Encryption Basics for Lawyers

Introduction

Electronic communications and "cloud" based computing continues to expand for lawyers. We are also using more tablets, smart phones, jump drives, and other portable devices in our practice. As such, a basic understanding of encrypted communications and data storage is critical for attorneys attempting to protect their clients' confidential information in cyberspace. This pamphlet is designed to provide a basic understanding of encryption technologies available for use in a law practice. *This is a starting place only*, and you should evaluate in more detail which encryption and security requirements best fit your law practice.

What Is Encryption?

Encryption is the process of making readable text or data unreadable, usually for storage on a hard drive or for sending through a network from one computer to another computer. To make the information readable, one must know the decryption "key" (usually a password). When proper encryption is in place, the client's computer files are unreadable without using the key and any transfers of information about the client can only be read by those who know the key. (Think of the encryption as a lock and the key as, well, the key.)

Where Do You Store Your Clients' Information?

Where you keep your clients' data will dictate what kinds of encryption protocols you should implement. Do you have client information on smart phones (addresses, phone numbers, client documents, e-mails)? On laptops? External or portable hard drives? Flash or jump drives? Desktop computers locked behind office doors? Or, do you keep all your client files on the "cloud"? Do your office computers have access to the Internet? Can you access your office computers (and client data) from the Internet? Everywhere you have electronic data you should keep it encrypted when stored, especially if the computer or device is not locked behind physical barriers (like your office door).

"Cloud" computing, in particular, is challenging lawyers to secure their clients' information because the data is stored and accessed on remote servers not under the attorney's exclusive control. Cloud services like Dropbox and iCloud make syncing data across devices — devices usually places *not* behind lock and key — extremely easy, convenient, and useful for providing legal services to the client. However, simply leaving a client's confidential information sitting on the cloud's server — who-knows-where in cyberspace and real space — risks others having unauthorized access to that information. For example, Dropbox and other cloud companies' employees have access to the physical machines, the accounts, and some parts, if not all, of the data. Plus, those companies often control the encryption keys, not you. Nonetheless, by encrypting your client's data *before* it goes into the cloud, you can use these great services and still protect your client's confidentiality. Many programs, as addressed below, can be used to

Revised February 6, 2014

create encrypted partitions (parts of hard drives) or files that can be placed in the cloud. Likewise, some cloud providers permit you to encrypt your client's data with only a key you know (e.g., www.backblaze.com, www.spideroak.com, or http://www.boxcryptor.com). Either way, make sure your client's data is protected in cyberspace.

Portable Storage Devices Need Encryption

If confidential client information is stored on portable devices that leave the security of your office, they should be encrypted so that the information cannot be easily accessed if the device is stolen or used by unauthorized persons. The most obvious examples are smart phones and tablets. These devices are small and easily lost or stolen and can contain significant amounts of information about your clients. For example, unencrypted e-mails often contain client data, legal advise and instructions, scanned files and other records and information transmitted between clients and their attorneys. On the plus side, most newer smart phone versions (like Android and Apple) provide for encryption of the data on the phone when a password is set, as well as, options to find or remotely erase your data if the device is lost or stolen. However, unless you use a strong password (see below), you're leaving your client's data vulnerable. Jump dives, flash drives, and portable external hard drives can all be created with encrypted partitions and those partitions should be used to hold your clients' data files.

Transmitting Electronic Information Through a Network Needs Encryption

Most often this includes sending e-mails or text messages with confidential client information. Unless the e-mail and its attachments are encrypted, the message can easily be intercepted and read. Remember, e-mails are usually sent through multiple computer systems in route to their destination. Moreover, many "free" e-mail services (e.g., Google, Yahoo, AOL) actually have full access to their users content. Unencrypted information transmitted and stored through their systems can be read by the e-mail company, other "in transit" computer systems, or any other person who may be granted access to that data (for example, state or federal prosecutors, as a result of your opposing counsel's subpoena, or enterprising hackers). Protecting information when connected to public Wi-Fi networks is critical also. Whenever possible, use encrypted Wi-Fi links or VPNs to transmit data when on public networks (i.e., the airport waiting area).

