

The Traveling Lawyer

By Jim Calloway

Technology today makes it possible to have virtually the entire set of tools that one would have in the law office almost anywhere one travels — except for your staff, of course.

Operating virtually works extremely well for lawyers. The major issue is devoting the time to learn about the available tools. While some amount of training may be needed for the lawyer to become an accomplished remote user, remote access is really more about advance planning and knowing the options than any superior level of technological expertise.

Let's examine the various methods of working on the computer while away from the physical law office environment.

E-MAIL ONLY

For most traveling lawyers, the basic tool for working on the road is having Internet access to login to check e-mail. Generally all that will be required for this arrangement is Internet access and a small laptop, perhaps even an extremely affordable netbook.

And, of course, it seems like every day new smart phones and smart phone apps are released, adding to the number of tasks one can now do from a smart phone. By definition, a smart phone should have e-mail access.

It appears that most lawyers now already check their office e-mail remotely from a home computer, a laptop and/or their phone. Since e-mail is the most popular method of electronic communication in our industry, a lawyer who does not have remote access to his or her e-mail is handicapped.

While the preferred method is to have some amount of remote access to office files by lap-

top computer, some lawyers have become so proficient at responding to their e-mail via their iPhone, Blackberry or other smart phones that this may meet their complete needs for accessing their e-mail outside the office.

Other lawyers will rely on web-based e-mail with either an account provided by their Internet service provider or online services like Gmail and Yahoo Mail. Some security experts have cautioned against the use of webmail, on security concerns or the terms of service of the user agreement. Other lawyers use Gmail regularly. Some lawyers even use Gmail for their primary office e-mail account.

The reason why many lawyers are satisfied with "e-mail only" access is that their staff back at the office can accomplish what cannot be done remotely with just e-mail, be it printing a document or scanning correspondence just received so that it can be sent to the lawyer as an e-mail attachment.

Of course, this only applies during business hours and if certain tasks could be done remotely without the need for staff intervention, it would free up the staff to do other tasks.

SECURITY

Internet security should always be a concern.

Wireless access over a WiFi network is only as good as the security applied by the individual who set up the wireless network. Generally speaking, you are always at risk when you logon to an unencrypted wireless network that

does not require you to have a password to access it. At the large national chain stores and coffee shops where free WiFi is offered, the risk is small if you have antivirus and firewall updated and running. I still would not do online banking on these connections.

For example, we have an unsecured network at the Oklahoma Bar Center that guests here can use. There is no need to login and a firewall offers protection from our guests being compromised externally over the Internet. Theoretically, one guest user with technical expertise might access another guest user's machine. There are safeguards against that and if our IT department didn't feel good about the service we wouldn't offer it. But it could not be considered perfect.

At the other end of the spectrum, if you are at an airport and notice a "Free WiFi" available on your laptop, there is a great likelihood that it is not a wireless access point but another computer somewhere in the airport broadcasting the signal. It is probably nothing dangerous, but could be waiting to capture credit card numbers, bank login information and other personal data. The airports that offer free WiFi will normally have signs all over touting it and explaining how to log in. Most airport WiFi access will be through a paid provider. (But at least it is safe to give the provider your credit card number.)

Anyone can go online or to a local store and pick up a wireless router for \$50 or less. So, to repeat, you are at the mercy of both the competence and the pure motives of the person who set it up. These WiFi hotspots, if left unsecured, could be a significant risk or a minimal one.

Many people now have home WiFi networks that may be used by a computer or two, an Xbox, or an iTouch. A lawyer does not want to host an unsecured home network even if no legal business is done via the network. Most lawyers might want to use their home WiFi network to log into the office from time to time.

I will pass along some advice I gave a lawyer a while back. He has an old wireless G router he had set up years ago without security at home and wanted to secure it but didn't know where the documentation was and how to proceed. I told him to stop by the big box store on the way home and buy a nice new fast N Wireless router (\$70 - \$110) and set it up with appropriate security and to give the (long) password

to everyone in the household and tell them their devices couldn't connect to the Internet without the password. After a little setup time, they now had faster, secure wireless Internet and when the parents forget the password, they can just go ask one of the children.

