

Brett Burney

Principal, Burney Consultants LLC
burney@burneyconsultants.com

Brett Burney is Principal of Burney Consultants LLC, and focuses the bulk of his time on bridging the chasm between the legal and technology frontiers of electronic discovery. Brett is also very active in the Mac-using lawyer community, working with lawyers who want to integrate Macs, iPhones & iPads into their practice. Prior to establishing Burney Consultants LLC, Brett spent over 5 years at the law firm of Thompson Hine LLP where he worked with litigation teams in building document databases, counseling on electronic discovery issues, and supporting them at trial. Brett graduated from the University of Dayton School of Law in 2000 and quickly became active in the world of legal technology. Brett is a frequent contributor to Legaltech News and speaks around the country on litigation support, e-discovery, Mac and iOS-related topics.

In 2015, Brett Burney served at the Chair of the Planning Board for the annual ABA TECHSHOW (www.techshow.com). Brett is the author of the ABA-published book “Macs in Law: The Definitive Guide for the Mac-Curious, Windows-Using Attorney” (www.macsinlawbook.com) and also posts on the popular Apps in Law blog (www.appsinlaw.com) where he reviews apps for the legal community. Lastly, Brett is also the co-author of the eDiscovery Buyers Guide that can be freely downloaded at www.ediscoverybuyersguide.com.

Website: <http://www.burneyconsultants.com>

E-Discovery Blog: <http://www.ediscoveryinfo.com>
eDiscovery Buyers Guide: <http://www.ediscoverybuyersguide.com>

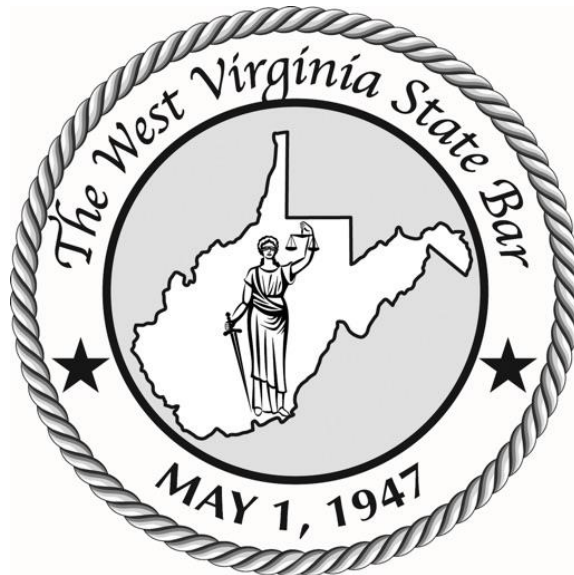
Macs for Lawyers: <http://www.macsinlaw.com>
Apps for Lawyers: <http://www.appsinlaw.com>

Law in Motion:

