Three Steps to Start a Mobile Device Policy for Lawyers

Mobile devices have been around awhile. Their capabilities have grown so steadily, however, that many lawyers can't remember the exact moments when desktop computer slipped off our desks and into our pockets - into our smartphones, tablets and laptops. That might explain why so many lawyers have a mobile device but not a mobile device policy.[1. ©2016 Brandon L. Blankenship, Image Credit: Pac-Man Sander Muller CC flickr 4MAY2015.]

This phenomenon may be the reason that a portion of your work load may have been outsourced right under your nose. Outsourcing usually conjures thoughts of contracting services with foreign vendors. But it can mean obtaining services from an outside, especially in place of an internal source. So, when an employee carries work of the firm outside of the firm on a mobile device and works on it, haven't you effectively outsourced legal services?

A deliberate, well thought out decision to outsource would mostly result in a written contract that ensured knowledge and competence of ethical rules. The contract may contain, for example, confidentiality provisions and establishing a secure way to share files. But, there is no corresponding internal policy for the use of mobile devices outside the firm.

Then someone in your firm accesses a file on their smartphone using StarBucks™ WIFI.

And works on the file.

The firm just obtained services from a source outside the firm.

And unless the firm has established policies about services being performed outside the firm, the risks are incalculable. Here are three things to consider when establishing written mobile device policies.

One: No Public WIFI

When a firm employee jumps on free WIFI, their communication becomes part of the WIFI provider's data stream. It is governed by the WIFI provider's policies. It is subject to subpoena or voluntary disclosure. There may or may not be privacy protections to protect the release of account numbers, passwords, personal information, and so on.

Even though public WIFI is evermore available, there is no way to include the providers of the WIFI (like Starbucks™) in a contract that ensures security.

More so, many public WIFI providers are so insecure that they do not restrict other people on the same public WIFI from seeing each other's communications. The kid on the other side of the room may look like he is playing a video game when he is actually reading your emails as you send and

receive them.

The easy solution is have a written policy that prohibits the use of public WIFI for devices (smartphones, tablets, laptops, etc.) that contain firm files.

Two: No BYOD

Many organizations cut costs by simply requiring employees to BYOD - Bring Your Own Device. The employee's personal device then fills up with a mixed bag of personal data and firm data.

This practice is problematic:

- When an employee raises a privacy objection in response to a discovery request or subpoena;
- Where a firm employee is suspected of inappropriate actions and the firm cannot legally access the cell phone;
- Where the firm requires that firm files are backed up using an encrypted backup method. This concern is growing. The iPhone 7, for example, will be released with 32 GB of storage. This is enough storage to hold the files of a solo practice. It is difficult to backup only firm files without also backing up personal files. There is also the concern that the user manages the password and may refuse or be unable to provide it when it is most needed;
- When the device is lost or stolen. Firm devices that contain client information should be configured to self-delete in the event they are lost or stolen.[2. See, I Felt Pretty Secure About Our Computer Server, I Shouldn't Have.] Firm employees that BYOD may see the deletion of their personal files as a privacy invasion.

A mobile device policy should draw a hard line between the firm's device and personal devices. Firm devices should require a pass code to access and take the considerations above into account.

Three: Teach Your Mobile Device Policy

Do it yourself, ask a firm employee to do it or ask a technology vendor to do it for you. Having a mobile device policy is meaningless if someone doesn't understand it. It is worth a working lunch or an hour off-site to educate firm employees. Data security is only as strong as the one person that gets sloppy. Once your data is compromised, it is all compromised.

And here is a tip that makes reading this article worth it (if nothing else does.) Video your training. Then, each new hire can watch the video. By doing this you emphasis to the new hire the importance you place on the mobile device policy and that is one way to create a culture of compliance.

Brandon L. Blankenship

- About
- Latest Posts

Brandon Blankenship

Presenter at Enemy In The Camp

Brandon L. Blankenship is a continuing legal education presenter and business educator. He is the author of Unmasking Hour. He writes weekly posts on the legal industry and is a contributor to the Nobility Academy. He and his wife Donnalee live on their hobby farm south of Birmingham, Alabama.

Latest posts by Brandon Blankenship (see all)

- Protect Your Law Firm From a Social Engineering Fraudster - October 24, 2016
- It's Not the Pokémon In Your Law Practice – It's What You Are Missing Because of It - August 11, 2016
- Protect Attorney Email From Going Viral - August 1, 2016