Fund Assembly
May 11, 2018
Orlando, Florida

Modern Technology and The Practice of Law: Lessons We Learned from the Three Little Pigs

Michael D. Simon, Esq.
Gunster, Yoakley & Stewart, P.A.
West Palm Beach, FL 33401
msimon@gunster.com

Introduction

Does anyone still use a rotary phone, a paper map, or a Rolodex ? When was the last time you wrote someone a letter – on paper – with a pen ? Advances in technology have transformed the way we live our lives. In many ways, new technology has made the practice of law easier, helped us to be more productive, and allowed us to conduct business from almost any place on Earth. However, these changes in technology have led to additional duties and obligations, which can be easily breached by an uninformed or careless attorney. For example, there are significant legal and ethical obligations relating to client confidentiality that come with many of the technological tools we use every day. In addition, developing areas of technology, such as Dropbox, Google Drive, and other cloud computing services, are the subject of several Florida ethics opinions.

In order to satisfy his or her duty of competence, a Florida lawyer must be reasonably up to date on technological advances that affect the practice of law. Keeping up with ever-changing technology can be challenging, but it is not impossible. Just knowing some basics concepts, and putting them into practice, may save both the lawyer and client from many of the hazards that modern technology can bring to the practice of law. The following topics are simply a few examples of the issues a lawyer may encounter in his or her everyday practice. These materials will provide a basic overview of the issues and offer a few examples of practical approaches to deal with them. Some issues are easier to address than others. For example, upgrading to a more complex password is fairly easy to accomplish. Convincing Google to change their End User License Agreement will be a bit more difficult. Finally, the author feels compelled to provide a disclaimer and a word of caution. Although quite a bit of research went into this endeavor, the author is not a technology expert, and these materials are provided merely to raise the reader's awareness of some issues we all face in the modern practice of law. Further, because technology changes quite rapidly, writings dealing with technology issues, such as these materials, can become outdated very quickly. Use these materials as a place to start, but do not rely on them exclusively.

The Three Little Pigs

Once upon a time there were three little pigs. One pig built a house of straw while the second pig built his house with sticks. They built their houses very quickly and then sang and danced all day because they were lazy. The third little pig worked hard all day and built his house with bricks.

Most of us remember the story of the Three Little Pigs. In this classic fairy tale, an old mother pig sends her three little pigs out into the world to seek their fortunes. Each of the little pigs has an unpleasant encounter with a big bad wolf. For two of the little pigs, the story does not end well. Although the third little pig must deal with the same wolf as his siblings, he fares much better. His success with the wolf was due, in large part, to his actions prior to the wolf showing up at his door. He understood the perils of the world (e.g. the Big Bad Wolf). He recognized he was a tempting target (i.e. wolves like to eat pigs). He made a plan to protect himself (I'll build a house instead of sleeping outside). He chose materials appropriate for the job (bricks instead of straw or sticks). Finally, he worked hard and carried out his plan before he was in trouble (He did not sing and dance the day away like his siblings).

The wisdom in this classic tale can provide us with valuable lessons in our world of rapidly changing technology. Which little pig will you be ?

1. We Are "Fiduciaries"

These materials focus on technology as it affects the practice of law, rather than our personal lives. As such, the concept of fiduciary duty comes into play.

The relationship between an attorney and client is a fiduciary relationship of the very highest character. *See, Elkind v. Bennett*, 958 So. 2d 1088 (Fla. 4th DCA 2007), relying on *Forgione v. Dennis Pirtle Agency, Inc.*, 701 So. 2d 557 (Fla. 1997). A fiduciary relationship exists "when confidence is reposed on one side and there is resulting superiority and influence on the other, and the relation and duties involved in it need not be legal, but may be moral, social, domestic, or merely personal." *See, e.g. Metcalf v. Leedy, Wheeler & Co.*, 191 So. 690 (Fla. 1939). A fiduciary relationship can be either express or implied. *Maxwell v. First United Bank*, 782 So. 2d 931 (Fla. 4th DCA 2001).

Recognizing that a lawyer occupies a fiduciary role will help put the rest of these materials, and the authority cited herein, in the proper perspective. For a good discussion of fiduciary relationships *see, Understanding Fiduciary Duty*, by John F. Mariani, Christopher W. Kammerer, and Nancy Guffey-Landers, Fla. Bar Journal, March 2010, at 20.

2. ABA Formal Opinion 477R (May 22, 2017)

Formal Opinion 477R was issued by The American Bar Association's Standing Committee on Ethics and Professional Responsibility on May 22, 2017. 477R may be the most comprehensive ethics opinion issued to date on the subject of the use of technology by lawyers. A detailed review of 477R is beyond the scope of these materials, but the following are a few of the highlights of the opinion.

