Mobile Security 101 for Attorneys

Evan Benet February 25, 2021

In 2021, whether you realize it or not, you're a "mobile" lawyer. The digitalization of the world we live in has made the proliferation of cellphones and on-the-go devices an undeniable part of our everyday routine.

Did you know that as of 4 years ago, nearly 100% of lawyers were using mobile computing tools for at least some aspect of their practice? So now, it isn't "nearly," it is a resounding "everybody." Everyone has a cell phone and everyone uses it both for personal and professional reasons. We are all working in a mobile world these days and the expectation is that we will have access to our information from wherever we are.

The first time many of us remember seeing a mobile device was in the 1987 action flick, *Lethal Weapon*. It was this massive square hunk of material connected to this even clunkier receiver that Roger Murtaugh lugged around across LA. Since then, we have seen this evolution from our Nokia candy-bar phones to flip phones and Blackberrys. But now many decades later, 80% of attorneys are using these beautiful slabs of indestructible (so they say) glass called iPhones. We think of these devices as mobile phones that happen to do a few other things on top of making calls and sending texts. But, think about all the things your phone has replaced… we're talking about email, calendaring, camera, books, TV, games, tickets, GPS the list goes on and on.

What you should be taking away from this is the fact that these devices are no longer small, single-serving phones. They are an entire personal computer. Our phones have become the primary PC that most of us use on a constant basis. Of course, we have desktops and laptops, but these sleeker and portable devices are one of the first places we go to when we wake up and the last thing we put down at night. There is no other piece of technology that we own that is so pervasive in our lives.

You may be asking yourself, so what? Isn't technology supposed to grow and evolve and improve? And obviously, the answer to that is yes, but what hasn't evolved with the changes in our technology is how we protect the information we interact with. Right now, our mobile devices are still thought of as "phones." And how we protect and monitor them reflects that. However, we go to much greater lengths to protect our servers and our computers. But think about what we just talked about. Our phones are our computers too, and they must be protected as

diligently.

Duty of Competence

A few years ago the ABA President started a Commission where they were tasked with looking at whether or not they should make any changes to the Model Rules of Professional Conduct to address the idea that technology today affects nearly every aspect of our legal work. This includes how we store information, how we communicate with clients, how we conduct discovery, and so on.

The ABA went on further to say that: “In the past, lawyers communicated with clients by telephone, in person, by facsimile, but today, lawyers communicate with clients electronically. Confidential information is stored on mobile devices, including the cloud.” Ultimately, this Commission determined that there needed to be some changes to the Model Rules of Professional Conduct. These changes emphasized that it is part of a lawyer’s general and ethical duty to remain competent in a digital age.

To be more specific, this change was most reflected in Rule 1.1- The General Duty of Competence. There was no major change to this actual rule, but an addition was made to comment 8. The section opener remained the same: “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..*” This means the technology you use to run your practice. Every firm uses technology in its practice. Whether it’s simply Microsoft Word or a billing software, everyone uses something. We hear some firms say that they only care about the states that are relevant to their operations. Currently, 38 states have adopted this revised Duty of Competence.

Application to Your Daily Practice

So what does this mean when it applies to your daily practice, from a practical level? We typically think of technology competence as protecting our client’s information, but if we dig deeper, we will find that it incorporates these 5 things:

1. Safeguarding client information and remaining up to date on the various risks and benefits associated with relevant technologies
2. eDiscovery, including the preservation, review, and production of ESI (This includes social media discovery, which opens a Pandora’s box of ethical issues)
3. The technology that lawyers use to run their practices (This can include communication and file

share technologies, software for document generation, electronic calendaring, and docketing tools. Many of these applications store information in the cloud so this realm includes competence with cloud-based operations)
4. Understanding the technology used by your clients to design or manufacture products or to offer particular services
5. The technology used to present information in the courtroom

Let's dig a little deeper into points 1 and 3…

What does that mean exactly when we say the benefits and risks associated with relevant technologies?