More secure wireless connections are available by purchasing a cellular modem with a plan from a cell phone provider. These will allow a subscriber Internet access anywhere one can get a cell phone signal, at 3G broadband speeds in urban areas and at somewhat slower speed in more remote areas. See "How to Buy a Cellular Modem," *PC Magazine* (March 27, 2009) at tinyurl.com/2325su4 and "Logging onto the Internet from (Almost) Anywhere" by Jim Calloway, *The Oklahoma Bar Journal*, Aug. 9, 2008 — Vol. 79; No.20 and at tinyurl.com/2cjabxk.

“ Even placing a USB Flash drive into a photo kiosk to get pictures printed could be a security risk. ”



What about those computer kiosks you see set up at conferences or using the computers provided in hotel business centers? For their main purposes, they are fine. You should feel free to use them for Internet searches, locating places to go for dinner, getting driving directions and printing off boarding passes for airlines. Many use them for e-mail access. Again, I personally would never enter credit card or banking information into these. In fact, I have stopped using them for checking e-mail. My best guess is that the computers set up for conferences are safer than those that sit unattended in hotel business centers. The danger is that someone will install a keystroke logger device (either hardware or software) to record every

keystroke typed into the machine. Studies have shown that a high percentage of the hotel business centers have such malware installed.

Even placing a USB Flash drive into a photo kiosk to get pictures printed could be a security risk. See "Photo Kiosks Spread Malware via USB Sticks" *SPAMfighter News* — July 19, 2010, at tinyurl.com/27wx3jb.

Security is even more of a concern when the remote user is not just checking e-mail but logging into a virtual office environment.

REMOTE ACCESS TO THE OFFICE NETWORK

Logging into the office to enjoy the full office experience from anywhere virtually is a different matter than just checking your e-mail. You can access all of your files of the network and, depending on the tool used, run applications or operate the remote computer to print and do other things. Larger firm lawyers depend on their IT departments to set up this arrangement for them. Small firm lawyers will login to a remote desktop situation using commercial remote access tools.

One of the secure tools for doing this is a Virtual Private Network or VPN. If your firm has IT support, you probably already have this option.

If you are a small firm lawyer or a lawyer whose firm is not going to set up a VPN anytime soon, consider using commercial remote access products like GoToMyPC (www.gotomypc.com), LogMeIn (www.logmein.com), or Symantec's PCAnywhere (<http://bit.ly/PCAnywhere>). LogMeIn is free for basic operations. There are various levels of potential access.

Logging into a computer remotely means that computer will be left on all of the time. This means a good surge protector/uninterruptible power supply/battery backup is required.

Of course, you can only access what is on the computer or computer network. Remote access to files is a significant reason why more law firms are going to digital client files. If it is on the network, even just as a scanned image, it can be set up to be accessed remotely. Documents sitting in physical file folders cannot, absent assistance from your staff.

I predict the majority of lawyers will have complete remote access and not just "e-mail only" access fairly soon, if that is not already true.

CLOUD COMPUTING

Travis Pickens' article in this *Oklahoma Bar Journal* — "Ethics up in the Clouds," covers the emerging area of cloud-based law office computing applications. The practice of using software provided by (and storing data with) an online third-party provider has become a reality for many lawyers. Many are rightfully concerned about the security and propriety of hosting confidential client data online.

Clearly, if all confidentiality concerns were addressed, this practice has huge implications for the traveling lawyer. If on a day-to-day basis, the lawyer works on remote applications via a web browser, then assuming good Internet access, the "working on the road" experience will differ little from the "in the office" experience.

THE GOOGLIZED OFFICE

As previously noted, many lawyers say that Google apps are not an appropriate method of a lawyer running an office. Meanwhile, other lawyers say that they can run their entire office using Google tools. Certainly the allure of the great Google products is apparent. Gmail, Google Calendar, Google Reader, Google Docs and Spreadsheets and other Google products (both now and those in the future) provide powerful tools, either for free or at a nominal expense.

One can certainly run a law office exclusively on Google, but the question remains, should you? At this point, all that can be said is that lawyers and security experts disagree. Some use Gmail and other apps without concern and others say it is not appropriate to do so.