- The committee stressed process over results;
- There are no safe harbors – it is a case by case analysis;
- "While the basic obligations of confidentiality remain applicable today, the role and risks of technology in the practice of law have evolved…"
- "How a lawyer should comply with the core duty of confidentiality in an ever-changing technological world requires some reflection"
- The Committee rejected requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopted a fact specific approach to business security obligations that requires a process to:
    - assess risks;
    - identify and implement appropriate security measures responsive to those risks;
    - verify that they are effectively implemented; and
    - ensure that they are continually updated in response to new developments.
- A lawyer must make "reasonable efforts" to prevent the access or disclosure of client confidential information.
- The committee cited to Comment 18 to Model Rule 1.6(c) for a list of nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:
    - the sensitivity of the information;
    - the likelihood of disclosure if additional safeguards are not employed;
    - the cost of employing additional safeguards;
    - the difficulty of implementing the safeguards; and
    - 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).

3. The Rules Regulating The Florida Bar Apply To Our Use Of Technology

Although it may seem obvious, the Rules Regulating the Florida Bar apply to our use (or lack of use) of technology in our practice of law. The three Rules that seem to have the greatest relevance to the present analysis are: (1) Rule 4-1.1 Duty of Competence; (2) Rule 4-1.6 Duty of Confidentiality; and (3) Rule 4-5.3 Duty to Supervise. Listed below are a few relevant points about each of these Rules.

I. **Competence** (*Rule 4-1.1*)

a. Rule 4-1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skills, thoroughness, and preparation reasonably necessary for the representation."

b. If a lawyer chooses to use devices that contain storage media (i.e. any device that contains a hard drive or other data storage device – e.g. you phone,) the lawyer has a duty to keep abreast of changes in technology. *See, Florida Ethics Opinion 10-2 (revised 9-24-14)* addressing *Rule 4-1.1.*

c. "This committee has previously opined that lawyers have an obligation to remain current not only to developments in the law, but also developments in technology that affect the practice of law." *See, Florida Ethics Opinion* 12-3 *(revised 4-26-16)* .

d. What is "the cloud"? *See, Florida Ethics Opinion 12-3 (revised 4-26-16)* .

e. Lawyers who use cloud computing have an ethical obligation to understand the technology they are using and how it potentially impacts confidentiality of information relating to client matters, so that the lawyers may take appropriate steps to comply with their ethical obligations. *Florida Ethics Opinion 12-3 (revised 4-26-16).*

f. Using the cloud – due diligence.

   (i.) Cloud computing is permissible as long as the lawyer adequately addresses the potential risks associated with it. The lawyer must perform due diligence in researching the outside service provider to ensure that adequate safeguards exist to protect information stored by the service providers. *See, Florida Ethics Opinion 12-3 (revised 4-26-16).*

g. What is adequate due diligence?

   (i.) The appropriate due diligence a lawyer should perform before storing files electronically with a third party using cloud computing includes determining:

      1. that the lawyer will have adequate access to the stored information;

      2. the lawyer will be able to restrict access of others to the stored information;

      3. whether data is encrypted and password protected; and

4. what will happen to the information in the event the lawyer defaults on an agreement with the third party provider or terminates the relationship with the third party provider?

See, Iowa Ethics Opinion 11-01.

II. **Confidentiality** (*Rule 4-1.6*)

a. Documents or data leaving the lawyer's office.

(i.) In order to maintain confidentiality under *Rule 4-1.6(a)*, Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyer's offices, including electronic documents and electronic communications with other lawyers and third parties. *See, Florida Ethics Opinion 06-2 (revised 8-24-11).*

b. Warn your clients.

(i.) A lawyer sending or receiving substantive communications with a client via email or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party may gain access. *See, ABA Formal Opinion 11-459.*

c. Theft or inadvertence.

(i.) An attorney is required to take competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence. *See, Arizona Ethics Opinion 05-04.*

d. Electronic storage of client files.

(i.) This committee concludes that the main consideration in file storage is that the appropriate documents be maintained, not necessarily the method by which they are stored. Therefore, a law firm may store files electronically unless: a statute or rule requires retention of an original document, the original document is the property of the client, or destruction of a paper document adversely affects the client's interests. However, lawyers must take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records. *See, Florida Ethics Opinion 06-1 (revised 4-27-16)*

e. Florida Information Protection Act of 2014 – *§ 501.171, Fla. Stat.*

(i.) Those subject to the Act must take reasonable measures to protect a client's confidential information.

III. **Duty to Supervise** (*Rule 4-5.3*)

a. Supervision of non-lawyers

(i.) Any work done by an attorney's non-lawyer employees must be supervised by the attorney as required by *Rule 4-5.3* to ensure that the non-lawyer employee's conduct is compatible with the professional obligations of the attorney. *See, Florida Ethics Opinion 00-4 (revised 8-31-11)*

(ii.) Rule 4-5.3, Rules Regulating The Florida Bar, requires an attorney to directly supervise nonlawyers who are employed or retained by the attorney. The rule also requires that the attorney make reasonable efforts to ensure that the nonlawyers' conduct is consistent with the ethics rules. A lawyer must give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client. The measures employed in supervising nonlawyers should take account of the level of their legal training and the fact that they are not subject to professional discipline. *See, Florida Ethics Opinion 07-2 (revised 10-21-16)*

4. Metadata and You

Simply stated, Metadata is "data about data." The most fundamental property of metadata is that it is distinct from the data itself. Some easy examples of metadata would be the name of the file, the file's location within the system, the type of file, the date it was edited, the editor, the date it was accessed, how long the file was worked on, and the file's size. Just from these few examples, we can begin to understand the significance of metadata.