How to Ethically Protect the Information You Carry on Your Mobile Device

Brett Burney
Burney Consultants LLC
www.burneyconsultants.com

Apps in Law Blog
www.appsinlaw.com



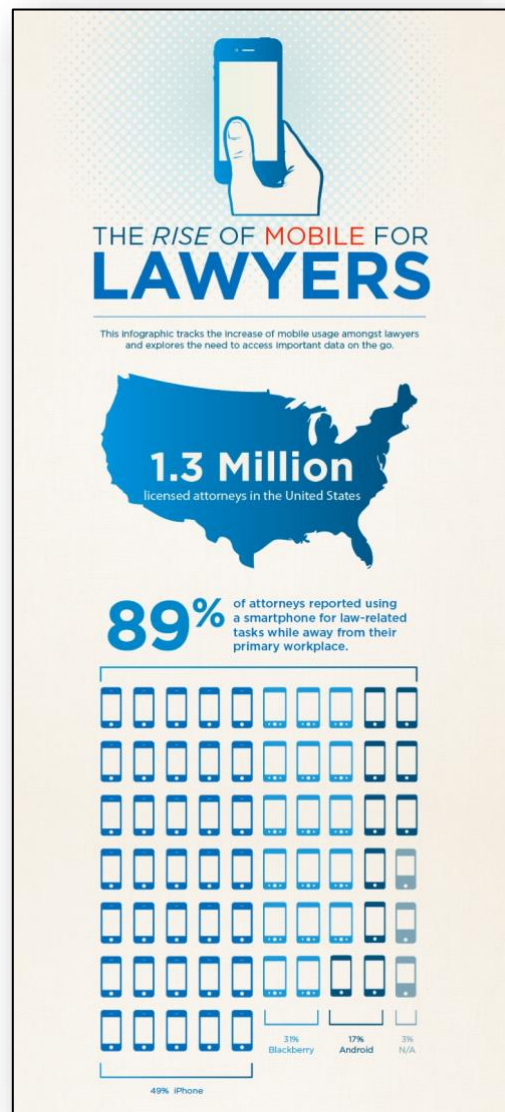
In the "Rise of Mobile for Lawyers" infographic¹, 89% of lawyers reported using a smartphone for law-related tasks while away from their primary workplace. In addition, 60% of those lawyers stated that they used tablets for work related purposes (with 91% of those respondents replacing the word "tablet" with "iPad").

The trend is undeniable – it's a mobile world and lawyers are adapting appropriately. The only complication is that lawyers must be aware of risks of carrying so much client confidential information on smartphones and tablets.

The "Rise of Mobile for Lawyers" infographic also supplies a nice list of "items lawyers need access to on the go":

- E-mail
- Calendar
- Time & Expense
- Documents
- Messaging
- Contact Info
- Case Info
- Tasks
- Invoice & Bills
- Accounting

All of items listed above involve information related to clients, and "information related to the representation of clients" is covered by the ABA Model Rules of Professional Conduct. If any of the information above gets inadvertently exposed to someone outside of the attorney-client relationship, that compromising situation could be actionable under the ABA Model Rules.



¹ See "9 out of 10 Lawyers Use Mobile Devices to Do Their Jobs [Infographic]" (<http://newstex.com/2013/04/25/9-out-of-10-lawyers-use-mobile-devices-to-do-their-jobs-infographic/>)

Mobility in the Model Rules

ABA Model Rule 1.6(a) states that “a lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent.” Rule 1.6(c) further states that “a lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of ... information relating to the representation of a client.”

Comment 19 to Model Rule 1.6 dictates that lawyers must take “reasonable precautions” to prevent confidential client information from “coming into the hands of unintended recipients.”

And finally, Comment 18 to the Rule requires “a lawyer to act competently to safeguard information relating to the representation of a client.”

It’s that competency requirement that has received a recent and fundamental tweak.

Model Rule 1.1 states that “**competent representation** requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” This rule obviously covers awareness of substantive changes to the law but in August 2012, the ABA House of Delegates adopted changes to Comment 8 of Rule 1.1² requiring a lawyer to “**keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.**”

The “benefits” of using mobile devices are countless – lawyers are able to do more than ever before when they’re out of the traditional office surroundings. There are so many more options for communicating with clients today, and with the rise of tablet devices, lawyers can carry hundreds of thousands of documents right under their arm in one small portable device.

The “risks” of using mobile devices pose some grave considerations that cannot be taken lightly. Since there is so much client confidential information that is stored and carried around on these mobile devices, it would be a serious breach of client

² See generally “ABA Amends Model Rules of Professional Conduct to Address Changes Brought by Technology and Globalization” (<http://www.jdsupra.com/legalnews/aba-amends-model-rules-of-professional-c-23504/>), JD Supra Law News, May 7, 2013.

confidentiality if that mobile device was lost or stolen. Mobile devices are so appealing because of their amazing mobility, but the risks are that they are that much more easier to lose or misplace than a laptop or desktop computer.

Just think of the amount of privileged and confidential information that you carry in email, both in the body of email messages as well as the attachments. If someone were to access your email from your mobile device, would they not have access to the most sensitive and confidential information that has been entrusted to you?

That's why it's imperative to take the minimum "reasonable precautions" to protect the risk of exposing that information in your email unnecessarily. And one of the best methods to prevent that exposure is to place a passcode on your mobile device.