Google has upgraded its security. See "Google Upgrades Security on Gmail," *New York Times* (Jan.13, 2010) at tinyurl.com/2cyu8mq.

ONLINE DOCUMENT REPOSITORIES

The mention of Google Docs leads to a discussion of online document repositories generally.

An online repository for client files is one thing, but what about your own document repository for documents you might need or want to be able to grab from your smart phone?

Think of populating a document repository with new client information sheets that clients

Tips for Using Public Wi-Fi

By John Brewer

It is preferable to access a wireless device when encryption is enabled. The most common forms of wireless encryption are known as WEP and WPA. WPA is better than the WEP, but WEP is better than no encryption. WEP and WPA require the use of a “key” that must be entered on the mobile wireless device in order to permit a connection to the access point. If encryption is not used, then data that is sent over the wireless connection is “visible.”

Many computer users utilize webmail (e.g., Hotmail, Gmail and Yahoo). It is prudent to use a webmail service on a wireless basis that utilizes the SSL/TLS protocol. The web uses a protocol called HTTP (hypertext transfer protocol). One can see HTTP as the first letters in the URL of a website. HTTPS indicates that the transmissions are encrypted with the SSL/TLS protocol. Users of webmail should look at the URL for their service to see if the URL includes HTTPS as the first letters of the URL. The main idea of HTTPS is to create a secure channel over an unsecure network. A HTTP connection is not secure. Users of these webmail applications should look for a secure login and once logged into the application, that the application maintains a secure connection and does not revert to a HTTP connection.

Windows 7 has additional security options when using a public network. It can block all incoming connections, including those in the list of allowed programs. This setting blocks all unsolicited attempts to connect to one's computer. One should use this setting when maximum protection is prudent, such as when connecting to a public network in a hotel or airport, or when a computer worm is spreading over the Internet. With this setting, the user is not notified when Windows Firewall blocks programs, and programs in the list of allowed programs are ignored. When blocking all incoming connections, one can still view most web pages, send and receive e mail, and send and receive instant messages. There are other settings available in Windows Firewall.

iPhone users should be cautious of AT&T Wi-Fi hot spots. It is reported that iPhones are configured to recognize AT&T Wi-Fi connections by the name “attwifi.” One article stated that iPhone users can protect themselves by disabling the Wi-Fi, or by

complete, informative packets that you send prospective clients, all of your attorney client contracts and a few other basic documents that would be handy if your office network was down and/or physically inaccessible. Some can be set to automatically sync with a folder on the office network, making them an additional backup.

There are many choices. Among the leaders are Dropbox, Drop.io and SugarSync. Dropbox is now widely used by many. It is one of my favorite applications because it is free and easy to use. It just installs a folder under My Documents called My Dropbox. Any documents saved there are available on all other computers I have synchronized with Dropbox as well as on my smart phone. Up to two gigabytes of storage is free and you can add to that by referring others to Dropbox.

VIRTUAL ASSISTANTS

Some lawyers who are on the road more than in the office have opted to dispense of staff and rely on virtual assistants. I know of one Oklahoma City lawyer who decided to try that when the best assistant he ever had moved across the country. He has been pleased with the results. With most virtual assistants, one can pay either by the project or by the hour.

A virtual assistant is one who works outside of your office from their home or office. Typically they are paid by the project, but some are paid hourly. E-mail is used for project assignment and communication. Logically, it might seem that a virtual assistant would be an independent contractor, unless used on a full-time basis, but each law firm needs to make that decision working with their tax advisor.

TETHERING

Tethering refers to connecting a laptop computer to the Internet via your mobile phone. Why should you have to pay for a data plan for both your computer and your laptop when you can tether?

Suffice it to say that the big telecom companies are going to do everything possible to prevent users from tethering, including convincing them that it is just a bad idea. Tethering may be barred by your current service provider's contract or require “jailbreaking” a mobile phone. And many do not feel like 3G service is consistently good in some of the areas that they frequent anyway.

Nevertheless, it seems to be a matter of time before tethering becomes more common and perhaps even a “tethering friendly plan” may be marketed by the big telecoms.