Attorneys often think about metadata when referring to emails. However, metadata is not limited to email. It provides information about virtually every electronic document or file we deal with in our practice of law. This information includes the date, to, from, file size, attachments, folder, dates accessed, etc. Thus, metadata can provide valuable insight into the context, creation, modification and transmission of a message. Further, important associations can be revealed when metadata is properly analyzed.[1] Accordingly, it is important to know what metadata you are sending out and what metadata you are receiving.

In 2006, the Florida Bar published Ethics Opinion 06-2, which details a lawyer's obligations when sending an electronic document. Of particular note, Ethics Opinion 06-2 states: "A lawyer who is sending an electronic document should take care to ensure the

[1] See MIT Project "Immersion" which demonstrates the use of metadata in a user's Gmail account. https://immersion.media.mit.edu/

confidentiality of all information contained in the document,..." That sounds easy enough - until you read the next two words "… including metadata." The Florida Bar says not only do we need to know what metadata is, we need to know how to keep it confidential. In other words, it is no longer enough that lawyers take reasonable measures to ensure that the content of an electronic document remains confidential, but lawyers must now take reasonable measures to ensure that even the information about the data file (i.e. "metadata") remains confidential. The Florida Bar does not stand alone in this view. State Bars all over the country have issued similar opinions.[2]

Florida Ethics Opinion 06-2 notes that the disclosure of metadata requires the same consent to disclosure from a client as any other information associated with a representation under Rule 4-1.6. An attorney who inadvertently receives metadata falls within the scope of Rule 4-4.4(b). As such, an attorney inadvertently receiving metadata is required to promptly notify the sender in order to permit the sender to take any protective or remedial measures he or she deems necessary. Many attorneys do not realize that an attorney who receives a file is not allowed to "mine" the document for metadata if he or she has reason to believe that the disclosure of that metadata was unintentional. Florida's view on mining metadata appears to be more restrictive than the view expressed in ABA Formal Ethics Opinion 06-442. The ABA Ethics opinion seems to take a more liberal approach, and would allow an attorney to utilize metadata obtained inadvertently as long as the metadata was not obtained in a manner that was criminal, fraudulent, deceitful, or otherwise improper. Under the ABA opinion, the attorney has an obligation to inform the opposing lawyer of the inadvertent disclosure, but there is no restriction on the attorney's ability to utilize the metadata.

When sending electronic documents outside the law firm, an attorney should "scrub" the documents of any metadata that is intended to remain confidential. It is important to note that an attorney may have an obligation to produce electronic documents, with the metadata intact, when responding to formal discovery requests. A crude, but effective, way to ensure that metadata is not transmitted along with an electronic document is to print the document, scan it and then send the scanned version of the document to the intended recipient. By printing the document, you are, in effect, taking a picture of the document. The printed document is simply a piece of paper, which obviously has no imbedded electronic data. When you scan the printed document there will be no metadata remaining from the original document to transmit. A much faster, and more convenient, method to remove the metadata is to use one of many programs available to scrub metadata from outgoing electronic documents. Many of these programs are included within other programs already used by attorneys on a daily basis. The following are some examples:

Microsoft Word 2010

1) Go to File > Info > Check for Issues > Inspect Document

[2] ABA Metadata Ethics Opinions Around the U.S. (accessible at http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.)

2) Check all of the boxes
3) Click “Inspect”
4) Click “Remove All” for any sections which return results.

Adobe Acrobat [3]

1) Go to Document > Examine Document from the pull-down menu
2) Select Expand All to preview the hidden information
3) Click Remove then confirm removal
4) The changes are not applied until you Save the document

Although scrubbing files of metadata is necessary in some circumstances, as stated above, there are other circumstances when there may be restrictions on the destruction of this valuable information. The duty to preserve documents and data is not limited to the “surface layer” content of a document. Destruction of metadata can be considered a violation of a legal obligation to preserve evidence. Florida Rule of Civil Procedure 1.350 allows a request for Electronically Stored Information (“ESI”) to specify the form in which the ESI is produced. Rule 1.350 states that if no form is specified, the ESI shall be produced in the form in which the ESI is ordinarily maintained or in a reasonably useable format. As such, the safe path would be to preserve and produce the metadata, or to notify the other side that you are not producing the metadata.