Cracking the Passcode

There are no specific requirements for lawyers carrying mobile devices, but at the very least, a "reasonable precaution" would require a lawyer to enable a passcode on any device that they carry that gives them access to their e-mail.

A lawyer's e-mail today is chock full of important and confidential information relating to the representation of a client. Without a passcode to lock the device, anyone that picked up the mobile device would have complete and unfettered access to all of the client-related messages and attachments.

Most passcodes for mobile devices are simply a 4-digit number, similar to a banking ATM PIN (although the latest iPhones require a 6-digit number to be more secure). Some mobile devices allow you to switch to a more lengthy alphanumeric password. A longer password would certainly be much more secure than a 4-digit number, but it



would be incredibly inconvenient to have to type that password into your device every time you need to use it.

In some circumstances, a lawyer may need to use a longer password if the information on their mobile device is especially sensitive. But the 4-digit or 6-digit number will be adequate and reasonable for most circumstances.

Passcodes are not without fault and they can certainly be compromised, but they act as a strong deterrent for anyone attempting to easily compromise the information stored on a lawyer's mobile device. Just be sure the passcode that you select is difficult for anyone to guess. A simple passcode (such as "1234") is worthless since it can be guessed so easily.

Good Password Hygiene and Management

Another excellent practice for legal professionals is to start using a password manager such as 1Password (www.1password.com) or LastPass (www.lastpass.com).

Password managers keep track of all the passwords that you usually have to remember **and keep in your head. It's impossible to keep track of all the** passwords that we have to remember, so most of us just resort to using the same password over and over and over on every website, **and we usually choose a password that's short and easy to** remember.

The repercussions of this practice are dangerous and negligent because once a password is compromised in a **"data hack"** or similar, then that password is no longer secure.

A password manager such as 1Password or LastPass remembers all the passwords for you, so you can focus on more important legal work. Plus, password managers can also generate highly-secure



passwords for you which allows you to use different passwords on different websites. And all of these passwords are kept secure under one, single, highly-secure password that you have to remember.

While password managers certainly work on your Mac or PC, both 1Password and LastPass have robust mobile apps that give you access to your passwords from anywhere. In addition, both apps allow you to store other sensitive information such as your social security number, credit card numbers, etc.

If you've never used a password manager, it is absolutely imperative that you download a trial version of either 1Password (www.1password.com) or LastPass (www.lastpass.com) and become familiar **with the “benefits” of using a password manager to avoid the “risks” of NOT using one!**

The screenshot shows the 'Apps in Law' website. The main content area features a podcast episode titled 'AiL004 – Jeff Richardson only remembers one password' dated March 30, 2017, by Brett Burney. The episode description includes a logo for 'Apps in Law Podcast' and a photo of Jeff Richardson, a lawyer at Adams and Reese LLP. A sidebar on the right contains a search bar, a sign-up form for app reviews, and a 'Recent Posts' section listing other episodes.

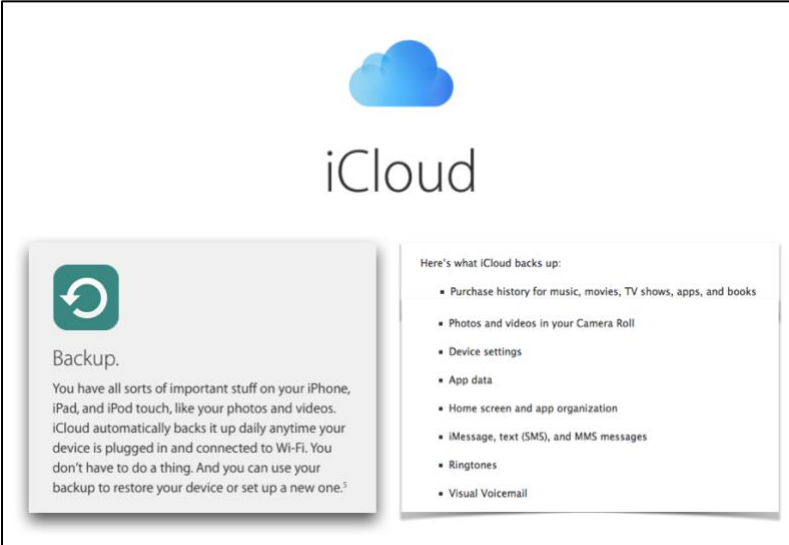
Hear how one attorney uses 1Password on the Apps in Law podcast:
<https://appsinlaw.com/ail004-jeff-richardson-only-remembers-one-password/>