For some step-by-step instructions to tethering with some phone service providers go to tinyurl.com/dh3dbm.

See also, for example, AT&T’s data plans at www.wireless.att.com/businesscenter/.

Those AT&T data plans that allow tethering also have a per KB charge for the bandwidth.

THE TRAVELING LAWYER’S BAG

Some traveling lawyer bags look like a traditional briefcase. But a lawyer who spends much time in airports may soon opt for either a wheeled bag or a backpack. Don’t be penny-wise and pound foolish here. It may make sense to have two (or more) computer bags: a light briefcase style for day-to-day use and the wheeled or backpack version for overnight road trips.

A real road warrior who wants to take a complete office setup on the road will definitely need a separate wheeled bag. This can carry the full “law office to go” with the portable printer, portable scanner, paper and some other office supplies. Generally speaking, a portable scanner and a portable printer, along with a laptop and paper, will give you complete document production and management capabilities. A word of warning: If you are going to make much use of portable printers, you may want to travel with spare ink cartridges as it seems that ink runs out at the very worst time.

For those lawyers who go through airport security frequently, checkpoint friendly bags can save time and reduce aggravation. See *PC World’s* 2008 review of “8 Checkpoint-Friendly Laptop Bags” for the products and an overview of the regulations at tinyurl.com/6xkchf.

What’s in the computer bag besides the laptop?

I never travel without a stash of several USB flash drives. You never can tell when you will need one of them, and I have made more than one friend by having an extra to give away. Even if you do not carry several flash drives, you must carry at least two — one that is encrypted and one that is not encrypted. On the encrypted drive you can have your credit card numbers and 800 numbers for each company, medical insurance and other important personal

turning off the automatic joining of AT&T networks, but only if the device is within range of the existing AT&T hot spot. iPhone users should investigate this issue more fully.

Instant messaging is popular with many people. Most instant messaging services transmit communications as clear (unencrypted) text. One can check with the instant messaging service provider to learn more about the specific instant messaging service and its security features, if any. Such clear text communications are unencrypted whether instant messaging is used on wired or wireless devices and networks. Unencrypted instant messaging is vulnerable to illicit attempts to intercept and read the content of messages sent and received. If one chooses to use instant messaging on a public Wi-Fi connection, it is recommended that one avoid using it to transmit information deemed confidential.

At a minimum, heed the following (especially if using a laptop/net book computer):

- 1) Use a firewall. The operating system should have a firewall included with the OS. Make sure it is turned on. Third-party firewalls are also an option.
- 2) Hide your files. When you use public Wi-Fi, network encryption is often out of your control. Check the privacy statement on the network’s website to learn about the type of encryption in use. If there is no privacy statement, that is a warning sign. Consider encrypting sensitive folders on your hard drive.
- 3) Do not type in credit card numbers or passwords unless there is a secure connection.
- 4) Turn off your wireless network if not needed. If one is not surfing the Internet or sending e-mail, but still using the computer in an area where there is a public wireless network, disable the wireless connection. If using an external Wi-Fi card, it can be removed. If the computer has an internal card, disable the card.

Common sense and caution are both essential when using a public Wi-Fi connection. The consequences of ignoring security issues could be damaging to the health of one’s computer and/or bank account.

information. Think of the encrypted flash drive as the “I lost my wallet” backup, although it is great for carrying confidential client documents, too.

If you don't want to learn do-it-yourself encryption, there are many USB flash drives that come with it preinstalled. A favorite among many is the Ironkey brand at www.ironkey.com. Taking a cue from the *Mission Impossible* series and movies, this can be set to delete your data if it is lost and the finder enters the wrong password a set number of times.

If you need to carry a lot of data safely or just want to have a backup of your data to carry with you, look at portable hard drives which are designed for rough treatment like the Hitachi SimpleTOUGH. Amazon offered these at a price of \$65.93 for 320 GB and \$107.29 for 500 GB at the time I was preparing this paper.

If weight is a big concern, the Seagate FreeAgent Go (<http://bit.ly/FreeAgentGo>) is one of the thinnest and lightest hard drives available - it only weighs 5.6 ounces! It comes in 250GB, 320GB and 500GB models.

