SECURE MOBILE COMPUTING

Sponsor:  Small Firm Practice & Management Section
CLE Credit:   1.0
Wednesday, June 18, 2014
3:35 p.m. - 4:35 p.m.
Ballroom A
Northern Kentucky Convention Center
Covington, Kentucky
A NOTE CONCERNING THE PROGRAM MATERIALS

The materials included in this Kentucky Bar Association Continuing Legal Education handbook are intended to provide current and accurate information about the subject matter covered. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgment of the individual legal practitioner. The faculty and staff of this Kentucky Bar Association CLE program disclaim liability therefore. Attorneys using these materials, or information otherwise conveyed during the program, in dealing with a specific legal matter have a duty to research original and current sources of authority.

Printed by: Evolution Creative Solutions
7107 Shona Drive
Cincinnati, Ohio 45237
Kentucky Bar Association
# TABLE OF CONTENTS

The Presenters........................................................................................................................................... i

Secure Mobile Computing .......................................................................................................................... 1

  Introduction........................................................................................................................................... 1

  Ethics of Mobile Computing ............................................................................................................... 1

  Determining the Level of Mobility / Choosing a Device ................................................................. 5

  Device, Personal and Network Security ............................................................................................. 7

  Vetting Third Parties ......................................................................................................................... 9

  How Much Does Your Client Know? ................................................................................................. 10

  Training .............................................................................................................................................. 10

  Summary ........................................................................................................................................... 11

Bonus Material....................................................................................................................................... 11
THE PRESENTERS

Mark S. Medlin
113 East First Street
Post Office Box 457
La Center, Kentucky 42056
(270) 665-9529
medlinlaw@gmail.com

MARK S. MEDLIN maintains a private practice in La Center, Kentucky. He received his B.A. from the University of Kentucky and his J.D. from the University of Kentucky College of Law. Mr. Medlin is a Fellow of the Kentucky Bar Foundation and a member of the Kentucky Bar Association’s Business Law, Probate & Trust Law, and Small Firm Practice & Management Sections.

Jeffery L. Sallee
Jeffery L. Sallee, Attorney at Law
102 Lake Park Dr.
Alexandria, Kentucky 41001
(859) 445-2920
Jeff.sallee@twc.com

JEFFERY L. SALLEE is a solo practitioner of general law in Alexandria, Kentucky. Mr. Sallee is a graduate of Purdue University where he received a B.A. in German and a B.S. in Computer Technology. He went on to receive his J.D. from Northern Kentucky University’s Chase College of Law. Mr. Sallee is a member of the Kentucky Bar Association, and is also licensed to practice law in Indiana. He has been employed by Proctor & Gamble in the IT department since 1993. Mr. Sallee is a Kentucky Colonel and serves as the Chair of the Kentucky Bar Association’s Small Firm Practice and Management Section.
I. INTRODUCTION

The theme of this CLE is Secure Mobile Computing. As someone who is very deep in the weeds on the topic, the first thing you need to know is that security and mobile computing exist on a continuum and the level of security you need to embrace should reflect the amount of risk you expect. When even our most secret of secret agencies finds its secrets on Wikileaks, it should be obvious that there is no such thing as a complete and unbreakable security. One of the best cartons I have seen that brings this point home is here: http://xkcd.com/538/.

This session will provide you with the basic information you need to thwart the average attack. Hacking is now a full-time business. And as with most businesses, the hacker wants to make the most profit with the least effort and the lowest risk. If your practice area brings you into a situation where your opponent happens to be a nation state or a criminal organization which is willing to spend the time and effort needed to break into your systems, the tips in this session will only slow them down. If you need to protect your files from the future ex-spouse in a divorce case or the family of someone you prosecuted, then this will likely protect you.

II. ETHICS OF MOBILE COMPUTING

It should be no surprise that the ABA has been pushing attorneys to increase their technical capabilities. The Model Rules were updated to clarify that attorneys need to protect their clients' privacy in all locations, not just the attorney's office.
A. Comment 81 to Model Rule 1.1 tells us to "keep abreast of changes in the
law and its practice, including the benefits and risks associated with
relevant technology."

B. Comment 42 to Model Rule 1.4 tells us that "A lawyer should promptly
respond to or acknowledge client communications." In today's world, this
means email and text messages as well as phone calls.

