Computer Security Tools & Concepts for Lawyers

Kendra Albert

Lawyers have ethical duties to their clients to keep information that is client confidential (learned in the course of the representation) secure and private.[1] Ethical boards have interpreted most uses of modern technology as consistent with this duty.[2] That includes storage of client confidential material in the cloud, so long as the lawyer takes basic precautions, including to (1) review and regularly revisit a vendor's terms of service, security practices, and restrictions on access to data; (2) follow clients' express instructions regarding use of cloud technology to store or transmit data; and (3) obtain client approval for storing and transmitting particularly sensitive client information via the internet.[3]

The fact that lawyers' ethical obligations do not prohibit them from using modern technology is certainly positive. But these steps, although ade-

---

Kendra Albert is an Associate at Zeitgeist Law and an Affiliate at the Berkman Klein Center for Internet & Society. *This paper was written in their personal capacity. It was last updated October 12, 2016, v4. Because computer security can be a fast-moving field, information related to particular products or services may be out of date.*

[1] ABA Model Rules of Professional Conduct, Rule 1.6.

[2] See Daniel Solove, Attorney Confidentiality, Cybersecurity, and the Cloud, LinkedIn Pulse (June 6, 2016), www.linkedin.com/pulse/attorney-confidentiality-cybersecurity-cloud-daniel-solove, ar-chived at perma.cc/EZ9U-SKAA.

[3] See, e.g., Ethics Opinions: Opinion No. 89-3 (June 9, 1989), www.massbar.org/publications/ethics-opinions/1980-1989/1989/opinion-no-89-3, archived at perma.cc/5AZG-KD27 (finding that a lawyer's use of a billing service equated with sharing their confidences with employees, which Disciplinary Rule 4-101(D) contemplates).

quate from an ethical perspective, do not necessarily provide substantive protection for client data, or fully encompass all reasonable efforts to prevent access or disclosure of client data. The Model Rules of Professional Conduct also state that lawyers must "act competently to safeguard information relating to the representation of a client against unauthorized access by third parties."[4] For that, lawyers must look away from ethical guidelines to the modern practices of computer and information security.

With an eye towards preserving client confidential information, this paper will provide an overview of some key concepts from computer security. Building on those concepts, it will suggest standard minimum practices for lawyers who are interested in securing their online lives, and thus the information of their clients. Simple steps, like use of a password manager, encryption of resting data, and two-factor authorization can greatly decrease the probability of unauthorized access to client data. Security of one's personal accounts is an important first step, and these steps can also be implemented in some practice settings.

Computer security can seem full of jargon and technical specifications that are unintelligible to the average lawyer. However, many of the core principles that underlie good security practices are intimately familiar. Security more broadly includes taking steps to ensure that confidential information does not leak due to people's bad actions, often called "operational security." This kind of thinking is not new to most lawyers. They often protect client confidentiality by not talking about sensitive information in public,[5] or shredding confidential papers rather than leaving them in a garbage can. But the introduction of technology can complicate and problematize commonly held notions about how operational security should work. Most lawyers have a good sense of what venues are appropriate for discussions of confidential information in physical space, but sometimes don't understand how those practices translate to virtual space.

We can contrast operational security with information security, which is the practice of defending information from unauthorized access, modification or disclosure. Information security is the literal technical processes

---

[4] ABA Model Rules of Professional Conduct, Rule 1.6 Comment [18].

[5] But see Kathryn Rubino, Lawyers Acting Badly on the Train, Above The Law (May 21, 2015), abovethelaw.com/2015/05/lawyers-acting-badly-on-a-train, archived at perma.cc/Y9S5-WY76.

or software changes that make certain computing devices more secure. When lawyers think about computer security, they often identify information security as the core goal – worries about hackers who break into computer networks abound. Steps for increasing information security are usually technical – they could include building software in a securable way or locking down key components of the network.

Information security is an important component of maintaining client confidences. Nonetheless, most lawyers are not in a position of control over the information security environment where they work. Additionally, most lawyers do not face targeted information security threats to clients on a regular basis. The major worry for most lawyers should not be well-resourced hackers breaking into their firm network, but rather the lost laptop, the chatty partner, and the reused password. Thus, most recommendations in this guide are based on operational security concerns.