The Benefits

The benefits of mobile devices are incredible. That is an undisputed statement. We can now get our work done anywhere at any time, and now with the necessity to work remotely, this capability has become even more critical. Speed is also another advantage, we can communicate so much faster with both our internal teams and our clients without missing a beat. And if you're on a cloud-based practice management system, you can truly access any file, any document, anything about all your matters from wherever you are all from your phone.

The Risks

The first and most obvious risk with mobile devices is the chance of either misplacing, losing, damaging, or getting it stolen. The question isn't if this will happen, it is when it will happen.

It was reported that women are 42% more likely to have their phone stolen while men are 57% more likely to drop their phone in the toilet. And a recent study released from Kensington revealed the costs associated with the loss or theft is far greater than the cost of the device itself, thanks to lost productivity, the loss of intellectual property, data breaches, and legal fees.

Regardless of whether your phone is stolen or lost, there are a lot of associated risks that come with that. But no application on our phones runs as much risk as our email does. Today, we use email to communicate with our clients and colleagues. Today we use email as the primary means to transport files and documents. If someone was able to access your phone, they may not be a hacker, but they know what the mail app looks like. If they are able to open this app, they will

have complete and unfettered access to the most confidential and sensitive information that has been entrusted to you. And it isn't just the messages or communications, it's the attachments! Even with eDiscovery, a vast number of loose files (word documents, pdf, photos), are attached and sent via email.

Ultimately, this is the inherent risk involved.

So what can we do? Let's find out…

Best Practices to Protect Your Mobile Information

No one expects you to be a mobile security expert. Things happen and the best you can do is be prepared and stay informed of the things you can do. So, with this in mind, when you're using a mobile device, be aware of these things:

1. Wifi- Open public wifi networks, as convenient and accessible as they are, pose risks. For one, your data can be accessed by third parties, hackers, or the stranger sitting next to you. It's also important to note that this person or entity doesn't have to be physically sitting near you, they could be anywhere in the vicinity to ascertain your data as it flows across the router and across the network.
2. GPS- The GPS feature in our phones today is unprecedented. However, there is another setting in your phone called "significant locations," where you can access a list of all the major cities and places you have been to over the course of a few weeks. This feature is automatically enabled, so it is important you are aware of it so you can disable it if you so choose. If someone gained access to inside your phone, they would be able to quickly find out where you go and for how long.
3. Phone Updates- It is important to be aware of these updates because oftentimes they contain bug fixes and patches to problems in the older iterations of the software. Keep this in mind with your apps as well, if you let things get too far behind on updates, you risk data breaches and security threats.
4. Passwords- The most dangerous thing that people do with their smartphones is that they do not put a password on them. Fortunately, most software now requires you to put a password on your device. If you have a password on your phone, make sure it is a good one. In 2019 alone, "123456" was the most commonly used password, accounting for 23.2 million accounts. Your password is the gatekeeper to everything confidential in your life so don't take this security step lightly. Tools like 1Password will help you manage and automatically generate lengthy passwords that are then stored in a vault that is protected by a PBKDF2-guarded master password that you create. Don't sacrifice security for convenience.
5. Erase Data- This feature on your phone sounds scary, but hear us out. When you enable this feature, the first thing it does is turn on "data protection." This is a powerful security mechanism and when it is enabled, it ensures that any files created by an app are automatically

encrypted on your phone's file system. This means that if someone were to come into the possession of your phone and you have a passcode on it, they would not be able to access any data stored on your device, even if they plug it into a computer.

6. Cloud Backups- Cloud backup enables your organization to send a copy of your cloud data to another location so that if your data is compromised, you can restore the information, ensure business continuity, and defend against devastating IT crises.

The Takeaway

All of these best practices serve to help you protect the information stored on your personal computer (your cellphone). It is important to note that "reasonable efforts" and "reasonable precautions" means reasonableness. Not perfection. You have an obligation to do what you can, stay informed, and mitigate risks. You do not have to be a technology or smartphone expert to practice the above-mentioned best tips.