C. Comment 183 to Model Rule 1.6 provides us with the factors we need to
consider regarding what are reasonable efforts at preserving
confidentiality:

1. The sensitivity of the information;
2. The likelihood of disclosure if additional safeguards are not
   employed;
3. The cost of employing additional safeguards, the difficulty of
   implementing the safeguards; and
4. The extent to which the safeguards adversely affect the lawyer's
   ability to represent clients (e.g., by making a device or important
   piece of software excessively difficult to use).

D. Comment 34 to Model Rule 5.3 is crucial to you as a mobile lawyer. "A
lawyer must make reasonable efforts to ensure that the services are
provided in a manner that is compatible with the lawyer's professional
obligations. ... the nature of the services involved; the terms of any
arrangements concerning the protection of client information; and the
legal and ethical environments of the jurisdictions in which the services
will be performed, particularly with regard to confidentiality."

Just as case law helps us define the limits and required elements in court, the
ethics opinions help us define the scope of the ABA's Model Rules. The links
below show that where state bar associations have published opinions on cloud
computing and mobile computing, they have found them to be ethical for

1http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html (last visited April 28, 2014).

2http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_4_communications/comment_on_rule_1_4.html (last visited April 28, 2014).


4http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_5_3_responsibilities_regarding_nonlawyer_assistant/comment_on_rule_5_3.html (last visited April 28, 2014).
attorneys to use, as long as reasonable measures are taken to protect client confidentiality.

A. Alabama State Bar Association – Ethics Opinion 2010-02

B. State Bar Association of Arizona – Ethics Opinion 09-04


D. Connecticut Bar Association – Ethics Opinion 2013-07

E. Florida Bar Association – Ethics Op. 12-3

F. Iowa State Bar Association – Ethics Op. 11-01

G. Maine State Bar Association – Ethics Op. 194

H. Massachusetts Bar Association – Ethics Op. 12-03

I. State Bar of Nevada – Ethics Op. 33


Kentucky does not have a direct ethics opinion on point. The closest is Kentucky Bar Association – Ethics Op. 403. Question 1 tells us the email does not need to be encrypted unless there are unusual circumstances. Only the largest law firms have the resources to manage their own email infrastructure.

We need to consider the Supreme Court’s Rules of Professional Conduct, specifically SCR 3.130(1.6) Confidentiality of information. Part (a) states "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b)." Comment 4 is closest to addressing the issues with mobile computing and cloud computing.

---


"(4) Paragraph (a) prohibits a lawyer from revealing information relating to the representation of a client. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal protected information but could reasonably lead to the discovery of such information by a third person. …"

Yesterday's security was reasonable if you had a locked filing cabinet in a locked office. If we stayed with that analogy, you would now have unknown building staff entering your office at all hours to clean, rearrange your office, and even replace your filing cabinets. How much do you know about these people?

III. DETERMINING THE LEVEL OF MOBILITY/CHOOSING A DEVICE

The first step is to determine what kind of hardware and software you want to use. As an IT professional as well as an attorney, I am asked this question frequently. It is one of those rare situations where the answer is the same for both professions: It depends. The best way to answer this question is to decide what you need to meet your goals. This includes:

- How much do you plan to work outside your office?
- How important is security for your law practice?
- What kind of budget do you have for this?
- Do you need cell phone coverage or will WiFi do?
- Which network should you use?

Mobile computing for attorneys is basically the idea that an attorney should be able to work anywhere using any computing device. This includes everything from a laptop, to a tablet, to a smart phone, to the latest wearable devices like Google Gear and the Sony smartwatch.

<table>
<thead>
<tr>
<th>Benefits of Mobile Computing</th>
<th>Disadvantages of Mobile Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>• You can get to your &quot;office&quot; from anywhere.</td>
<td>• If the &quot;Internet is down&quot;, so are you.</td>
</tr>
<tr>
<td>• You do not have to manage your IT infrastructure, just your own devices.</td>
<td>• You do not have the same degree of control over your IT infrastructure.</td>
</tr>
<tr>
<td>• You can automate routine work processes.</td>
<td>• Your data is easier to hack.</td>
</tr>
<tr>
<td>• Enhanced speed of communication.</td>
<td>• Speed of communication can result in miscommunication.</td>
</tr>
<tr>
<td>• Capital costs are moved to expenses.</td>
<td>• The vendors you want to use may not have the security you need.</td>
</tr>
<tr>
<td>• Most apps have free updates</td>
<td></td>
</tr>
<tr>
<td>• Most apps work on any platform.</td>
<td>• Mobile apps tend to have fewer features than traditional programs.</td>
</tr>
<tr>
<td>• Most apps are inexpensive.</td>
<td>• Mobile apps do not share well with other applications.</td>
</tr>
</tbody>
</table>