Forward Thinking to Backing Up

Another reasonable precaution to protect confidential client information stored on mobile devices is to create frequent backups of the information. This ensures that the information can be recovered or restored in the event a mobile device is lost, stolen or misplaced. Just like lawyers should have backups of information stored on their computers and servers, it is just as important to have backups of information stored on their Androids, iPhones & iPads.

For iOS devices, you can use the iTunes software application on either a Windows or Mac computer to back up the contents of an iPhone or iPad. But now with Apple's iCloud service, all of the contents of your iOS device can be backed up automatically to the cloud. Anytime that you can automate a backup is preferred simply because that means the lawyers doesn't have to remember to initiate the backup and it just happens in the background.

Backups are important because the information can be "restored" from a backup when necessary. For example, if a lawyer has an iPad stolen while traveling, they can remotely erase all of the information stored on the device so that it is not compromised. Once they purchase a replacement iPad, they can connect to their iCloud account and restore all of their information to the new device and continue working without missing a beat.



The graphic features the iCloud logo at the top center. Below it, on the left, is a grey box with a green circular arrow icon and the heading "Backup." followed by text explaining that iCloud automatically backs up data from iPhones, iPads, and iPod touches daily when connected to Wi-Fi. On the right is a white box titled "Here's what iCloud backs up:" containing a bulleted list of backed-up items.

iCloud

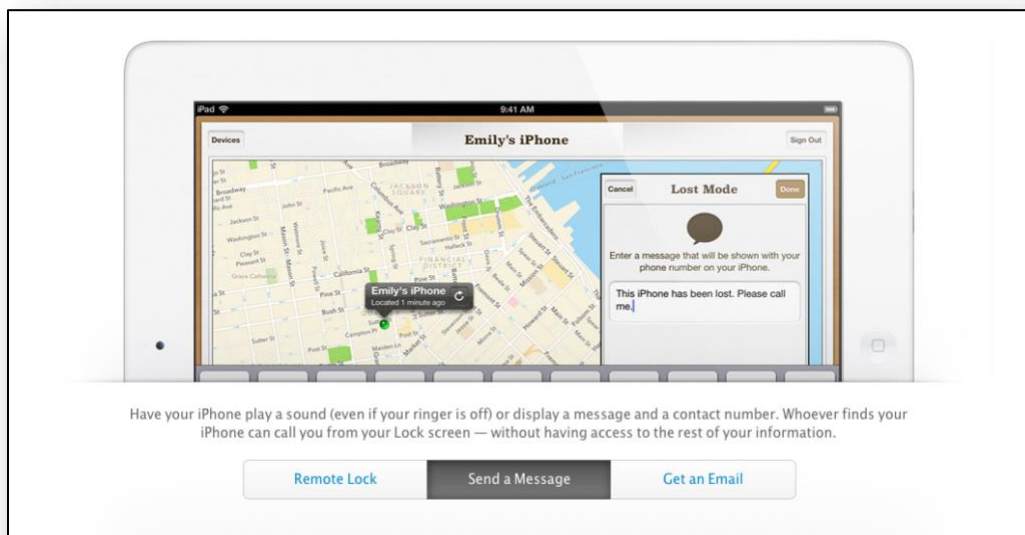
Backup.
You have all sorts of important stuff on your iPhone, iPad, and iPod touch, like your photos and videos. iCloud automatically backs it up daily anytime your device is plugged in and connected to Wi-Fi. You don't have to do a thing. And you can use your backup to restore your device or set up a new one.⁵

Here's what iCloud backs up:

- Purchase history for music, movies, TV shows, apps, and books
- Photos and videos in your Camera Roll
- Device settings
- App data
- Home screen and app organization
- iMessage, text (SMS), and MMS messages
- Ringtones
- Visual Voicemail

Find My iPhone / iPad Service

Another important "reasonable precaution" that lawyers can take to protect their mobile devices is to utilize a service like "Find My iPhone" offered by Apple for iPhones and iPads. There are similar services available for other devices but nothing is quite as integrated as the "Find My iPhone / iPad" services offered by Apple.