As the Model Rules recognize,[6] good computer security practices are based around the concept of trade-offs. All security practices are costly, in terms of time, convenience, or actual money. Perfect security is not impossible – it is just so costly in terms of those three factors as to be an unrealistic choice. The goal should be for lawyers to pick a reasonable set of compromises between convenience and security. Any security choice should be made in terms of an analysis that compares the costs of being more secure, the risks involved in the information being revealed, and the likelihood that it will be revealed if the security step is not taken.

Overview of Key Security Concepts

With the difference in mind between operational security and information security, we'll now turn to some core concepts that help illuminate how to make better decisions about what security practices to put in place.

---

[6] "Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)." ABA Model Rules of Professional Conduct, Rule 1.6 Comment [18].

Threat modeling

An important component of security practice is the threat model. Threat models help determine what levels or steps for security might be appropriate. Basically, the idea behind threat modeling is that different risks require different protections. The steps to prevent or mitigate a thief stealing one's laptop to resell it are very different from the steps taken to prevent a litigation opponent from hacking into one's email server. Identifying one's threats is the key towards successful security practices.

Here are a couple of different threat models, which might apply to different areas of practice.

1. Non-Targeted Model:
   - Primary threat: attempt to gain access to client confidential data as part of a non-targeted attempt. In this threat model, the attacker is not targeting the lawyer or client in particular, but rather, just looking for vulnerable targets more generally.
   - For this threat, the best practices adopted by non-lawyers are likely appropriate, as they minimize risk without adding substantial overhead. These methods are discussed further in the "Basic Security Advice" section below.

2. Targeted Model:
   - Primary threat: attempt to gain access to a specific client's data. In this threat model, the attacker is targeting the lawyer or client specifically.
   - For this threat, methods that protect specific information are appropriate. This includes encrypting files and using secure communications methods.

3. Lawful Process Model:
   - Primary threat: the government or lawful actors attempting to access information through legal channels.
   - This threat model is outside the scope of this paper, and indeed, is relevant to very few lawyers. Those lawyers should take a very specific set of specialized precautions, and may want to adopt strategies that have high overhead costs if such strategies will prevent possible access by government.

Because these models are different and suggest different balances, the discussion below assumes the first, lowest risk model, except when otherwise noted. Sophisticated clients may view their files as particularly important, independent of threat, and so might request that lawyers use more caution. If so, lawyers should follow the general best practice of using communication methods that clients are comfortable with, in line with the Model Rules.

Social engineering

Social engineering refers to gaining information or access by manipulating people rather than technical systems. Phishing, or getting users to click on email links and "verify" information by submitting it to a third party, is a common form of this. Other methods include using information gained from attempting to reset one account to gain access to another,[7] or asking for an employee to help the hacker gain access to data they shouldn't have. (If you've ever gotten someone to let you into a building you didn't have a key for, either by following them in or by asking, that's social engineering.)

Social engineering is a term worth knowing because it demonstrates the importance of thinking holistically about security. Although some methods are highly technical, it can often be easier to get a target to divulge information or allow access without any technical expertise at all.

The best way to prevent social engineering is to be aware that it exists, to be cautious of emails that ask you to do unexpected things (log into accounts, change passwords, open unsolicited resumes or financial files), and to set up a culture that allows people to verify the authenticity of requests without feeling like they are wasting people's time. Lawyers who double check with clients re: files that are sent, with colleagues about suspicious activity, or with providers about password reset requests should be lauded for their caution. Additionally, one should be skeptical of unsolicited phone calls or emails from banks or other financial institutions. Rather than giving out important information on the spot, verify the number for the institution online or from a reputable, non-connected source and then call back or follow up.

---

[7] Mat Honan, How Apple and Amazon Security Flaws Led to My Epic Hacking, WIRED (Aug. 6, 2012), www.wired.com/2012/08/apple-amazon-mat-honan-hacking/, archived at perma.cc/R2Z7-UB2S.

Types of Encryption

Often, the term encryption is used as if it is a panacea for all kinds of security problems. It can be very helpful for protecting information, but different usages of encryption result in different kinds of protection.

At-rest encryption is encryption of data that resides on a device (data "at-rest"). Encrypting your computer or phone's hard drive is at-rest encryption. At-rest encryption generally prevents someone from accessing the information without an (encryption) key to the device.

