American Bar Association
Section of Labor and Employment Law
Employee Benefits Committee

2018 Midwinter Meeting
February 9, 2018
Clearwater Beach, Florida

Ethics in a Digital World: What Should an Ethical Lawyer Know about Technology?

J.S. "Chris" Christie, Jr. ©
Christie for Alabama Attorney General
PO Box 59141
Birmingham, AL 35259
(205) 914-8570
Chris@Christie4AlabamaAG.com

J.S. "Chris" Christie, Jr., is a Birmingham, Alabama, lawyer who left his partnership at Bradley Arant Boult Cummings LLP as of January 1, 2018, to be a 2018 candidate for Alabama Attorney General. The American College of Employee Benefits Counsel selected him as a Fellow, *The Best Lawyers in America* has listed him since 2005, and *Super Lawyers* named him a Top 50 Attorney in Alabama. He graduated from Rhodes College with a B.A. and from Duke University with an M.A. and a J.D. He served as a Peace Corps Volunteer, teaching at the University of Yaoundé School of Law.

The above paper is an update of the article published in 46(2) *The Brief* 40 (2017). Parts of this paper were published as *Ethics and Technology*, 75(1) Ala. Law. 31 (2014).

What Should an Ethical Lawyer Know about Technology?

by

J.S. "Chris" Christie, Jr.

Most states recently updated their ethical rules to emphasize a lawyer's duties to keep up with technology. In light of these updated rules and ever changing technology, what should an ethical lawyer know about technology?

I. Ethical Rules on Technology and Confidentiality

In light of new technology and evolving security concerns, and to guide lawyers regarding the use of technology, the ABA Model Rules of Professional Conduct were amended in August 2012.[1] These "Technology Amendments" changed Model Rules 1.6 (Confidentiality of Information) and 1.1 (Competence).

Generally, state ethical rules govern lawyer conduct, not the ABA Model Rules. Nonetheless, all states except California have adopted a version of the ABA Model Rules, with thirty-five states as of August 8, 2017, having adopted all or most of the 2012 Technology Amendments and another seven states reporting they are "studying" the amendments.[2] Even in a state that has not adopted these Technology Amendments, ethics and technology issues concern every lawyer practicing today. And lawyers' not adequately addressing technology might find themselves embarrassed, if not worse.

On May 11, 2017, as revised May 22, 2017, the ABA Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 477R.[3] This new opinion discusses advances in technology and cybersecurity threats, providing additional guidance as to when lawyers should consider enhanced security measures.[4]

As to Model Rule 1.6, the 2012 Technology Amendments add a new paragraph and change two Comments. The prior Comments already described a lawyer's ethical duty to take reasonable measures to protect a client's confidential information from inadvertent or unauthorized disclosures, as well as from unauthorized access. In light of the pervasive use of technology to store and send confidential client information, this pre-existing obligation is now stated explicitly in the black letter of Model Rule 1.6. The

---

[1] For background on these ABA Model Rules amendments, see the reports of the ABA Commission on Ethics 20/20, filed May 6, 2012 for the ABA Annual Meeting in August 2012. http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.

[2] As of December 30, 2017, the August 8, 2017 chart can be found at http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/state_implementation_selected_e20_20_rules.authcheckdam.pdf.

[3] https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf.

[4] *See* P. Geraghty, "ABA Formal Opinion 477R: Securing communication of protected client information," (June 2017) https://www.americanbar.org/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli.html.

Comments were also amended to offer lawyers more guidance about how to comply with this obligation.

The amended Model Rule 1.6 has the following new paragraph (c): "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."

Model Rule 1.6, Comment [16], was rewritten to include factors to be considered in determining the reasonableness of a lawyer's efforts to prevent disclosure or access. As examples, a lawyer should make reasonable efforts to prevent disclosures or access, such as avoiding a lawyer's sending an email to the wrong person, someone's "hacking" into a law firm's network, or staff's posting client information on the internet. As Comment [16] makes clear, not every disclosure is a violation, but reasonable precautions are required.

Model Rule 1.6, Comment [17], has the following new language: "Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these rules." In other words, lawyers should also consider duties arising under HIPAA,[5] Graham-Leach-Bliley ("GLB"),[6] and other laws intended to protect data privacy.

As to Rule 1.1, the Commission concluded that competent lawyers should be aware of basic features of technology. To emphasize this point, the Rule 1.1 amendments add language to two Comments.

Comment [6] of Model Rule 1.1 was amended to add that, "to stay abreast of changes in the law and its practice, lawyers need to have a basic understanding of the benefits and risks of relevant technology."