Tablets and smartphones are great ways to consume information, but if you really need to create content, then you should consider a laptop. Wearable devices really have more "wow" factor than practical use at this point. Cisco
estimates that by 2017, every Internet user will have five internet connected devices.23

This means that you may need to understand more than one operating system (OS) (e.g., Windows, Apple’s iOS, Android, and even Linux.) Even if you try to stay with one primary OS, like Windows, you will need to upgrade at times or risk a lack of support and security. In addition to the idea of planned obsolescence, companies add new features to the OS or have to reconfigure them to take advantage of improved hardware capabilities. When an OS is dropped from support, one of the key issues is the loss of security patches. When new security holes are found, they are not patched by the vendor. As of July 2013, >37 percent of all desktops were still running Windows XP²⁴, a system released in 2001.

You may have heard that you need to use a Mac, since Apples do not get viruses. Windows is the primary OS targeted on laptops and desktops, but it is mainly a question of market share and the size of the prize. Hackers focus on the Windows OS because this is the primary system used by businesses.

Macs were traditionally used by artists, media businesses and schools. They have grown in popularity as a personal computing device, but have only recently begun to work back into corporate settings. As they have, the number of viruses focused on Mac are growing. Details from this list of ten Mac viruses are available on-line at: http://blog.kaspersky.com/mac-viruses-are-here-to-stay10-examples-of-mac-viruses/ (last visited April 28, 2014). It shows that Mac viruses have been there since near the beginning.

- Elk Cloner, 1982
- nVIR, 1987
- MDEF, 1990
- Concept/Laroux, 1995-1996
- SevenDust 666/AutoStart 1998 and 2005
- Renepo/Leap-A, 2004 and 2006
- RSPlug-A, 2007
- iWorkS-A Trojan, 2009
- MacDefender, 2011
- Flashback/SabPub, 2012


When it comes to mobile devices, the top target is the Android OS. In addition to market share, the fact that the Android phones and tablets are usually distributed with older versions of the OS and rarely updated by users means that security patches are not applied and common vulnerabilities remain available for hackers to exploit. See the following site for more information on the Android situation: http://theunderstatement.com/post/11982112928/android-orphans-visualizing-a-sad-history-of-support (last visited April 28, 2014). The information is from 2011, but the issues have only become worse.

When it comes to laptops and smartphones, Apple products generally have a higher price tag. They also have a greater degree of security because of the update process, their market position and because the process to get an application on the Apple App Store forces a more rigid security review process. Android devices are less expensive, but have a far worse security footprint because of the patching issues and the fact that Google Play does less security vetting. If you really want to test drive an app before paying for it, Google has a better selection of trial-ware.

Before you commit to buying a mobile device, you need to consider if you can live with WiFi-only or if you need to have Internet connectivity as well. Laptops can use an adapter that can connect to the cellphone network. Generally a tablet has to have the capability built in. On the other hand, smartphones will generally be able to connect to WiFi as well as their cell provider.

When considering a cell provider, you need to investigate the coverage maps for the areas where you will use your system most frequently. That will also help you decide the plan options to consider. For instance, the Sprint network provides no service where I live, but AT&T has great service. T-Mobile's coverage only provides me with 2G speed to the Internet, so I would need to purchase lots of high-speed access.

Once you have decided on the device and OS you will be running, the first step I suggest is to get training. Unless you have an alter ego as an IT professional, you should seek out some training when you start. Even a Mac has some features that are not apparent without some training. The time you save by using your tools effectively will more than pay for the cost of the training.

IV. DEVICE, PERSONAL, AND NETWORK SECURITY

A. All Mobile Devices, Including Laptops, Should Be Set Up with the Following Features:

1. Activate a power-on/start up password.
2. Use full device encryption.
3. Set up an inactivity device lock.
4. Install a location app to find your device.
5. Set up the device to wipe after a number (ten) of unsuccessful logon attempts.

6. Turn off features that you do not need.

7. Do not "jail break" your device.

B. Avoid Dangerous Behaviors

1. Situational awareness is needed.
   a. Beware of shoulder surfing.
   b. Know that other people may be listening to your conversations.