In-transit encryption is encryption that covers data as it is moved from place to place. SSL/TLS, used to encrypt online shopping and banking transactions, is one prominent example. In-transit encryption comes in multiple types: channel encryption and end-to-end encryption. Channel encryption means that the data is secure against outsiders but the data can be known to the party that is transmitting it: for example, an email sent from a Gmail user may be encrypted on its way to Google's servers, between Google's various data centers, and then from its recipient to their computer. Google would be able to access the email, however, because they have access to the unencrypted information through their storage of the Gmail account, and they may also have the key to the encrypted links between servers. Channel encryption is secure so long as one trusts the party who is doing the transmitting.

This differs from end-to-end encryption, where the message is encrypted on one user's device and cannot be decrypted by anyone other than the user the message is intended for. Signal, PGP, and WhatsApp are examples of end-to-end encrypted messaging technologies. End-to-end encryption minimizes the chances that an outsider, lawful or unlawful, can gain access to the communications because they would have to compromise the end devices.

Lawyers should absolutely always be using channel-based encryption for their communications, and may want to use end-to-end encryption depending upon the use case and threat model.

Note that not all encryption is created equal. Although the full differences between different cipher suites, certificate providers, and TLS versions is outside the scope of this paper, it is worth noting that as a general rule, encryption becomes easier to crack over time and new vulnerabilities are patched regularly. Upgrading one's system regularly as new algorithms and protocol versions are released is vital to keeping data secure.

BASIC SECURITY ADVICE

An important note: no security advice is good for all threat models. Very high risk threat models may necessitate a totally different approach to security. Mileage may vary. All security advice is subject to change over time. Also, as a procedural matter, at this point, I'm switching over the tone of the paper to use the second person because saying "a lawyer should" all the time is quite awkward.

Use a Password Manager

Because of the technical tools used above for password cracking, the best passwords are long, randomly generated, and unique.[8] Humans are bad at both creating and remembering those types of passwords at a small scale; this makes it very difficult to remember the number of passwords needed for the many, many online services that require individual passwords. Thus, the best option is to use a password manager.[9]

A password manager is a program that includes tools both to generate passwords and to store them securely. It, in turn, is unlocked by an overall passphrase which should be long, unique, and easy to remember. XKCD's "Password Strength" comic explains the basic idea behind passphrases.[10] Long, unique and easy-to-remember passphrases can be generated using the "diceware" method, where you throw dice to create a string of numbers that correspond to words on a list, and then combine the words into a memorable phrase. Micah Lee's explainer on diceware provides step by step instructions.[11]

---

[8] See Dan Goodin, Why passwords have never been weaker – and crackers have never been stronger, ARS TECHNICA (Aug. 20, 2012), arstechnica.com/security/2012/08/passwords-under-assault/4/, archived at perma.cc/82QB-R7X5.

[9] April Glaser, You Need a Password Manager. Here Are Some Good Free Ones, WIRED (Jan. 24 2016), www.wired.com/2016/01/you-need-a-password-manager/, archived at perma.cc/GC6G-LNAH.

[10] Randall Munroe, Password Strength, XKCD, xkcd.com/936/, archived at perma.cc/X2GV-GE8U.

[11] Micah Lee, Passphrases That You Can Memorize – But That Even the NSA Can't Guess, The Intercept (Mar. 26, 2015), theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/, archived at perma.cc/5AVE-TQKL.

If you are using a password manager for the first time, you don't have to change all of your passwords at once; many password managers can import your existing passwords (either from memory or from your browser). Once your password manager is set up, you don't have to change all your passwords at once. You can just reset passwords as you use sites, slowly switching to unique passwords over time.

There are four current best-in-class options, depending on one's preferences and level of comfort: Encryptr, KeePassX,[12] LastPass,[13] and 1Password.[14] Each has different positives and negatives. In general, any of these password managers will work with a non-targeted model, whereas those worried about lawful process will want to make sure they are not using a manager with a recovery process controlled by a third-party.