5. P@sswords and Password Managers

Passwords on modern devices come in many forms. The iPhone gives you the choice of a 4 digit numerical passcode, a 6 digit numerical passcode, or an alphanumeric password. Although the alphanumeric password is the safer avenue, one must decide if, under the circumstances, it is necessary and worth the inconvenience. Android offers its own spin on passwords, by letting a user utilize a pattern based system rather than the traditional numbers and letters. Additionally, and depending on the device, you can use your fingerprint, your voice, or even a picture of your face as a “password”. These alternative “passwords” carry a cutting edge feel, but they may not be the most secure methods of protecting your data.[4]

So what is the most secure method of protecting confidential data? Simple math will provide some insight. A 4 digit, numbers only, passcode allows 10,000 possible combinations (10 x 10 x 10 x 10). Listed below are some further combinations of eight character passwords:

---

[3] http://www.flsd.uscourts.gov/wp-content/uploads/2012/10/RemovingHiddenInformationV9andX.pdf

[4] The permutations of a 5-character password compared to a 5-point pattern is approximately 390,536:1. http://www.makeuseof.com/tag/which-is-more-secure-a-password-or-a-pattern-lock/

Character Sets used in Password	Calculation	Possible Combinations
Dictionary words (in English): (It is debatable but let's generously say ~600,000 words)	—	600,000
Numbers Only	10^8	100,000,000
Lowercase Alpha Set only	26^8	208,827,064,576
Full Alpha Set	52^8	53,459,728,531,456
Full Alpha + Number Set	62^8	218,340,105,584,896
Full Set of allowed printable characters set	(10+26+26+19)^8	645,753,531,245,761

The longer your password, and the more characters used (e.g. number, letters and symbols), the more secure it becomes. Using the full set of allowed printable characters, we can increase the number of combinations by more than 44 Quadrillion combinations (44 with fifteen zeros behind it for those less mathematically inclined). As you can see, adding one more character can really make a difference. What is the difference between a 4 character, numbers only, passcode and a 4 character passcode with letters and numbers? Answer - 14,766,336 combinations. Using letters and numbers rather than just numbers makes a huge difference.

So now that you know to use a few different characters and a little bit longer password, you may ask: "What makes a good password?"[5] The answer is that complexity can be just as important as length. It is easier to guess "GoGators" than it is to guess "8y@h2". These are a few characteristics which security professionals agree make a strong password[6]:

1) It cannot be found in a dictionary;
2) It contains special characters and numbers;
3) It contains a mix of upper and lower case letters;
4) It has a minimum length of 10 characters;
5) It cannot be guessed easily based on user information (birthdate, postal code, phone number, etc.); and
6) It is not duplicated on multiple websites.

OK, great. "G52&px3T?22" is a strong password, but how are you supposed to remember it? What is the perfect trade-off between password security and practical considerations (such as actually being able to remember your password when you need it) ?

[5] The 10 most used passwords of 2016 as garnered from the many published stolen passwords throughout the year: (1) 123456, (2) 123456789, (3) qwerty, (4) 12345678, (5) 111111, (6) 1234567890, (7) 1234567, (8) password, (9) 123123, (10) 987654321

[6] http://www.makeuseof.com/tag/create-strong-password-forget/; http://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/

Welcome to the great debate. By the way, there is no easy answer, but here are some tips. Randomly replace letters with numbers, such as L to 1 or T to 7. Many people use anagrams to create complex, memorable passwords. As an example, "My first house was 6241 Jiminy Street and I paid $650 a month rent" translates to "Mfhw6JSaIp$6amr" which is suddenly much easier to remember. You might also try picking a password and then moving your fingers to a different location on the keyboard while typing the same pattern – for example "password" suddenly becomes – "-qww204e."

Another popular alternative to memorizing multiple, complicated, passwords is a Password Manager program. These programs store all of your passwords in one location so that they are accessible when needed. The Password Manager account is typically secured by multi-factor authentication (a password and a second means of confirming your identity such as a text message, email, or confirmation grid) and requires a much more complex initial password. The theory behind Password Managers is that everyone is capable of remembering one complicated password that can be used to access your other passwords. The Password Manager will typically offer things like a random password generator. Truly random passwords are far more usable when they are being remembered for you, rather than by you. Additionally, the majority of Password Managers will provide notice when your Password Manager account is accessed from an unexpected location, providing an added level of safety. Some options for Password Managers include Dashlane, LastPass, and RoboForm.[7] In addition, both Apple and Google offer password management within the operating system and their respective browsers. However, these "default" services do not provide near the features that third party programs currently allow.

6. Protecting your device from theft or loss

Until fairly recently, the risk of a loss of a significant amount of confidential client information was very small. A fire or a natural disaster, such as a flood or hurricane, were the only likely ways a large amount of client data could be lost. In those rare events, the data itself may be lost, but the confidential nature of the data was not compromised. The chances of a thief breaking into a law office or a warehouse containing client documents and making off with hundreds of boxes of documents was nearly zero. Times have certainly changed !

In the days before smartphones, laptops and computer tablets, a lawyer would rarely leave the office with more than a few hundred pages of client files on his or her person at any one time. Today, an iPhone 6 (128 GB) can store more than 85 million pages of text files. That is the equivalent of more than 17,000 banker's boxes of documents in your pocket. The iPhone 7 (256 GB) can store more than 173 Million pages of text files. These documents could contain

[7] http://www.pcmag.com/article2/0,2817,2407168,00.asp.

very sensitive client information, including, Social Security numbers, dates of birth, bank account numbers, PIN numbers, and tax filings.