Comment [8] of Model Rule 1.1 was amended to add the phrase beginning with *including*: "a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology*** (emphasis added)." Without the amendment, a lawyer already had a duty to keep up with technology; the amendment emphasizes that duty.[7]

---

[5] The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, and HIPAA's implementing regulations, 45 C.F.R. §§ 160-64, regulate the collection, use and disclosure of medical information by healthcare providers and their Business Associates (entities that do business with healthcare providers; *i.e.*, lawyers with doctors as clients).

[6] The Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act), 15 U.S.C. §§ 6801-6827, regulates the collection, use and disclosure of non-public financial information by financial institutions and entities that receive non-public financial information from financial institutions (*i.e.*, lawyers with banks as clients).

[7] *See e.g.*, ABA Formal Op. 466, Lawyer Reviewing Jurors' Internet Presence at 2 n. 3 (Apr. 24, 2014) (as to whether a lawyer should research a juror's internet presence, saying "we are mindful of the recent addition of Comment [8] to Model Rule 1.1."); Florida Ethics Op. 10-2 (Sept. 24, 2010) ("If a lawyer chooses to use these Devices that contain Storage Media, the lawyer has a duty to keep abreast of changes in technology to the extent that the lawyer can identify potential threats to maintaining confidentiality.").

II. What Risk-Reducing Steps Should a Lawyer Take?

While common sense, the steps a lawyer ethically should take to reduce risks from technology depends on the circumstances. As Comment [16] to new Model Rule 1.6(c) explains, a lawyer is not responsible for data breaches "if the lawyer has made reasonable efforts to prevent the access or disclosure." What are the reasonable steps a lawyer should take? Comment [16] indicates as follows:

> 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).

In other words, the Model Rules Comment recognizes that what technology safeguards a lawyer should adopt depends on many factors and requires judgment.

The U.S. Post Office, Federal Express, and UPS all could lose or mis-deliver a lawyer's package with confidential client information. Instead of sending a package by mail, a lawyer might pay a paralegal to hand-deliver the package to reduce the risk. Almost all lawyers would probably agree that such effort is rarely, if ever, required. On the other hand, a lawyer would want to make sure the mailed package was properly sealed, was correctly addressed, and did not have see-through packaging. Which technology safeguards are comparable to ensuring a package is sealed properly and which are comparable to hand-delivery by a paralegal? The following suggestions intend to give insights to guide a lawyer's judgment when deciding what steps are reasonable.

III. Ethics and Technology: Practical Considerations for Lawyers

In light of the Model Rules 2012 technology amendments, what are technology risks in 2017 for lawyers? In addition to computer system security, every lawyer should consider avoiding scams, password fundamentals, and mobile security.[8]

[8] The focus here is on legal ethics and the security of confidential information, without attempting to cover all legal ethics issues arising from new technology. For example, legal ethics and social media is not discussed. Many state advisory ethics opinions address legal ethics and social media, with the ABA Legal Technology Resource Center ("LTRC") gathering resources: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/social_media.html. Another topic not discussed here is legal ethics and metadata. http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html. The LTRC has help for a lawyer on many topics: http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis.html.

A. Lawyers and Computer System Security

A hacker can gain computer access by taking advantage of computer systems' vulnerabilities. When identifying parts of a computer system to safeguard, a lawyer should consider not only servers, desktops, and laptops, but also tablets, smart phones, copiers, scanners, and any other device that can connect to a computer system. A lawyer should take reasonable steps to make computer systems more secure and to limit the vulnerabilities.

A lawyer should make sure that his or her computer system has updated antivirus software and other security software, including a firewall. The specifics on programs as safeguards to protect entire computer systems may require a consultant. Unless one is the rare lawyer with the technical skills, finding someone with expertise to help is advisable.

A lawyer should consider regularly updating software and replacing software that is no longer being updated. For example, ten percent of the lawyers responding to the ABA's 2015 Legal Technology Survey Report responded that they still use Windows XP. Windows XP has not been updated or patched since April 2014.[9] Because Microsoft no longer supports Windows XP, it no longer has security updates. Windows XP still operates, but becomes more and more vulnerable to security risks and malware infections as time passes.

According to the ABA 2017 Legal Technology Survey Report, security breaches ranged from a high of 35% for firms with 10-49 attorneys to a low of 10% for solos. Yet, law firms report only an overall use of full drive encryption of only 21% (up from 15% last year), ranging from 15% for solos to 42% for firms of over 500 lawyers. File encryption protects individual files rather than all the data on a drive or device. Reported use of file encryption is higher than full disk but still only at 45% overall, ranging from 38% for solos to 65% in firms of over 500 lawyers.[10]

For all electronic data (*i.e.*, information), a lawyer should consider whether the data should be encrypted. Encryption is the process of encoding data so hackers cannot read it, but authorized parties can. Encryption turns words into scrambled gibberish. Many modern encryption programs use factoring and prime numbers. A prime number can only be divided by one and itself. Factoring is identifying the prime numbers multiplied together that result in a number. Encryption today can make it very difficult for computers to decipher encrypted data without the key.