The "Find My iPhone" service is completely free and part of iCloud. Once an iPhone or iPad is set up to access the service, that device can be located on a map from any computer or mobile device connected to the Internet.

Once the device is located, there are several things that can be done with the device. First, it can be remotely locked with a passcode if the user has neglected to set one up before.

Second, a message can be sent to the device that contains the phone number of the owner along with a message containing instructions on how to return the device.

And lastly, if the device is unable to be recovered, the device can be triggered to completely erase itself so that no information can be recovered.

Mobile Device Management (MDM)

If you practice at large law firm or corporation, your device may already be controlled by an internal IT staff member. Many large firms and corporations have mobile device management (MDM) systems that can remotely control, secure, and wipe mobile devices. For example, BlackBerry devices work very well with a BlackBerry Enterprise Server (BES) that can remotely control and manage devices "over-the-air." There are other similar services such a Good Enterprise (www.good.com) and MobileIron (www.mobileiron.com).

Even if your firm or organization has a Microsoft Exchange server for e-mail, the Microsoft ActiveSync software can be used on the server to require things like a passcode on the device before the device is allowed to receive e-mail.

You'll need to check with your IT department to inquire is an MDM system is set up at your organization. The important thing to understand is what exactly the MDM system is accomplishing vs. your own responsibility. For example, some MDM systems are used to restrict access to certain apps that can be downloaded and installed on iPhones or iPads, but they will not perform a backup of the device which means you may need to set up your own iCloud account to accomplish this task.

Stephen is a frequent speaker, blogger and writer. He publishes [TechLaw Crossroads](#), a blog devoted to the examination of the tension between technology, the law and the practice of law. He is co-chair of Secretary and part of the Leadership Council of the ABA's [Law Practice Division](#). Stephen serves as Chair of the Kentucky Bar Association's Law Practice Task Force and Webinar Chair and Steering Committee member of [Defense Research Institute's Law Practice Management section](#). Stephen is a national litigator and advisor primarily in the mass tort, business and consumer class action, and privacy and data breach arenas. .

The Ethical and Practical Case for Lawyer Technological Competency

1.0 What is Technological Competence?

Before getting into the ethical and practical reasons for lawyers to have some level of technological competence, it is worth considering what technological competence really means. Some believe technologic competence means knowing, for example, how to code. Some mistakenly believe technological competence means knowing anything and everything about all technology. Both are wrong.

Quite simply what technological competence for lawyers really means is being knowledgeable about and using that technology which is or could relate to what you do in your practice. It means knowing what technology is available to help your clients and help us as lawyers to be better at our chosen profession. It means knowing what technology that is relevant to our practice can and can't do.

2.0 Ethical Reasons for Technological Competency

The ethical duties of a lawyer relating to technology are found in Model Rule 1.1 (competence), Rule 1.6 (confidentiality), Rule 1.5 (ethical billing) and Rules 5.1 and 5.3 (supervisory responsibilities). These rules and their nuances are discussed below.

2.1 Competence (Rule 1.1)

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

To understand what this means in terms of technology, it is necessary to look at the findings of the 2009 Ethics 20/20 Commission created by the American Bar Association (ABA) which was charged with looking at how technology might affect the Model Rules of Professional Conduct. The Commission determined that "Technology is irrevocably changing the

practice of law” and that lawyer has a responsibility to understand technology to serve their clients.

Stemming from these conclusions, in 2012, the ABA adopted Comment 8 to Model rule 1.1 which sets out the core competency duties of a lawyer:

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.

Several things to note about Comment 8 to the Model Rules: First, it says a lawyer should-not must—understand the benefits and risks of technology. In January 2015, however, West Virginia adopted the Model Comment but changed it in a significant way:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer **must** 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.