- Encryptr (Windows, OS X, Linux, Android OS, iOS) is a commercial password manager produced by SpiderOak that is open source. It's free and does cloud syncing, without giving SpiderOak access to your passwords.
- KeePassX ("cross platform") is a free software option that is community developed, but has some sacrifices in usability and may not be best for non-technical users. It is also difficult to sync passwords across devices.
- LastPass (operating system independent, mobile apps available) uses cloud-syncing and stores hashed versions of the overall password on their servers, which is a centralized target. LastPass also allows for recovery of one's overall password once, based upon browser information, and requires a subscription to access some features. LastPass's servers have been a target for hackers.[15]
- 1Password (OSX, Windows, Android, iOS, web interface) has two different models, a subscription service and a license

[12] www.keepassx.org/.

[13] lastpass.com/.

[14] agilebits.com/.

[15] Joe Siegrist, LastPass Security Notice, LASTPASS (June 15, 2015), blog.lastpass.com/2015/06/lastpass-security-notice.html/, archived at perma.cc/GVZ8-SQPQ.

based model. The subscription service stores encrypted passwords centrally.[16] The license-based model stores the encrypted password file locally, although one can make back-ups and sync the file to multiple devices either over wi-fi or via Dropbox. The license-based model has more distributed risk, because there is no centralized database of overall passwords. But independent of option, there is no password recovery. If you forget your overall password, you are out of luck.

Although using a password manager is the best option for maintaining unique, strong passwords for many accounts, it is still worth memorizing a small number of important diceware passphrases for accounts that you cannot afford to lose access to: email or banking, for example.

Turn on Two Factor Authentication

Two factor authentication is a security method by which a service authenticates you using two different pieces of information.[17] Usually, this is based on two things: something you have and something you know. ATM access is an example of this model –the "something you have" is the ATM card, and the "something you know" is your PIN number.

For online accounts, two factor-authorization usually uses a password ("something you know") and a one-time or limited-time code ("something you have"). Two-factor authentication means that even if an attacker has your password, they still can't access your account without the additional code.

Most two-factor authentication schemes either use text messages (SMS) or authenticator applications (like Google Authenticator or Authy). A message is sent to you after you correctly enter your password into a site – you then must type in the code in order to access the account.[18] Many service providers offer two-factor authentication options, including Gmail, Outlook.com, Dropbox, Twitter, and Facebook.[19] Two factor authentication

[16] See 1Password, Security, 1password.com/security/.

[17] How to Enable Two Factor Authentication, SURVEILLANCE SELF DEFENSE, ssd.eff.org/en/module/how-enable-two-factor-authentication, archived at perma.cc/PJ5J-CBC5.

[18] See, for example, Google's 2 Step Verification page, www.google.com/landing/2step/.

[19] Two Factor Auth is a list of services that provide two factor authentication. twofactorauth.org/.

should be enabled for all accounts that contain client information and that are supported by the service provider.

If the option is offered, using an authenticator app is better than SMS for two-factor authentication. Authenticator apps usually function without a cell phone signal or network connection, which means that they can work in situations where SMS might block account log in, such as in other countries or in buildings without cell phone services. Also, if you are using a targeted threat model, SMS can be more easily compromised via contacting your cell phone provider or replacing your SIM card.[20]

Another form of two-factor authentication is USB authentication, such as a YubiKey.[21] This may be suitable for some high-risk threat models.

Provide Secure Communication Options

Obviously not all communications are potentially problematic if exposed. However, if the contents of the client communication are potentially sensitive, providing methods of discussion that are not susceptible to interception is an important step.

Perhaps the most well-known secure communication method is PGP/GPG.[22] PGP is a signing and encryption method which can be used for email, and allows for end-to-end encryption. PGP is not particularly easy to use, but can be a good solution for technically savvy lawyers or people with clients who are particularly concerned about government interception.[23] For high risk PGP applications, consult an expert as to setup and DO NOT solely rely on this guide.

The best guide to setting up PGP is the Electronic Frontier Foundation's Surveillance Self-Defense guide,[24] which works with a desktop email client.

---

[20] Emily Dreyfuss, @Deray's Twitter Hack Reminds Us Even Two-Factor Isn't Enough, WIRED (June 10, 2016), www.wired.com/2016/06/deray-twitter-hack-2-factor-isnt-enough/, archived at perma.cc/PC4N-CXQN.

[21] www.yubico.com/products/yubikey-hardware/.

[22] PGP stands for "Pretty Good Privacy" and GPG stands for "GNU Privacy Guard." GPG is the free software version of PGP and is widely used, however, people often refer to the implementations without distinguishing as PGP.

