.g.*, encrypted at rest on your firm's server and never placed on a portable device such as a laptop or flash card. **Privacy, on the other hand,** is not about the data, but rather, the desire to remain anonymous.

We teach our employees that the weakest link between the user and a data breach . . . is the user. Phishing emails are sophisticated. Laptops are easily stolen. Corporate espionage exists. And, if you are on a network that you do not own or control, you should consider it an unsecured network.

VPNs can not only help you maintain privacy, but also secure data when connecting to the internet. VPNs utilize a tunneling protocol that creates a virtual tunnel around the data you are transmitting to and from your computer. Then, the VPN encrypts your data traveling through the virtual tunnel (if configured correctly). Therefore, if a hacker was trying to reach your data, he or she would first encounter your VPN tunnel. If the attack was sophisticated enough to penetrate the tunnel and intercept any of your data packets, the hacker should not be able to interpret the data because it has been encrypted. Therefore, even if you use a VPN, it is important to make sure you use a strong encryption algorithm. Find a VPN that offers AES-128 or AES-256 encryption.

The VPN's tunneling protocol is always on guard monitoring for penetration threats. If the VPN believes an intrusion is detected, the tunnel is automatically shut down and reestablished. Unfortunately, there are always trade-offs. The higher the encryption and the more security protocols you use, the slower your connection will be.

Think of your home network. If you are like many, you have a modem that is connected to a router that creates a wireless access point. You then connect to the wireless access point to gain access to the internet. Your internet service provider, *e.g.*, Spectrum, will assign you a public Internet Protocol Address (IP Address). Your public IP address can reveal a lot about you. It can geolocate you. Have you ever wondered why you get ads for the pizzeria down the street when using Google Chrome? Although it may not pinpoint your address, it may get close. If you want to know, google "what is my ip address?" Cell phones do the same thing.

When you use a VPN, you use your IP address to connect to one of your VPN's servers. Subsequently, all of your traffic is routed through the VPN's server, creating the virtual tunnel for your online traffic to travel. Because of your VPN tunnel, your ISP provider should not be able to see any website you visited or any data transmitted over the connection.

Not all VPNs are the same. One consideration, if privacy is a high concern, is whether your VPN logs your sessions, *i.e.*, although your ISP's IP address is shielded, your VPN still knows your IP address and logs every website you visited. Such information may be especially important if you are representing international defendants, who may be subject to restrictive nation states.

You should also consider where your VPN is headquartered. For example, a VPN provider located in the US may be subject to different law enforcement than, say, a VPN provider headquartered in the British Virgin Islands. If your VPN provider keeps zero logs on its users, however, it does not matter where you visited or servers to which you connected because even with a governmental request, there is no data to provide.

VPNs are no longer just a security and privacy tool reserved for large organizations with sophisticated IT departments. There are numerous VPNs targeted directly to consumers. Sometimes, VPNs even have benefits beyond encryption and privacy. For example, many of the mainstream VPNs have servers throughout the world. Many of your favorite websites may geo-restrict date, *i.e.*, if you are on your device outside of the United States, you will not be able to have access to those same websites because your IP address will identify you as a server in a restricted country. In that scenario, your VPN would allow you to connect to a server within the United States, and then connect to the same website and access the previously restricted data.

Another VPN benefit may just save you some money for getting to an international destination. It has been reported that when making travel arrangements, often times the price of the same flight may differ depending on where you are in the world. Therefore, you should use your VPN to compare flight prices from your local IP address to, say, one from a European country. So, the next time you can't afford NOT to go to Curacao, I hear the Marazul Resort is really nice.

THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

At the end of the day, every lawyer should have a VPN installed on every device he or she uses as it is a very affordable security measure.

About the Author

Patrick W. Stufflebeam is a partner in *HeplerBroom's* Litigation and Cybersecurity practice groups. He concentrates his practice primarily on the defense of civil litigation including toxic tort (asbestos, benzene, and mixed toxin), premises liability, product liability, and commercial litigation. Mr. Stufflebeam counsels clients and attorneys regarding cybersecurity and the use of technology in the law. He lives and offices in Edwardsville, Illinois (Madison County). He is admitted to practice in Illinois, Missouri, and the Southern District of Illinois. He received his J.D. from Saint Louis University School of Law and his B.A. from Western Illinois University. Mr. Stufflebeam is a frequent lecturer on many topics, most recently on the issues of legal technology and ethics. He is listed as AV Preeminent/Peer Reviewed by Martindale-Hubbell and a 2018 Leading Lawyer in the areas of Product Liability and Toxic Tort. He served as an elected Director of IDC from 2011-2017 and is also a member of the Madison County Bar Association.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at www.iadtc.org or contact us at PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, idc@iadtc.org.