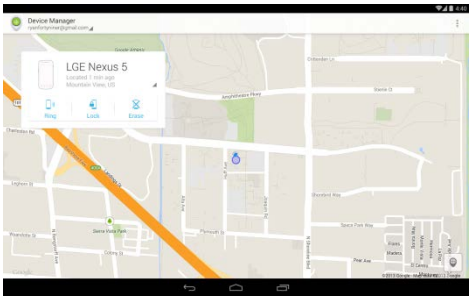
Florida lawyers have a duty to protect client information from theft or loss. This duty has become even more significant in light of the quantity of confidential client information a lawyer can now carry on his or her person. Florida ethics opinion 06-2 states: "In order to maintain confidentiality under Rule 4-1.6(a), Florida lawyers must take reasonable steps to protect confidential information in all types of documents and information that leave the lawyers' offices…". Arizona ethics opinion 05-04 is even more specific and requires an attorney to take "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence." According to Consumer Reports, in 2013, approximately 3.1 million Americans were victims of smartphone theft. In light of this statistic, a strong password and keeping a close eye on your mobile devices are some of the best ways to protect confidential client information. In the event your mobile device is lost or stolen, the ability to remotely delete (or "wipe") confidential client information from the device is invaluable.

7. Remote Wiping (i.e. Deleting) Data from Your Lost or Stolen Device

What happens when you leave your mobile device at a restaurant, in a taxi, or sitting on a park bench ? Once you conclude that the device is forever lost, it is time to hit the self destruct button.

Both Apple and Android provide mechanisms for remote wiping of your device. Neither manufacturer offers a perfect solution, but both provide an added level of security to your confidential information. In order to utilize these programs you must do the initial set up while you still have the mobile device in your possession. iPhones utilize a well-known service called "Find My iPhone" and Android phones have access to a similar program called "Find My Device." Both of these applications provide a way to locate a lost device, and in a worst case scenario, they provide the ability to wipe (delete) all of the data from the lost device.

Android Find My Device



Apple Find My iPhone

As you can see from the above screenshots, both services give you multiple methods to locate and secure your phone. First, you can play a sound to help locate your lost phone. This can

be quite important if you have lost your device with the ringer turned to silent. The service uses your device's GPS to show the last known location of the device (typically this will get you to the last building the device was in). Both services give you the ability to lock your phone. This means that in order to get into the device a user would need to have your passcode. An added feature of this remote lock is that you can display a message and telephone number (presumably somewhere you can be reached) that will immediately appear on the screen. This is a great way to recover your phone if it has fallen into the hands of an honest person.

If you have determined that the phone is not going to be recovered, the Wipe/Erase options give you the ability to remotely wipe the device. In other words, you can delete all of the data on the device, even though it is not in your possession. The remote wipe feature works like this: (1) a signal is sent over the internet to the phone that the remote wipe feature has been activated; (2) the next time the phone is connected to the internet (whether it is via a wifi connection, computer connection, or mobile network) all of the data on the device will be deleted and the device will reset to the factory settings; and (3) after the device is wiped, a confirmation email is sent to your registered email address saying that the data on the device has been erased. While this does not recover your device, and you are likely out a few hundred dollars for a new device, it does give you the comfort of knowing your confidential data is secure.

iPhone: Using Find My iPhone

Pre-Loss[8]

1) Go to Settings
2) Tap "iCloud"
3) Scroll to the bottom and tap "Find My iPhone"
4) Slide to turn on Find My iPhone and Send Last Location

Post-Loss[9]

1) Go to iCloud.com and log in with your Apple ID and password
2) Click "All Devices", then select the device you want to find/erase
3) In the devices info window, click "Play Sound", "Lost Mode", or "Erase iPhone" depending on which option you want to use.
4) Follow the onscreen prompts.

Android: Using Find My Device

Pre-Loss[10]

1) Go to Settings > Security & Location > Find My Device

[8] https://support.apple.com/en-us/HT205362
[9] https://support.apple.com/kb/ph2696?locale=en_US
[10] https://support.google.com/accounts/answer/3265955?hl=en

2) Turn on "Remotely locate this device" and "Allow remote lock and erase."

Post-Loss[11]

1) From any desktop go to "google.com/android/find" or simply google "find my phone" (Quick tip: if you are already logged into Google Chrome, simply google the phrase "Where is My Phone")
2) Log in using your Google sign-in
3) In the devices info window, click "Play Sound", "Lock", or "Erase" depending on which option you want to use.

8. Mobile Data Storage Devices (Thumb Drives and External Hard Drives)

Thumb drives are miracles of modern science. An average laptop purchased in 2002 had a 2 GB hard drive which was more than capable of holding almost every digital asset most people had accumulated up to that point in time. Today, you can buy a 16 GB thumb drive for $5 on Amazon.com. These small devices have become one of the primary ways we transport our electronic files, both confidential and not confidential. However, they can also be completely unsecure if you do not utilize the available security measures, both on the hardware and software side.

One of the easiest ways to safeguard your information is to password protect the files you place on a thumb drive. Programs like Microsoft Word and Adobe PDF have native methods for password protection, which are detailed below. Additionally, putting files into a password protected ZIP folder can just as easily do the trick (if you know what a ZIP folder is). These methods provide an added layer of security if your thumb drive is lost or stolen.