A lawyer should consider what data might need to be encrypted. ABA Formal Op. 477R, p. 5, warns that "it is not always reasonable to rely on the use of unencrypted

[9] C. Reach, "Arsenic and Old Lace: Technology Competency," *Addendum* (Oct. 2016) https://www.alabar.org/assets/uploads/2016/10/Addendum-Oct-2016.pdf.
[10] D. Ries, "Security," ABA TechReport 2017 https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security.html.

email."[11] As discussed below, some email programs automatically encrypt data when sent.

Another issue is whether to encrypt data at rest. Such encryption complicates the user experience; encrypting all electronic information interferes with using the information efficiently. Data shipped or data otherwise taken out of the office creates additional risks. If data relating to the representation of a client is on a portable hard drive, a thumb drive, a mobile device, or attached to an email, whether it should be encrypted requires more thought and depends on a number of factors. Many free encryption tools are available.[12]

A lawyer should consider what steps to take when an employee leaves. When staff changes, unused user accounts should be terminated, passwords changed, and other steps considered.[13]

A lawyer should consider whether his or her safeguards are HIPAA and GLB compliant. Even if the lawyer does not represent healthcare providers or financial institutions, he or she is likely to have medical and financial information that raises the same or similar confidentiality issues. One might also argue that all confidential information, including attorney-client communications, should be protected with the same or similar safeguards.

A lawyer should consider regular automatic backups of computer systems. In anticipation of natural disasters, a lawyer should also consider having such backups in more than one location or at least remote geographically from the main computer systems.

Another issue is whether lawyers can use the cloud. First, this cloud has nothing to do with weather. Years ago, when engineers were diagramming computer networks, they did not know how to represent the internet, so they just drew a cloud. Today, "the cloud" means a computer accessible through the internet. If a lawyer is using the cloud, the lawyer stores data on a computer owned by a third party. Because cloud computing places client data on remote servers not in a lawyer's direct control, an issue is can lawyers use the cloud.

Twenty states have considered whether a lawyer can use cloud computing and they all advised yes, if reasonable care is used.[14] Often, using a cloud vendor is more secure than what a lawyer might be able to have on the lawyer's own computer systems.

---

[11] https://www.americanbar.org/publications/youraba/2017/june-2017/aba-formal-opinion-477r--securing-communication-of-protected-cli.html.

[12] http://www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/.

[13] M. McGee, Mitigating Threats Posed by Terminated Employees, Data Breach Today, (Dec. 1, 2017) https://www.databreachtoday.com/mitigating-threats-posed-by-terminated-employees-a-10503; "Insider Threats and Termination Procedures, U.S. Dept. HHS (Nov. 2017) https://www.hhs.gov/sites/default/files/november-cybersecurity-newsletter-11292017.pdf?language=es.

[14] http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html.

A cloud vendor is also likely to have better backup capability. If considering a cloud vendor, a lawyer might include asking or investigating the following questions:

- How does the vendor safeguard data?
- Are the vendor's safeguards HIPAA and GLB compliant?
- After data is deleted, can the vendor certify that it is destroyed?
- How often does the vendor backup data?
- Does the vendor backup data in multiple locations?
- How stable is the vendor as a business entity?
- Does accessing the lawyer's data require proprietary software?
- If the relationship ends, how is the data accessed and returned?
- What confidentiality provisions are in the vendor's standard contract?
- Will the vendor agree to other confidentiality provisions?

In summary, when choosing a cloud vendor, a lawyer should consider whether the data will be secure and backed-up and whether he or she will have any problems if and when his or her relationship with the vendor might end.