A portable wireless mouse – Usually I can deal with the touchpad for most computer work. But sometimes I want the control of a regular mouse. A corded mouse creates more clutter in my bag, so a portable wireless mouse is the perfect solution. Just plug in the small USB antenna and your mouse is ready to go. My current wireless portable mouse is the Logitech VX Nano Cordless Laser Mouse (tinyurl.com/2enc5gt, \$69.99).

“No fly” bag — In the olden days of flight I used to travel with a little kit that included several small screwdrivers, scissors and a pocket knife. Now I try never to toss anything into my computer bag that cannot pass an airport screening. One way is to keep all of the banned carry-on items in one “no fly” bag that could easily be transferred into one’s checked bag when flying. You never know when you are going to be really glad you had a screwdriver (or a corkscrew) with you when traveling.

Another bit of information for the road warrior to carry is the Help Desk numbers for your software applications and the serial numbers just in case you need help.

Chargers and cords — If the traveling lawyer isn't careful, he or she may find the computer bag full of cords and chargers for a variety of devices. Some consolidation may be in order and you might consider a setup that will charge more than one device. Chargers that have tips for a number of different devices are now inexpensive and compact. See The “Octo-

pus Cable Charges 10 Devices (via USB) for Just 10 Dollars” at tinyurl.com/kjhhke.

A similar setup to charge with AC power is found at www.igo.com. These products are reasonably inexpensive and leave you carrying a lighter computer bag through the airport.

Although many laptops have built-in surge protection, a small portable surge protector is a wise investment. For example, here's an inexpensive combination of surge protector, “power strip” and USB charger, a Belkin Mini Surge Protector (www.belkin.com, \$24.99). It offers two convenient USB power ports as well as three AC outlets and has a very good 918 joule rating.

“ A corded mouse creates more clutter in my bag, so a portable wireless mouse is the perfect solution. ”

Along the same line, I know I'm not “supposed” to use them, but I carry one of the little two-to-three prong electrical adaptors in my bag. Most big city hotels have all upgraded to grounded three-prong AC outlets, but every now and then in the hinterlands, you will find a hotel room with only two-pronged outlets. I wouldn't use this for working on my laptop for long stretches.

I will also note that I have just started using my new iPad for travel. It is clear that it is a superior traveling tool, being very light and easy to read.

TRAVEL PLANNING

There are a number of online services and resources related to travel. For more information, check out an article that I co-authored with colleague, Courtney Kennaday, that reviews trip planning and deal sites, “Sites For Sore Eyes — The Travel Site Less Visited.” The article, published in the September 2009 ABA *GP | Solo eTechnology Newsletter* is available online at tinyurl.com/m8l8j9.

If you are not familiar with websites and services like Kayak.com, TripAdvisor.com, Chowhound.com, SeatGuru.com and TripIt.com, you really need to review this article. These services are critical for the traveling lawyer.

CONCLUSION

Hopefully, this article has given you some new tools that you can use when you find yourself thrust into the role of the traveling lawyer. Our tools for the road continue to evolve as smart phones get smarter and online tools become more secure and more powerful. Whether you carry all the tools you need with you or rely on a remote connection to your office network, I hope you find these tips to help you become more productive on the road.

ABOUT THE AUTHORS

John Brewer is a solo practitioner in Oklahoma City. He graduated from the OU College of Law in 1974 and has been active in technology issues pertaining to the OBA and other nonprofit organizations. He has presented numerous presentations regarding technology as it relates to the practice of law for the OBA and other organizations. He has a particular interest in mental health issues and the role that lawyers can play in improving the lives of those challenged with mental health issues.



Jim Calloway is the director of the OBA Management Assistance Program and manages the OBA Solo & Small Firm Conference. He served as the chair of the 2005 ABA TECHSHOW board. His Law Practice Tips blog and Digital Edge podcast cover technology and management issues. He speaks frequently

on law office management, legal technology, ethics and business operations.

OKNEWSBAR

- The latest Oklahoma and U.S. Supreme Court opinions
- Up-to-date legal news
- Law practice management tips

...all in one place.



www.okbar.org/oknewsbar.htm