Managing Your Firm While on the Road[1]

Jennifer Ellis
Jennifer Ellis, JD, LLC
https://jlellis.net

These days, clients expect us to be available to them. On the other hand, we often need to be out of the office, and a reasonable work/life balance would be nice. Fortunately, there are tools you can use to make certain you can access anything or anyone you need.

Remember, under PA Ethics Rule 1.1, you are required to be competent in practice. This obligation includes the use of technology. As such, if you decide to implement any of the technology recommended, please make certain that you have an appropriate understanding of both the risks and rewards. You must be able to properly mitigate those risks.[2] This does not mean you need to be an expert, but it does mean that you should hire someone to help or obtain enough familiarity yourself to be competent.

These are tools that will help you stay connected to your office, your files, your staff, and your clients:

1. A strong Internet connection both in and out of the office.
    a. We are reliant on the Internet. You cannot afford to lose your connection. If you are in a larger firm, it might be worth it to have two providers supporting your connection. For example, if you mainly use Verizon, you can also add a Comcast connection. Then you can add a tool which will automatically switch over to Comcast if your Verizon connection drops. This is especially important if you have VOIP and connect to your phones through the Internet.
    b. In a smaller firm, and for traveling purposes, it is wise to have a Mi-Fi or something that will serve as a hot spot[3]. A MI-Fi[4] is a small device that works as a secure Internet connection. You can buy a pay-as-you go service, or you can have a monthly service.
        i. Depending on your phone and service, you may be able to use your phone as a hot spot. Normally a phone is only good for connecting one device. A Mi-Fi can handle a couple of devices. As a result, if the device needs to serve as a backup to your small law firm, you will want a Mi-Fi instead of a phone hot spot.
2. Secure your Internet connection
    a. If you ever connect to the Internet from restaurants, hotels, and so on, make certain you have a secure connection. The best way to have a secure connection is to use a VPN

---

[1] Jennifer Ellis, Jennifer Ellis, JD, LLC, jennifer@jlellis.net.

[2] Comment 8 to PA Ethics Rule 1.1 states, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

[3] A hot spot is a location where you can connect to the Internet. In this case, we are referring to a mobile hot spot. Sometimes you will hear restaurants that provide WiFi referred to as hotspots as well. https://whatis.techtarget.com/definition/mobile-hotspot

[4] https://www.lifewire.com/what-is-mifi-818311

client. (This is different from the VPN discussed later.) A VPN client encrypts the data you send and receive over the Internet. Even the Internet provider cannot see the details of what you are doing on the web when you use one of these clients.

b. We use Nord for our VPN client, but there are many options available.[5]
c. Remember, your office is only as secure as your weakest connection. If staff connect from home or while traveling and fail to provide a secure connection, this will be a source of attack. Make certain that people who work from home secure their WiFi connections properly.[6]

3. Put your data in the cloud.
    a. There are many reliable services you can use to put your data online. What service is best for you will depend on your needs and the size of your firm. In a larger firm, you might want to create your own cloud. In a smaller firm, you will likely want to use a service that already exists. When you put your data in the cloud, you can easily access it from anywhere with a secure connection.
        i. Regardless of the type of service you choose, you are ethically obligated to make certain that the service is appropriate. The Pennsylvania Bar Institute ethics committee provided an opinion[7] that contains a checklist that will help you determine whether your cloud provider is appropriate for a lawyer's use.
        ii. It is very important to be aware that some cloud providers do not offer the appropriate level of security. These providers keep your data secure while it is on your computer or while it is on the provider's server. But not while the data is travelling between the two. If you choose to use one of these providers, it may be necessary to add additional encryption to protect your clients' data. Dropbox, while a very popular provider, has this problem. Spideroak, on the other hand, is very secure. In addition, Spideroak is Zero Knowledge. This means that no one at Spideroak can access your password.
            1. How much security you need for your files depends on the level of risk to your specific type of data. PA Ethics Rule 1.6 (d) addresses your need to protect client data. Comment 25 provides the factors to consider when determining the level of protection required. Comment 26 provides further guidance as relates to obligations to protect data while it is being transmitted. Comment 25 provides a safe harbor for lawyers who take "reasonable" steps to protect client data.
                a. Sensitivity of the information.
                b. Likelihood of disclosure if additional safeguards are not employed.
                c. Cost of employing additional safeguards.
                d. Difficulty of implementing the safeguards.

