

## TECHGEAR

Microsoft's Surface Pro 3 (from \$799)



serves as both a tablet and a laptop, with Windows 8.1, a digital pen, and storage options intersecting in a lightweight device that can be used on its own or with an attachable keyboard.

## WEBLINKS



A shareholder in the Dallas office of Ogletree, Deakins, Nash, Smoak & Stewart, **ALICIA VOLTMER** represents clients in labor and employment matters. She is a member of the Academy of Hospitality Industry Attorneys and is certified in labor and employment law by the Texas Board of Legal Specialization. Voltmer graduated from California Western School of Law in San Diego and holds a bachelor's and master's degree from Southern Methodist University.

### nrn.com

*Nation's Restaurant News* covers trends and personnel changes in the food service industry to help practitioners keep pace with clients.

### bop.gov

The Federal Bureau of Prisons website features a "Find an Inmate" search for determining whether a person has served time.

### law360.com

This paid service, which can be customized to address labor and employment law, offers summaries of court and agency decisions, news commentary, and information on pending legislation.

### fossilrim.org

Fossil Rim Wildlife Center in Glen Rose is a leader in conservation efforts for various species. Its website provides information regarding tours and activities.

### imdb.com

When you want to know when the sequel to your favorite movie will be released, view a trailer, or can't remember a star's name, rely on this site.

# Lost in Translation

*What you need to know about encryption—and keeping client files secure.*

BY WILLIAM WADE MILLER JR.

We are using tablets, smartphones, USB flash drives, and other portable devices, and a basic understanding of encrypted communications and data storage is critical for attorneys attempting to protect their clients' confidential information in cyberspace. *This article is a starting place only*, and you should evaluate in more detail which encryption and security requirements best fit your needs.

**What is encryption?** Encryption is the process of making readable text or data unreadable, usually for storage on a hard drive or for sending from one computer to another computer. To make encrypted information readable, one must know the decryption "key" (usually a password). When proper encryption is in place, the client's computer files are unreadable and any transfers of client information can be read only by those who know 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 (addresses, phone numbers, client documents, emails) on a smartphone? On a laptop? External/portable hard drive? USB flash drive? A desktop computer 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 store electronic data, you should keep it encrypted, especially if the computer or device is not locked behind physical barriers.

Cloud computing, in particular, is chal-

lenging 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—which typically are *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, cloud company employees have access to the physical machines, the accounts, and some, if not all, of the data. Plus, the companies—not the users—often control the encryption keys. Nonetheless, by encrypting your clients' data *before* it goes to the cloud, you can use these great services and still protect their confidentiality. Many programs can be used to 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 clients' data with a key that only you know (e.g., backblaze.com, spideroak.com, or boxcryptor.com). Either way, make sure the 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, it should be encrypted in case the device is used by unauthorized persons. The most obvious examples are smartphones and tablets. For example, unencrypted emails often contain client data, legal advice and instruc-

tions, scanned files, and other records and information. On the plus side, most newer smartphone models provide a way to encrypt data when a password is set, as well as options for finding or remotely erasing data. USB flash drives and portable external hard drives can all be created with encrypted partitions, and these should be used to hold your clients' data files.

**Electronic information needs encryption.** Most often this includes sending emails or text messages with confidential client information. Unless the email and its attachments are encrypted, the message can easily be intercepted and read. Remember—emails are usually sent through multiple computer systems in route to their destination. Moreover, many free email services (e.g., Google, Yahoo, AOL) actually have access to their users' content. Unencrypted information transmitted and stored through their systems can be read by the companies, 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 the opposing counsel's subpoena, or enterprising hackers). Protecting information when connected to public Wi-Fi networks is also critical. Whenever possible, use encrypted Wi-Fi links or virtual private networks to transmit data on public networks.

**How to encrypt your data.** Most hard drive manufacturers now offer downloadable encryption software—including Seagate (seagate.com), Hitachi (hitachi.us), HGST (hgst.com), and Western Digital Technologies (wdc.com)—or hard drives that come with encryption software already installed. Additionally, many programs exist that can encrypt parts of your current hard drive or encrypt the entire drive, as well as provide email encryption and authentication capabilities, including PGP Technology by Symantec (symantec.com/encryption),

GNU Privacy Guard (gpg4win.org for Windows; gpgtools.org for Mac), McAfee (mcafee.com), or Sophos (sophos.com).

If you have an encrypted hard drive, you can open, launch, or connect to the drive only after entering the required key. 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 on encryption in the system's settings.

**Don't use 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 cannot easily share the key to let other people encrypt data for you. On the other hand, asymmetric encryption means there are *two* keys: the "public key," which can be shared because it permits only the information to be encrypted, not decrypted; and the "private key," which must be kept highly confidential because it permits the information to be decrypted and read.

Asymmetric encryption is often used for email communications so that you can give your public key to anyone. They can load that key into their encryption program (usually incorporated into their email) and send you encrypted emails and attachments. Only you can open the emails because only you have the private key. Likewise, to send an encrypted email, you would encrypt the email with the public key so only they can open the email with their private key. Most of the programs

discussed in this article use a combination of these methods to encrypt information. Similarly, these programs also allow authentication of emails and data through the public/private key process.

Of importance is making sure your keys and passwords are strong. To correctly guess a four-digit pin, one needs only to try the numbers 0000 through 9999 (10,000 possible combinations). Today, this can be broken in a matter of about 11 seconds. Try Gibson Research Corp.'s Interactive Brute Force Password "Search Space" Calculator to test your password strength at [grc.com/haystack.htm](http://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 at least 10 letters, numbers, and/or symbols. The password need not be totally random, but should be uncommon, easy to remember, and personal to you. For example, don't use 1234567890. Instead, think of passwords like "MyRainbowCow#3" or a sentence such as "SusanLikesTheNumber3!". "MyRainbowCow#3" forms a mental picture, is easy to remember, and is composed of random words using both capital and lowercase letters, a symbol, and a number. According to GRC's Search Space Calculator, a massive cracking scenario of that password at *100 trillion guesses per second* would take 15.67 thousand centuries.

**Bottom line: Use strong passwords and encrypt your clients' data.** Encrypt any client data stored on hard drives, and encrypt your clients' data over email. If your clients are using a free email service, strongly encourage them to switch to a service that requires consent to view their data. **TBJ**

**WILLIAM WADE MILLER JR.**

*is a partner in Green & Miller in Texarkana. Licensed in Texas and Arkansas, he practices general civil litigation with a focus on business, construction, and personal injury.*