Additionally, there are programs now available which can be installed directly to the thumb drive which password protect the drive's contents. Free programs such as 7-zip allow you to create an encrypted archive on the flash drive.[12] You may also purchase other options like Encrypt Stick that can provide higher grade encryption. [13] By utilizing these programs a user can convert an unsecured flash drive into a secure flash drive in seconds without much additional effort.

If you often utilize flash storage, or you do not want to encrypt the drive yourself, you may want to invest in a secure thumb drive which comes with protections already built in. There are a number of companies that manufacture and sell secure thumb drives. Do your homework and choose one that meets your needs. One well-known manufacturer in this field is IronKey,

---

[11] Id.
[12] http://www.7-zip.org/
[13] http://www.encryptstick.com/

which makes a line of secure thumb drives with pre-installed software based encryption. These features significantly raise the price of a thumb drive (a 4GB IronKey drive is currently $119 on Amazon). However, if your confidential client information fall into the hands of an identity thief, it will be hard to explain to your client why you decided not to spend $119 to buy the secure thumb drive.

One drawback to software based protection placed directly on the thumb drive is that some networks do not allow an executable file to be run through an external hard drive (this means that any ".exe" files will not operate on that system unless installed by an administrator). In light of these restrictions, there are hardware based solutions such as the Imation Defender F200 and the Aegis Secure Key which require authentication to unlock the drive. The F200 uses a finger print scanner while the Aegis uses a 10 digit keypad. Although more secure, these thumb drives are expensive. One of these 4GB thumb drives costs about $119.

To utilize Password protections in the native programs, follow these steps:

Microsoft Word[14]**:**

1) Go to File > Save As
2) In the Save Dialog Box, select Tools > General Options
3) In the "Password to Open" field, enter your selected Password.
4) Save

Adobe Acrobat:

1) Go to Advanced > Security > Encrypt with Password
2) Select "Encrypt all document contents"
3) Select "Require a password to open the document"
4) Enter your selected password in the "Document Open Password"
5) Click OK
6) Confirm your new password
7) Save the Document to apply the new password settings.

9. Sharing Your Mobile Device and the Duty to Supervise

All Florida lawyers should be familiar with the concepts of attorney client privilege and the confidentiality of client communications under Rule 4-1.6. The comments to Rule 4-1.6 state: "The principle of confidentiality is given effect in 2 related bodies of law, the attorney-client privilege (which includes the work product doctrine) in the law of evidence and the rule of confidentiality established in professional ethics. The attorney-client privilege applies in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to

[14] https://support.office.com/en-ie/article/Password-protect-a-document-8f4afc43-62f9-4a3a-bbe1-45477d99fa68

produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. The confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source."

Rule 4-1.6(e) is particularly relevant to an analysis of a lawyer's ability to "share", "loan", or grant access to his or her mobile device to a third party, including a member of the lawyer's family (e.g. kids or spouse). The text of Rule 4-1.6(e) reads: "**(e) Inadvertent Disclosure of Information** A lawyer must make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

The comment to Rule 4-1.6(e) states: "**Acting Competently to Preserve Confidentiality** Paragraph (e) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See rules 4-1.1, 4-5.1 and 4-5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (e) *if the lawyer has made reasonable efforts to prevent the access or disclosure*. ***Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to***, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and 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). A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to forgo security measures that would otherwise be required by this rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, for example state and federal laws that govern data privacy or that impose notification requirements on the loss of, or unauthorized access to, electronic information, is beyond the scope of these rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see the comment to rule 4-5.3." (emphasis added).

Most lawyers do not intentionally violate the mandate of Rule 4-1.6(e), but quite a few may do so unintentionally. For example, sharing a computer with one's spouse or children, without taking measures to restrict access to email or other documents containing confidential information, may violate Rule 4-1.6(e). Unlocking your smart phone and handing it over to a friend to make an unsupervised phone call may also be a violation of the Rule. Even letting your children play games on your phone or iPad could violate Rule 4-1.6(e). While it may be difficult to explain to our family and non-lawyer friends the concepts of client confidentiality and fiduciary duty, those concepts govern our conduct and we must adhere to them.

Rule 4-5.3 addresses a lawyer's duty to supervise non-lawyers. Although this Rule is most commonly applied in the context of legal secretaries, paralegals, investigators and law student interns, it also applies to other types of non-lawyers outside the lawyer's firm. The comment to Rule 4-5.3 provides several examples of non-lawyers who fall within the scope of the Rule, such as employees of a document management company, printing service, or internet data storage service. Although the Rule provides examples of non-lawyers who fall within its scope, the Rule does not limit its scope to the specifically listed categories of non-lawyers. Thus, an employee of a computer repair company would seem to fall within the Rule, as would an employee of the Apple store at the mall. The comment to Rule 4-5.3 clearly states: "When using these services outside the firm, 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." There is no doubt that compliance with Rule 4-1.6 and Rule 4-5.3 will cause, at the very least, a minor amount of inconvenience and aggravation. Nevertheless, as members of the Florida Bar, lawyers are charged with certain duties, even if complying with them means our kids think we are "grumpy meanies", our friends think we are selfish with our phones, and the guy at the Apple store thinks we are crazy.