[23] Micah Lee, Ed Snowden Taught Me to Smuggle Secrets Past Incredible Danger. Now I Teach You, THE INTERCEPT (Oct. 28, 2014), theintercept.com/2014/10/28/smuggling-snowden-secrets/, archived at perma.cc/6D2S-32SW.

[24] For Macs: ssd.eff.org/en/module/how-use-pgp-mac-os-x. For Windows: ssd.eff.org/en/

If you primarily use webmail, Mailvelope may be a good solution. It's a desktop plug-in that allows for PGP use for Gmail, Outlook.com and Yahoo! Mail.[25] If using PGP or a similar email encryption service, it is important that the subject line of the email doesn't contain potentially confidential information – subject lines and recipients are not obfuscated by PGP.

For non-email communications, the best-in-class security solution is Signal, an open-source encryption communications platform developed by Whisper Systems.[26] Signal end-to-end encrypts text messages sent over data networks between Signal users, and has a key verification method.[27] Signal also allows for secure phone calls to other Signal users. There are also other solutions that aim to deal with similar problems – including Wickr,[28] which has ephemeral messaging for videos and photos, and allows for sending encrypted, expiring files.

Apply Security Updates and System Updates Promptly

System updates for devices or software are meant to fix recently discovered bugs or security holes, and security updates for browsers may protect against malware. Installing updates is actually one of the best defenses against common malware and viruses,[29] and is common practice among security experts.[30]

Encrypt Devices

All devices used to store client information should use full-disk encryption. That includes computers, phones, and tablets, as well as backups of

---

module/how-use-pgp-windows. For Linux: ssd.eff.org/en/module/how-use-pgp-linux/.

[25] www.mailvelope.com/.

[26] whispersystems.org/blog/signal/.

[27] For Android: ssd.eff.org/en/module/how-use-signal-android. For iOS: ssd.eff.org/en/module/how-use-signal-ios/.

[28] www.wickr.com/personal#features.

[29] Software Patches & OS Updates, MIT INFORMATION SYSTEMS AND TECHNOLOGY, ist.mit.edu/security/patches, archived at perma.cc/5K4V-A565.

[30] "New Research: Comparing how security experts and non-security experts stay safe online," Google Security Blog (July 23, 2015), security.googleblog.com/2015/07/new-research-comparing-how-security.html, archived at perma.cc/4JAD-JUMT.

any of these things. Full-disk encryption protects against a number of different threats, from client data leaking if an attorney's phone is left on public transit to if the FBI wants access to it.

Encryption software is built in on most modern computers – on Macs, it is called FileVault and is supported natively through the operating system.[31] Windows 10 includes encryption options with all versions, called BitLocker.[32] Earlier versions of Windows only included encryption for business or enterprise versions, however Veracrypt is an open source option for full disk encryption.[33] There are also Linux encryption options, like dm-crypt.[34]

Both iPhones and Android devices support full disk encryption on a system level. iPhones that are running iOS 8 or a later version of the operating system are encrypted by default,[35] whereas most Android devices have an option to turn on full disk encryption.[36]

As mentioned above, for all encryption, attorneys should use a strong, unique passphrase, ideally generated via diceware. For phone or tablet encryption, changing from the default numeric PIN to an alphanumeric password greatly increases the number and strength of possible passcodes and the security provided.

---

[31] FileVault, support.apple.com/en-us/HT204837.

[32] Bitlocker, windows.microsoft.com/en-us/windows-vista/bitlocker-drive-encryption-overview.

[33] Veracrypt is the successor to Truecrypt, which should no longer be used. veracrypt.codeplex.com/.

[34] Jeff Cogswell, How to Encrypt a Linux File System with DM-Crypt, LINUX.COM (June 23, 2015), www.linux.com/learn/how-encrypt-linux-file-system-dm-crypt. See also Disk Encryption, ARCHLINUX WIKI, wiki.archlinux.org/index.php/disk_encryption#Data_encryption_vs_system_encryption.

[35] How to Encrypt Your iPhone, SURVEILLANCE SELF DEFENSE, ssd.eff.org/en/module/how-encrypt-your-iphone.

[36] Full Disk Encryption, ANDROID OPEN SOURCE PROJECT, source.android.com/security/encryption/. See also Cameron Summerson, How to Encrypt Your Android Phone (and Why You Might Want to), HOW-TO GEEK (Apr. 17, 2016), www.howtogeek.com/141953/how-to-encrypt-your-android-phone-and-why-you-might-want-to/.