Second, the Comment suggests that a lawyer understand the benefits and risks of technology-not that he or she understands how to code or create technology. Third, it contemplates a lawyer should understand the benefits and risks of relevant technology. It does not contemplate a lawyer know about all technology. It does not contemplate a lawyer be familiar with technology that he or she does not use in their practice. But the Comment does contemplate lawyers should know about the technology that’s relevant to their practice and their clients’ needs. So far 38 states have adopted Comment 8, the latest being Texas in February 2019.

There is, of course, an argument that Model Comment 8 really doesn’t change anything at all and that the obligation to be proficient in tech is already covered by the general statement about competency in Rule 1. And perhaps that’s so. But by providing this overlay of the importance of technology, it empathizes the duty and incentivizes state bar associations to endorse and provide CLE credit for technology-related programs. Again, in West Virginia, there is no issue: the West Virginia Comment requires being cognizant of the benefits and risks of relevant technology.

Other states that have not formally adopted Comment 8 have similar requirements. In New Hampshire, for example, a lawyer is required to keep abreast of tech changes. Delaware specifically recognizes the virtual impossibility of competently practicing without a basic technological understanding. Connecticut and Washington DC have ethical requirements that mirror Comment 8.

Florida adopted Comment 8 almost verbatim but then in late 2016 added a requirement that lawyers get at least 3 credit continuing legal education hours every 3 years on technology-related topics. North Carolina now requires its lawyers to get 1 hour of technology-related training each year.

In 2015, the California Bar Association came out with Formal Opinion 2015-193. While this opinion primarily deals with eDiscovery issues it does offer up some concepts relating to tech competency required of lawyers in general and will probably be recognized more and more by other states.

First, the Opinion favorably cites comment 8 and recognizes the truism that almost every case today involves e-discovery issues or could, which in and of itself requires some level of technological proficiency especially for litigators.

Secondly, the California bar recognizes that "a lack of technical knowledge in handling eDiscovery may render an attorney ethically incompetent... (even where the attorney may otherwise be highly experienced". And while the opinion recognizes that even though the lead lawyer may not have the requisite understanding and can farm out responsibility for e-discovery to another lawyer or a third-party provider, that lead lawyer still has overall supervisory responsibility, again contemplating some level of technological competency.

The opinion also states that failure to be technology competent may risk violation of a lawyer's duty to keep client information confidential. This duty is discussed below

The opinion also states that failure to be technical competent may risk violation of a lawyer's duty to keep client information confidential. This duty is discussed below.

2.2 Confidentiality (Rule 1.6)

Rule 1.6 provides “a lawyer shall not reveal information relating to the representation of a client” and “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

The latest discussion of this Rule by the ABA with respect to technology is contained in Opinion 477 which came out in May 2017. This Opinion deals with cybersecurity and ethical obligations with respect to emails among other things but also contains a good primer on the overall confidentiality rule as well.

A little background: the use of emails was covered previously by ABA Opinion 99-413 which provided that a lawyer generally may ethically use email to communicate with clients without violating ethical Rules as long as he or she takes “reasonable efforts to prevent inadvertent or unauthorized access” This was based on the idea that lawyers we have a reasonable expectation of privacy in communications made by all forms of e-mail, including unencrypted e-mail. Opinion 99-413 came out in 1999.

In Opinion 477, the ABA recognized that the ever-changing technological world required some additional reflections when it comes to the confidentiality duty to clients and that some new rules were in order. The ABA noted that there are no “hard and fast rules” with respect to confidentiality in this ever-changing world and whether lawyers are ethically protecting client confidences depends on several factors.

The Opinion recognizes that different types of electronic communications may need different levels of confidentiality protection. Among the non-exclusive factors for a lawyer to consider in deciding what level of protection to use are:

- 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 those safeguards, and
- The extent to which the safeguards adversely affect the lawyer’s ability to represent clients.

The ABA thus recognizes that there may be situations where the communications are sensitive and require additional electronic protection beyond what would normally be used.