---

[5] https://nordvpn.com/

[6] https://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2016/01/15/don-t-let-technology-get-you-in-trouble.aspx

[7] Ethical obligations for attorneys using cloud computing software as a service while fulfilling the duties of confidentiality and preservation of client property, formal opinion 2011-200.

e. Extent to which the safeguards adversely affect the lawyer's ability to represent clients.
f. Consider relevant laws (such as HIPAA) or client requests.

iii. Make certain that the provider puts a copy of all files locally on your computer. This way, even if you lose your Internet connection, you can still access your files. These copies should sync across all computers with a proper service.

4. Back up your data
    a. You should have at least two backups of all data. These backups should take the form of two different cloud providers, or one cloud provider and one local technology.
        i. If you use a local technology, be sure to encrypt it.
        ii. The benefit of a local backup, such as on a server or an external drive, is that the restoration can often be done faster. However, external drives are easily stolen, or destroyed in case of fire or water. This is why a cloud backup is also necessary.
    b. Consider having a mirror image[8] of your hard drive(s). A mirror is a complete copy, including the installation of software. If a computer or its hard drive fails, a mirror allows for quick set up of a new machine.
5. Get a VPN.
    a. VPN[9] stands for Virtual Private Network. VPNs allow you to connect to a computer in your office anywhere you have an Internet connection. A VPN allows you to control a computer in your office as if you are sitting there.
        i. VPNs provide encryption to make certain the data you are sending back and forth over the Internet is secure.
            1. Many operating systems have the ability to set up a VPN included within them. However, there is also both hardware and software you can use to set up a VPN.
        ii. Some choose to use services such as GoToMyPC or LogMeIn. On the whole, a VPN will cost substantially less money and is also more secure. The reason a VPN is more secure is because both GoToMyPC and LogMeIn are frequently targets of hackers who try to steal login and password information.
        iii. Make certain to secure any device which provides access to your office.
6. Use VOIP for your office phone service.
    a. VOIP stands for voice over internet protocol. Not only does a VOIP service allow you to connect your phone through the Internet, but many services allow you to easily take your phone with you and connect it to any computer that has an ethernet connection.
        i. Many of the providers allow you to forward your specific phone number, or the entire phone system, to another phone. This means that if your phones stop working due to a disaster or Internet outage, you can still get all calls.
        ii. With the proper app on your cell phone, anyone you call will see your office phone number and not your cell phone number. This ends the need to provide your cell phone number to clients.

[8] https://www.pcworld.com/article/2847308/when-to-image-a-drive-and-when-to-clone-it.html
[9] https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html

iii. Be certain that the phone provider offers the appropriate level of security for your firm. Ask the questions listed in the PBA Cloud opinion.

7. Use a cloud-based practice management system.
    a. There are myriad practice management systems that are solely or partially in the cloud. These systems allow you to access your documents and data anywhere. They can limit the need for you to connect to your computer or office when you are out and about and provide you the ability to easily access your data anywhere.
        i. Small firms should consider Rocket Matter or Clio. There are other options as well.
            1. Both of these services provide both practice management and document management.
        ii. Larger firms can consider these services as well but might find them cost prohibitive on a per seat basis. Such firms should consider whether creating their own cloud is the best option for them. Larger firms generally have in house IT and their IT can help them create an appropriate system.
        iii. Again, security is critical. Ask the right questions as discussed in the PBA Cloud Opinion.
8. Consider Office 365 or Google Business.
    a. Office 365 and Google Business both replace the need for an email server. While many small firms choose to use IMAP email, there are limits to that technology. IMAP does sync email across devices, but it does not sync contacts and calendar entries. Both large and small firms can use Office 365 or Google Business. The cost is not prohibitive.
        i. Do not use free services such as Gmail. They do not provide branding for your firm through the address, and there may be ethics issues relating to who can access the data. It is important to have your own domain name for branding purposes.
9. Make sure you have a high quality smart phone.
    a. Your smart phone is likely to be your headquarters while on the road. Make sure you get a quality phone and keep it up-to-date. It is critical to install all updates to keep the phone secure and working properly.
        i. Put a password on your phone to keep it secure.
        ii. Do not let anyone else access your phone.
        iii. Be careful what apps you put on the phone. Apple screens apps very carefully, Google less so. Check and see what the apps share with third parties before you install them.
        iv. Install apps that will locate the phone if it is stolen or lost. Both Android and Apple[10] provide free apps for this purpose.
            1. These apps allow you to wipe the phone if it is lost.
        v. During the time when you are still paying for the phone, consider purchasing insurance. This way if your phone is seriously damaged, you can replace your phone relatively easily and inexpensively. Remember to cancel the insurance when it is no longer necessary.