Encrypt Files

For client information that is rarely used, like social security numbers or back client files, attorneys should consider encrypting the files separately from the device. This covers a different threat model – individual file encryption can protect files even if an attacker gets access to the device or backup. There are a number of different tools to do this, but GPGTools, which can be used for PGP communication, makes it quite easy to do with a PGP key.

For larger sets of files, Veracrypt is a better option – it allows for the creation of encrypted file containers that can be moved from computer to computer securely, and it uses symmetric encryption, which is faster than asymmetric encryption methods like PGP.

Be Careful About Backups

Having backups of client files and other important information is a key step and part of any good recovery plan. However, if client files are backed up with a cloud services provider, or stored on an unencrypted backup hard drive, that can undo all of the hard work of encrypting the files in the first place. Storing material with a third party always creates another method by which it can be accessed, or, under a lawful process model, involves another company who could be forced by law enforcement to turn over information. Think carefully about what the best backup option is – some cloud services providers allow users to keep their own keys and use end-to-end encryption, which may be a good option to protect data under Targeted or Lawful Process threat models. Be sure to maintain control over your own encryption keys. If a cloud service has access to keys, it could be more easily compelled through legal process to provide access to your files.

Use a VPN when on public networks

Unsecured Wi-Fi (a network without a password or with a password everyone has access to, like a coffee shop) is vulnerable to packet sniffing, where someone else on the network looks at unencrypted wireless traffic to or from your device.[37] Additionally, it is possible to spoof unsecured

[37] Adam Pash, A Guide to Sniffing Out Passwords and Cookies and How to Protect Yourself Against It, LIFEHACKER (Oct. 26, 2011), lifehacker.com/5853483/a-guide-to-sniffing-out-

wireless networks, setting up a fake network that captures information from your computer.[38] Because of this, it's best to avoid using unsecured wireless networks, but if you must, use a VPN (virtual private network). VPNs route traffic through an encrypted tunnel to another network before reaching out to the broader Internet. To use a term from the encryption types above, they channel encrypt all wireless traffic, preventing an attacker from being able to see unsecured traffic on the network.

Free VPNs can often be problematic, because providers often do not have the best incentives to protect data,[39] but luckily, there are a number of low cost monthly subscription services for people who do not have access to a VPN through work or school. The ideal VPN service is one that turns on automatically when on unfamiliar networks, so you don't have to think about when to use it. For people who use primarily Apple devices, Cloak may be a good option.[40] There are some different sites that compare options.[41]

Minimize Information Available

Finally, the best way to prevent attackers from gaining access to your client information is to minimize the amount of client information that is available. While retaining client files can be important, it's recommended that you move sensitive but rarely used files to a safer location than your everyday computer. If most client information is on an encrypted back-up hard drive that is unconnected to the Internet, many attackers are going to have serious difficulties getting to it. Likewise, information that is not important to retain and is high risk for either you or your client should be deleted, securely.

---

passwords-and-cookies-and-how-to-protect-yourself-against-it, archived at perma.cc/GLJ5-TF6B.

[38] Troy Hunt, The Beginners Guide to Breaking Website Security with Nothing More than a Pineapple, TROYHUNT.COM (Apr. 17, 2013), www.troyhunt.com/the-beginners-guide-to-breaking-website/, archived at perma.cc/3KMT-MJUX.

[39] Alan Henry, How Do I know if my VPN Is Trustworthy?, LIFEHACKER (May 20, 2013), lifehacker.com/how-do-i-know-if-my-vpn-is-trustworthy-508866499, archived at perma.cc/G49P-BAAG.

[40] Cloak, www.getcloak.com/.

[41] Choosing the VPN That's Right for You, SURVEILLANCE SELF-DEFENSE, ssd.eff.org/en/module/choosing-vpn-thats-right-you. VPN Comparison Charts, thatoneprivacysite.net/.

Conclusion

For lawyers, taking steps to ensure the security of client information is not just a good idea, it is required under the ethical obligations of the profession. The techniques described in this paper provide a starting point for beginning to identify security risks, understand practices that can reduce risk, and implement changes without knowing too much about the technical side of computer security.