The ABA further notes that a lawyer has some duty to understand the nature of the threat to confidentiality and whether the client’s matter and materials

are subject to a higher risk for a cyber intrusion. And the Opinion also provides that it is important to have a discussion at the beginning of the client/lawyer relationship about what levels of security will be necessary given the threat.

Without having some knowledge of technology and its risks and benefits, it would be difficult to satisfy the duties described in Opinion 477 and have the required discussions contemplated.

The Opinion also addresses cloud computing: once again, the opinion says the duties of the lawyer here depend. But the ABA suggests several non-exclusive factors for a lawyer to consider in deciding whether to use and how to select a cloud service in order to ensure the confidentiality duty is not breached. These include a duty to investigate the qualification, competence, and diligence of the provider, including its reputation and longevity. The duty also may require an examination of the contractual protections being offered, the ownership of the data, the obligation to return the information, the emergency procedures in place, and how the provider will respond to subpoenas.

Finally, the Opinion also addresses the outsourcing of work and provides several suggestions here as well for a lawyer to meet his or her duties of due diligence to ensure confidences are protected. These include such things as getting reference checks and reviewing vendor credentials, looking at the vendor's security policies and hiring protocols and making sure the confidentiality agreements are adequate.

2.3 Supervision (Rules 5.1 and 5.3)

Rule 5.1 provides "A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct."

Similarly, Rule 5.3 provides a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer".

The parameters of these Rules in connection with technology were also addressed in Opinion 477 referenced above. According to the Opinion, when retaining or directing a nonlawyer, lawyers should communicate appropriate directions so as to provide reasonable assurance that the nonlawyer's conduct is consistent with the professional responsibilities. And the lawyer has the responsibility to monitor how those services are being performed

Again, some technological competence is required to satisfy these duties: how can the duty be satisfied without some knowledge about what you are supervising?

2.4 Ethical Billing (Rule 1.5)

Finally, Rule 1.5 provides "A lawyer shall not make an agreement for, charge, or collect an unreasonable fee or an unreasonable amount for expenses. This in turn strongly implies that a lawyer work in a cost-effective manner. And while there are several factors in play here, to some extent lawyers are required to work in a way that's normally accepted and to use the tools normally expected to be used by a legal professional. Increasingly, the norm bends toward more efficient use of technology.

3.0 Practical Reasons for Technologic Competence

In addition to the ethical reasons to be technologically proficient, there are also some 6 very sound practical reasons lawyers should be familiar with and welcome technology and, as expressed in Comment 8, know of its benefits and risks.

3.1 Everyone Uses Technology

First, no matter the nature of a lawyer's practice or the size of his or her firm, clients, adversaries, judges and juries are constantly using technology every day in many ways. They demand and expect it.

According to the Kleiner Perkins 2017 Internet Trends Study, the time spent online and with digital media has been steadily increasing; in less than 10 years it has increased from 2.7 hours per day to 5.6 hours PER DAY. Virtually everyone communicates, interacts and learns online and with digital media. The expectation is instant access and immediate results and the use of technological bells and whistles in connection with almost anything being presented.

Clients are expecting and demanding that their lawyers use available technology to do more for less. To use data and data analytics to better

predict what the fees and outcomes will likely be. The only way to keep up with these demands is to be knowledgeable and aware of what technology is available and what this predictive technology will and will not do.

For trial lawyers, this also means being familiar with state-of-the-art trial presentation technology. The lawyers who aren't will be at a tremendous disadvantage to those that know how to leverage technology in the courtroom or even in the discovery process. And the expectations of those on juries, judges and those who you communicate with and are trying to persuade are that lawyers will use technological tools to tell their story.

3.2 Security

The second practical reason lawyers should know something about technology is security. More and more law firms are themselves targets of hacks and data breaches. The Panama Papers scandal. The cyber-attack on DLA Piper that almost shut the firm entirely down. The Cravath attack that led to serious insider trading problems.

According to the 2016 ABA TechReport, the primary targets of cyber-attacks seem to be the mid-size and large law firms although no firm is immune. But despite these statistics, some 21% overall of the firms surveyed in the 2016 ABA Tech Survey reported they had no security and 7% of the survey respondents simply didn't know.