[10] https://www.apple.com/icloud/find-my-iphone/

vi. Most new smart phones have encryption, but you must turn it on. Google "phone type turn on encryption". Follow the instructions.
vii. Back up the data properly. Make sure the data backup is secure.
viii. Turn on blue tooth in your car. This will help you avoid holding your phone while driving.
1. If your car does not have blue tooth, you can purchase a device that will provide this connectivity. These devices are inexpensive.

10. Consider purchasing a tablet.
    a. The negative about smart phones is that they are very small, and it can be difficult to do productive work on them. Many tablets now have access to applications which allow you to conduct work on them. Don't overlook the Windows tablet.
        i. Office 365 works well with tablets and is usable on both Apple and Android products.
        ii. Purchase a keyboard to go with the tablet. There are many options.
        iii. Secure the tablet with a password.
        iv. Add the apps that help you find your tablet if it is lost or stolen.
            1. Same as for phones.
        v. Turn on encryption if available.
        vi. Securely backup the data.
11. Purchase a laptop.
    a. In some cases, a tablet with a keyboard will be enough. In other cases, it will not, and you will want a laptop. It is not generally necessary to purchase an expensive laptop. Laptops under $1000 are more than enough for most lawyers.
        i. Make certain to secure the laptop with a proper password.
        ii. Encrypt the hard drive.
        iii. Add software[11] to help you find the laptop if it is lost and that will allow you to wipe it if it cannot be found.
12. Organizational Tip: Consider Google Home or Amazon Alexa to help you stay organized.
    a. Both Google Home and Alexa can be connected to your calendar. You can easily set alarms or ask your device what is on your schedule for the day.
        i. If you are concerned about ease dropping, turn off the microphone when you are not using the device.
13. A word about texting with clients.
    a. If you text with your clients, you must preserve the texts. There are myriad applications which allow you to download texts and place them into your client's file.
14. Security Tip #1: Do not use public computers.
    a. Public computers such as those in coffee shops or hotels are not secure. They almost always have malware on them. This malware will steal all usernames and passwords you type into the computer.
15. Security Tip #2: Use malware protection on all devices.
    a. There are many options for malware protection. You can purchase one suite and use it on your computer(s), phone(s), and tablet(s).

[1111] https://www.windowspasswordsrecovery.com/win10-tips/top-3-ways-to-remotely-wipe-windows-10-laptop.html

        i. Some IT professionals will discourage use of malware protection on servers. This is an outdated view. Your servers need protection.
        ii. Even apple devices need malware protection these days.
        iii. Be certain to keep the malware software up-to-date. Automatic updates are your best choice.
16. Security Tip #3: Keep your computer's operating system up-to-date.
    a. Either use automatic updates or keep a schedule.
17. Security Tip #4: Have an alarm system at home.
    a. If you keep files at home, you must keep them secure.
    b. Wireless alarm system that call you instead of an alarm company are available and inexpensive. They can be easily installed and do not require you to run any wires.
        i. Use removable two-way Velcro stickers and you do not need to put holes in your walls or doors.
18. Security Tip #5: Encrypt USB drives and external hard drives.
    a. Anything that can easily "walk away" should be encrypted. Many USB drives and external hard drives can be purchased already encrypted. There is also software available for easy encryption of these devices.