How Do You Encrypt Your Data?

While the types and levels of encryption can appear complicated, most computer systems now offer easy to use encrypting software for both hard drives and electronic communications, may of these programs are open source and free. Most hard drive manufacturers now offer downloadable encryption software, for example Seagate (www.seagate.com), Hitachi, (www.hgst.com), Western Digital (www.wdc.com), or hard drives that come complete with encryption software already installed. Additionally, many programs exist that can create encrypted parts of your current hard drives or encrypt the entire drive. For example, PGP by Symantec (www.symantec.com), GnuPG (www.gpg4win.org for Windows; www.gpgtools.org for Mac), Mcafee (www.mcafee.com), or Sophos (www.sophos.com) as well as provide e-mail encryption and authentication capabilities.

Once you have an encrypted hard drive, you can "open," "launch," or "connect to" the drive only after entering the required key for the decryption. Once "unlocked" the encrypted hard drive can be used like any other. However, while the drive is "closed" the data remains on the hard drive in

an encrypted state . . . safe from unauthorized access (assuming you have a strong key). Current versions of Windows and Mac operating systems also have built in encryption capabilities to turn your computer's hard drive into Fort Knox. You just need to turn the encryption processes "on" in the systems' settings. As explained further below, however, strong access passwords are a critical part of encryption security.

"Key" Creations or "Don't Make Easy Passwords"

Encryption programs typically provide either symmetric or asymmetric encryption. Simply put, symmetric encryption means ONE key encrypts and decrypts the data. It must be kept confidential. Anyone who knows the key can decrypt and read any data encrypted with that key, so you can't easily share the key to let other people encrypt data for you. On the other hand, asymmetric encryption means there are TWO keys that interrelate to each other. The public key can be freely given out because it only permits the information to be encrypted, not decrypted. The private key, however, must be kept highly confidential because it permits the information to be decrypted and read.

Symmetrical encryption is often used to encrypt files, documents, or complete hard drives. Use one password to open or close the file, document, or hard drive. Asymmetrical encryption is often used for e-mail communications so that you can give out your public key to anyone. They can load that key into their encryption program (usually incorporated into their e-mail program) and send you encrypted e-mails and attachments. Only you can open the e-mails because only you have the private key. Likewise, to send an encrypted e-mail to someone else you would encrypt the e-mail with their public key so only they can open the e-mail with their private key. Most of the programs listed above, use or a combination of these methods to encrypt the information you want kept private. Similarly, these programs also allow authentication of e-mails and data through the public/private key process.

Of importance is making sure your keys and passwords are strong, not weak. Think of the 4 digit "pin" numbers. To guess a 4 digit pin, one needs only try the numbers 0000 through 9999 to correctly gain the key (10,000 possible combinations). A 4 digit key/password is weak and can be broken in a matter of about 11 seconds today. See GRC's Interactive Brute Force Password "Search Space" Calculator to test your password strength: www.grc.com/haystack.htm. (WARNING: Don't try your actual password, just one constructed in a similar fashion!!) To have a strong password, one that may take centuries to break, use a combination of at least 10 letters, numbers, or symbols. The password need not be totally random but should not be common, should be easy to remember, and personal to you. For example, don't use 1234567890; while long, it is easily guessed. Instead, think of passwords like: MyRainbowCow#3 or a full, but reasonably short, sentence: "SusanLikesTheNumber3!". "MyRainbowCow#3" forms a mental picture and is easy to remember. It is composed of random words combined together using both capital and lowercase letters ("My," "Rainbow," and "Cow") and includes a symbol "#" and a number "3." According to Gibson Research Corporation's Search Space Calculator, trying a brute force discovery of that password at *one hundred trillion guesses per second* would require 15.67 thousand centuries to guess it. Good luck!

The Bottom Line: Use Strong Passwords and Encrypt Your Clients' Data!

Encrypt any client data stored on you hard drives that are not locked behind your office doors. Then encrypt the computer behind locked doors anyway . . . offices are broken into all the time and passive security systems fail. Encrypt your clients' data over e-mail. If your clients are using a free e-mail service, strongly encourage them to switch to a service that does not require consent to view their data.