10. Using Public WiFi

There are many people who believe that utilizing public WiFi is a bad idea.[15] We are warned about the hacker who is sitting nearby waiting for you to access your private information, the malicious hotspots that dupe you into joining, and computer viruses that attack while you sip your latte and browse Youtube. While these fears are by no means unfounded, and lawyers should exercise caution when accessing public wifi, no one is advocating that lawyers may never access a guest network.

The California bar has articulated the factors an attorney should consider when transferring data through unsecured networks.[16] The California Bar notes that an attorney may utilize emerging technology, such as public wifi, to transfer client materials, but the lawyer should consider: (a) the ability to assess the security of the technology; (b) the legal ramifications to third parties of accessing/intercepting this information; (c) the degree of sensitivity of the information being transferred; (d) the possible impact on the client of inadvertent disclosure; (e) the urgency of the situation; and (f) the client's instructions.[17] In essence, the attorney needs to stop and ask how secure is this network, do I need to do this now, and what are the ramifications if something goes wrong? Because most lawyers are going to use unsecure wifi from time to time, there are some things that lawyers should know when assessing the situation.

---

[15] http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/

[16] CA Eth. Op. 2010-179 (Cal. St. Bar. Comm. Prof. Resp.)

[17] Id. at *6.

First, evaluate the network you are logging in to. Just because you see a wifi network which is open to the public, does not mean you should be on it. Xfinity and ATT give wifi access at locations throughout the country. Unfortunately, it is fairly easy to set up a "rogue access point" titled "Xfinity" and make it accessible to everyone.[18] If you are in a location where you did not expect to see a wifi connection, you should make sure it is official before tapping into it. On iPhones purchased on the AT&T network, the handset is set up to automatically connect to AT&T networks by default. You have the ability to choose when your phone connects to those networks, but only if you choose this option.[19]

Some experts recommend that you utilize "https" addresses as much as possible while on public wifi.[20] These sites utilize additional security protocols, which make it more difficult to snoop on traffic.[21] Google, for instance, will soon begin marking all non-https sites as "nonsecure", meaning you get a warning any time you seek to access such a site. While https is by no means foolproof, it may add an additional level of protection. Please note that if you are asked to enter sensitive information into a website which is not "https" you should exercise caution because the transfer of data will not be secure and almost any reputable site would (or should) be running an "https" protocol at this point in time.

Finally, if you are frequently using unsecured wifi (i.e. you travel a lot) it may be time to invest in a Virtual Private Network or "VPN."[22] A VPN encrypts traffic between your device and the VPN server, making it much more difficult for intruders to intercept your data transmission. Most firms and businesses are now utilizing some type of VPN structure for people accessing their network from outside of the office's four walls. Check with your firm to determine if a VPN has already been set up for your use. Alternatively, there are both paid and free VPN services available. The paid services are offered at a relatively low price point.[23] The free services come with a certain amount of buyer-beware, as you are reliant on the VPN to keep your privacy properly encrypted and if they are not charging you a fee then the red flags may need to go up. All that being said, in light of the rolling back of regulations by the FCC on internet service providers under the Trump administration, having access to a VPN on a continuous basis is more necessary than ever.[24]

---

[18] http://arstechnica.com/security/2014/06/free-wi-fi-from-xfinity-and-att-also-frees-you-to-be-hacked/

[19] To turn off automatic connection go to Settings > Wi-Fi. Select the network you wish to not automatically join. Deselect "Automatically Join" if it is an available option. If "Automatically Join" is not an available option, click "Forget this Network" which will require your device to ask prior to joining the network again.

[20] http://www.forbes.com/sites/amadoudiallo/2014/03/04/hackers-love-public-wi-fi-but-you-can-make-it-safe/. For that matter, Google now labels any non-https site as insecure. https://security.googleblog.com/2016/09/moving-towards-more-secure-web.html

[21] http://www.snopes.com/computer/internet/https.asp

[22] http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html

[23] Supra FN 31.

[24] http://lifehacker.com/why-is-everyone-talking-about-vpns-1793768312

11. How to Get Rid of That Old Phone

The time has come to upgrade to that newer model smartphone (in today's world that means about six months has passed). For years this meant going into the AT&T store, signing up for a new contract and handing over your old phone in exchange for a fancy new one. In the age of flip phones, the amount of data you were handing over to AT&T was small, but not insignificant; telephone numbers, contacts, text messages, and (if you were cutting edge) some email. In the today's world, where you can have most of your client files in your pocket, one needs to be far more careful. You cannot just hand over your mobile device to the clerk and expect that he will take care of scrubbing it clean (deleting all data). You need to be proactive and be ready to handle it yourself - If you choose to hand over your mobile device at all.

Option 1: Wiping Your Phone

Exchanging your phone, or selling it to a third party vendor, can mean quick dollars. Selling or trading in an old device is the typical way people offset some of the costs of a new device. However, before you turn over your phone you need to be sure that you have properly deleted all of the confidential data on the device. "Properly" is the key term, as mining (legal and illegal) of confidential data has become a growing industry in the modern age. It is not hard to find examples of data mining. Deleted data is regularly recovered from used cell phones[25], scanned and copied documents are recovered from copy machines,[26] personal emails supposedly deleted are recovered from discarded servers.[27] While there is not a perfect way to prevent others from recovering data from your discarded mobile device, and still leave the device intact, there are methods available (even to the basic user) which can delete the majority of the data from your device, or at least render it inaccessible.