2. Do not use unencrypted public networks.

3. Do not share your WiFi signal.


5. Do not broadcast your presence.

6. Turn off any unneeded antennas (e.g., WiFi & Bluetooth). They can cause you problems.

7. Use strong passwords.

8. Change your passwords regularly (quarterly is good, but very strong passwords are probably good for a year).

9. Be very careful when sending email. Be certain that you are sending it to the right people.

C. Setting Up Secure Networks

1. Encrypt your firm’s wireless router and your home one as well.

2. Change all default passwords.

3. Set up a "firewall" to protect your network.

4. Do not broadcast your SSID (Service Set IDentifier) or Network Name, or choose a mundane name (i.e., not “LawOffice”).
V. VETTING THIRD PARTIES

A. When You Consider Purchasing Applications, Think about What You Are Doing with Them

1. What privileges are you granting the application? Can you limit what you grant?

2. Does your application send the information in the clear, or is it encrypted?

3. Is your information encrypted on the server?

4. How reputable is the vendor?

5. Have you read the terms & conditions for the application?

6. How often have the applications been updated? (Too often or too seldom may indicate poor development processes.)

7. Does the application store the data in a proprietary format?

8. Can you work on the application without cell phone or WiFi access?

B. Are You Providing the Right Level of Due Diligence When Saving Client Data in the Cloud?

1. Have you vetted the vendors?
   a. Are they audited by a third party (e.g., SSAE 16, Type 2)?
   b. Do they have their own systems, or are they virtual companies?
   c. Are they willing to vouch for their contractors?
   d. Do they promise more than their providers?
   e. If they are hacked, what are your options?
   f. Do they have a tested and verified backup plan?
   g. Do they state that they have an ownership interest in information stored on their site?
   h. Do they have a Service Level Agreement that includes:
      i. Confidentiality promises;
      ii. Availability promises;
iii. Speed/throughput promises; and

iv. A penalty / credit for failure to meet the promises.

2. Do you have an exit strategy with the vendor?
   a. Business arrangements do not last forever. Can you get your data back?
   b. If that vendor goes out of business, what happens to your data?
   c. Are you keeping your own backup outside the vendor's process?
   d. What happens if your vendor's hardware is seized?
   e. Have you tested your plan?

VI. HOW MUCH DOES YOUR CLIENT KNOW?

I suggest letting your client know that you are using mobile computing as part of your practice. Let them know that you are following reasonable business practices to maintain the confidentiality of their information, and that you do question the firms that provide your mobile services to ensure that they comply with your standards. Tell them that this enables you to be more productive and a better advocate for them.

Let them know that no security is perfect, and that even with your security practices and the assurances you have from your vendors, it is always possible that a vendor could be hacked. Assure them that if their information is breached, that you will let them know. Ensure that if they want you to email information to them, that they are aware that anyone who can read their email could access the information you send.

Put this language in your engagement letters and be sure to have them sign it.

VII. TRAINING

Keep informed about technology trends.

For those of you who have studied the 7 Habits by Covey, you know that you need to sharpen your saw; however, you do not need to become a computer guru or devote hours a day to keep up on all the trends. I suggest the following:

A. Read a Technical Law Blog Every Week

B. Keep Aware of the Trends in Computer Crimes

C. Review Your IT Strategy at Least Once a Year
VIII. SUMMARY

Mobile computing is here to stay. As technology changes, we must adapt. Changes in expectations from the ABA are forcing us to change. We cannot sit back and rely on the old business models and the old work processes, even if we wanted to. Even if you do not want to embrace this change, you need to know enough about technology changes that you can counsel your clients on these topics. This also is information you need to know for your own family.

IX. BONUS INFORMATION

A. Are you aware there are contact management systems that can actually track the number of times you read your email and some will even track the devices you used to open the email? This is generally done with imbedded images (often one pixel in size) that are specifically tagged to the email you were sent.

B. An article on Yahoo\textsuperscript{25} indicated that more people are wary about losing their banking data and email conversations than other content, including photos and address books. Apparently, almost one in three people surveyed had admitted to snooping on someone else’s phone. This article also provided some options to deal with that kind of snooping.

C. One of the best options for secure mobile computing is to use multiple email accounts. It is not unethical to do this, as long as you are not trying to deceive someone. I have an email account for my law office, one for my family, one for Procter & Gamble, one for junk email, one for lost passwords, and several others. One key thing I realized that confuses people when setting up accounts is that they do not realize they are not required to use their email password when signing up for the account. Usually, the account ID is the email address. When prompted for a password, some people think they need to use their email password. Do not do this. Use a different email password. If you cannot keep all of these passwords memorized, you can use password wallets like LastPass (https://lastpass.com/) to create and store these passwords.