Clients are demanding more and more that their lawyers keep their digital information secure. 31% of all lawyers in responding to the 2016 ABA Tech Survey said their clients have imposed security requirements on them. And when you look at larger firms the percent goes up to about 63%. These numbers will only grow: more and more clients expect their lawyers to know how to adequately protect their secrets. Again, lawyers need to be knowledgeable enough to have some basic understanding and awareness of how to keep digital information secure.

3.3 Leveling the Playing Field

Technology can level the playing field between large firms and small firms and solos. Tech tools can enable a single lawyer to do things it used to take an army of associates and paralegals to do. In addition, being at least

somewhat familiar with and aware of technology prevents legal professionals from being at the mercy of vendors. For trial lawyers, being knowledgeable about trial lawyers enhances the ability to tell a persuasive story in ways tech vendors cannot.

3.4 Death by a Thousand Cuts

The fourth reason to be technologically aware is to help prevent financial death by a thousand cuts and eliminate time-consuming non-billable tasks or non-collectible time.

According to a 2016 Clio Legal Trends Report, what lawyers-particularly lawyers in smaller firms--actually bill is roughly 81% of what could be billed and what is collected is about 86% of what is billed. Simply put, lawyers typically collect only 1.6 hours for 8 plus hours of work. Firm and billing technology can reduce the non-billable time and increase utilization, realization and collections rates.

Better using technology can help also help lawyers get back to practicing law and doing what they were trained to do instead of doing other tasks. And be more profitable.

3.5 Lack of A2J Threatens Us All

There is an embarrassing access to justice problem and the legal profession has some responsibility to both its profession and to the public that has extended to lawyers special self-regulating protections to try to something about it.

80% of people below the poverty line and more than 1/2 of those in the middle class—the people who need legal help the most--can not get access to even modest legal advice on serious issues like custody, divorce, and criminal questions. Small businesses and startups often ignore lawyers altogether and try to do things without a lawyer.

According to a recent survey, when asked why they didn't consult a lawyer on a serious legal matter, almost half of the respondents said they believe there was no need. Almost a quarter said it would make no difference. Sandefur, Rebecca, Accessing Justice in the Contemporary USA, the

University of Illinois at Urbana-Champaign: American Bar Foundation,
August 8, 2014.

Technology can help overcome this gap by making the practice of law more efficient and access more affordable. Being knowledgeable about technology allows the profession to use tools to be more efficient and more affordable to the underserved population.

3.6 The Winds of Change

The winds of change in the legal profession primarily driven by technology, are stronger than ever. Alternative service providers like RocketLawyer and LegalZoom are using technology to do things that lawyers once did. Last year it was estimated these and similar alternative legal service providers were an \$8.4 billion industry. More and more you find people using web sites not just to get documents like wills, contracts and articles of incorporation done but to also find and evaluate lawyers. To compete and continues to thrive, lawyers must be cognizant of these providers and how they are using technology.

Artificial intelligence (AI) technology is also threatening to alter the legal landscape, particularly for young lawyers. AI is taking over functions lawyers or paralegals used to perform. Clients and insurers are using AI and data analytics technology in new ways to evaluate lawyers, what they do and even how good they are.

All these things and more present new and different challenges and threats to the legal profession. To pretend they don't exist, ignore them and remain unfamiliar with them, their impact, and what technology can do creates a greater risk of becoming more and more irrelevant.

4.0 There You Have It

Don't be a Luddite. Don't brag about being technologically incompetent. Resolve to at least become more aware of technology and how it can help (or harm) you and your clients. The risk of not doing so could be catastrophic

Mike Mellace has been the Information Technology Directory at the West Virginia State Bar since 2012. He has a Bachelor's Degree from Marshall University in Management Information Systems and a Master's Degree from Marshall University in Technology Management. Mike has worked over the past 15 years in Education, Marketing and Legal organizations. As the IT Director, he has played a critical role in upgrading websites, databases, phone systems, and hardware internally at the State Bar Center.