The most utilized method to "wipe" a mobile device is encryption of your device's data, followed by the destruction of the encryption key. Apple's iPhone has been encrypting all of the data placed on it since the iPhone 3GS models (this also goes for all models of the iPad). In 2015 Android began default encryption with its Marshmallow (Android 6.0) operating system. Through the use of hardware encryption, all the data placed on your device is automatically encrypted through a hardware encryption key. The encryption function is turned on by default. Android phones made in the last few years also have this option (and some prior to that date) but it may not be turned on by default. This protection provided by encrypting the data is made stronger through the use of a passcode to unlock the device.

---

[25] In 2014, the company Avast claimed that they could easily purchase old Android phones off of Ebay and restore the deleted data through readily available data recovery software. See, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html.

[26] A 2010 CBS News report points to the ability of identity thieves to gain possession of old copy machines and recover the data that is contained on their hard drives. http://www.cbsnews.com/news/digital-photocopiers-loaded-with-secrets/

[27] Oh Hillary. http://www.bloomberg.com/politics/articles/2015-09-22/fbi-said-to-recover-personal-e-mails-from-hillary-clinton-server

Most of the time, when a user "deletes" the data from a properly encrypted device, the data is not actually deleted. Rather the "encryption key", which is used to unscramble the 1s and 0s used to write your message, is destroyed. By destroying the encryption key, the data is theoretically rendered unusable without resort to advanced software and recovery devices. At least, it makes recovery of the data far more expensive, difficult, and time consuming. "deletion" of the encryption key is the method most utilized to "wipe" a mobile device.

There is software available which will actually delete all of the data on your device. To do this, these programs overwrite your existing data with random, meaningless data. This is the most secure method to protect confidential data.

So now that you know the basics of data "deletion", here's how you do it:

iPhone:

Hardware Encryption: For iPhones it is automatic, so this step is already done.

Set a Passcode[28]:

1) Go to Settings > Touch ID & Passcode.
2) Tap "Turn Passcode On."
3) Enter a six-digit passcode, or tap Passcode Options to switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code.
4) Enter your passcode again to confirm it and activate it.

Secure Deletion[29]:

1) Go to Settings > iCloud. Scroll down and tap "Sign Out."
2) Tap "Sign Out" again, then tap "Delete from My iPhone" and enter your password.
3) Return to Settings and tap General > Reset > Erase All Content and Settings.
4) Enter your passcode.
5) Tap "Erase"

Android:

Hardware Encryption[30]:

1) Go to Settings > Security & Location > Encryption & Credentials.
2) Set a PIN (a/k/a passcode) if you have not already done so.
3) The phone will go through the encryption process and will reset itself, likely asking you to insert the PIN.

Set a Passcode[31]:

---

[28] https://support.apple.com/en-us/HT204060
[29] https://support.apple.com/en-us/HT201351
[30] https://siliconangle.com/blog/2016/03/16/we-know-your-android-phone-isnt-encrypted-so-heres-how-you-encrypt-it-in-a-few-easy-steps/

1) Go to Settings > Security & Location > Screen Lock.
2) Tap either “PIN” or “Password”
3) Enter a 4-digit Pin, Password, or Pattern.
4) Go to Settings > Security > Screen Lock.
5) Tap “Lock Screen”

Secure Deletion[32]:

1) Go to Settings > System > Reset Options >“Factory Data Reset” or “Erase all data”
2) Confirm you want to Erase
3) Enter your PIN
4) Confirm Deletion

Option 2: Physical Destruction

As described above, wiping your phone is not 100% safe. Even “deleting” all of your data with the proper methods can be overcome by advanced techniques. The most secure way to dispose of an old phone is keep it, or to physically destroy it. A hammer and a bucket of salt water will do the trick.[33] My recommendation, wait for a particularly tough day at the office, retire to your garage with your no longer needed electronic device, some eye protection, and your sturdiest hammer. Beat on the device until it is an unrecognizable pile of plastic and metal bits. Make sure to get at the insides of the device in addition to the screen (but have fun with the screen as well). Once finished, take the bulk of the materials and put them in a bucket of salt water (or acid, if you are a “Breaking Bad” fan) to soak for a few days. At this point the data should be, at a minimum, heavily compromised, and likely destroyed. Finally, take the pieces to any locally available electronic recycling center (Best Buy, for instance, allows old device drop offs).

[31] https://www.howtogeek.com/253101/how-to-secure-your-android-phone-with-a-pin-password-or-pattern/
[32] http://www.cnet.com/how-to/the-best-way-to-completely-wipe-your-android-device/
[33] As will a drill, baseball bat, flamethrower, blender, sledgehammer, bucket of acid, or gun. If these don’t suit your fancy, Youtube has plenty more good ideas as well. https://youtu.be/dk4adP2Pi-Q