Examples of cloud storage and sharing services include Dropbox, ShareFile, Google Drive, Box, Microsoft OneDrive For Business, and Apple iCloud.[15] Dropbox is the most popular cloud file storage and sharing service, including many lawyers. Whether Dropbox, even Dropbox for Business, is secure enough for businesses has been questioned.[16] In 2016, Dropbox apparently responded to these concerns, publishing "Dropbox Business security: A Dropbox whitepaper."[17] For whatever reasons, Dropbox has been identified annually since 2013 as the app that companies ban more than any other app.[18]

A final computer system consideration might be what to do with computers when they are no longer being used. Lawyers should be careful when discarding computers, copiers, and any other devices storing data. A possible risk that might be missed is data on leased computers and copiers. Note that Affinity Health Plan, Inc., paid a fine of $1,215,780 for alleged HIPAA violations after it returned multiple copiers to a leasing agent without erasing data on the copiers' hard drives.[19]

---

[15] "Top 10 Alternatives to Dropbox: Popular File Sharing Software Solutions, https://financesonline.com/top-10-alternatives-dropbox-popular-file-sharing-software-solutions/; Dropbox Alternatives: 10 Best Cloud Storage Services," Mar. 1, 2016, http://beebom.com/best-dropbox-alternatives-for-cloud-storage/.

[16] M. Batters, "Security Comment: Why are people still using Dropbox for business?," http://www.legaltechnology.com/latest-news/security-comment-why-are-people-still-using-dropbox-for-business/.

[17] https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vflDw-Ksl.pdf.

[18] J. Bourne, "MobileIron security report: iOS increases dominance, Dropbox most banned consumer app," Aug. 2, 2016, http://www.appstechnews.com/news/2016/aug/02/mobileiron-security-report-ios-increases-dominance-dropbox-most-banned-consumer-app/.

[19] http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html.

B. Lawyers and Avoiding Scams

Avoiding scams sounds almost too obvious to include as something lawyers should consider. Nonetheless, when people say their computer has been hacked, they probably mean the hacker deceived someone into allowing direct access to the computer or into sharing a password. A lawyer should learn how to detect and to avoid such scams and should train his or her staff on how to detect and to avoid scams.

Because secure computer systems are difficult to access from outside, hackers often attempt to can gain access by deceiving someone. Generally, hackers use two deceptive methods: (1) sending phishing and spoofing emails, which urge the email recipient to respond; or (2) using malware that a recipient downloads with games or other apps or downloads by opening infected email attachments, infected thumb drives, or unsafe websites that infect a computer visiting it.

With a phishing email, the sender is fishing for information to use for whatever purposes the sender can imagine. Spoofing is creating a deceptive email that looks like it is sent by a legitimate business – for example, a bank. Many phishing emails spoof a specific business's emails, often with an email address that looks like the spoofed business's email address.

If a cursor is hovered over (do not click) an email sender's name, the sender's email address and its domain name is shown. For an email with links, if a cursor is hovered over (do not click) the link, the link's internet website address (Uniform Resource Locator or "URL") is shown. The domain name or the URL should match what one expects. A creative spoofing email might have names that are close to those being spoofed, but with slight differences; for example, "bradlley" with two ls, rather than "bradley" with one l. If an email's sender's domain names or link URLs make one suspicious, the email is probably a phishing email.

Malware is short for malicious software. It includes computer viruses, worms, trojan horses, ransomware, spyware, and other malicious programs.

An infamous malware example is the Melissa virus, which first appeared in 1999.[20] Emails with an attachment spread this computer virus. After a Melissa virus email recipient opens the attachment, the virus replicates itself by creating emails with the same attachment and sending them to the first 50 addresses in the recipient's Outlook address book. Unless contained, the Melissa virus can shut down email systems with the huge number of emails.

Today, probably the most serious malware risk is ransomware.[21] Ransomware stops one from normally using an infected computer and requires doing something before normal computer use returns. Usually, ransomware requires paying money (a "ransom")

---

[20] *See* J. Strickland, "10 Worst Computer Viruses of All Time," http://computer.howstuffworks.com/worst-computer-viruses1.htm.

[21] *See* Ransomware, Microsoft Malware Protection Center, https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx.

to the hacker. Ransomware can encrypt files making them unusable, can prevent access to Windows, or can stop certain apps from working.

In 2016, ransomware attacks in the United States averaged 4,000 per day, costing over $200,000,000 in the first three months of 2016.[22] For example, in February 2016, Hollywood Presbyterian Medical Center paid a $17,000 ransom in bitcoin to a hacker who seized control of the hospital's computer systems.[23] Other examples include the WannaCry ransomware that infected 300,000 computers in May 2017 and ransomware attack that forced DLA Piper to shut down its computers worldwide in June 2017.[24], A September 2016 article reported that two-thirds of ransomware infected companies in the United Kingdom pay ransomware demands, but not all got their data back.[25]

When considering safeguards to protect against malware, the types of computers at risk include servers, desktops, laptops, tablets, smart phones, and any other device that can download data or can access the internet. Lawyers should be able to reduce malware risks,[26] including ransomware risks, with the following steps:

- Do not open risky emails or email attachments
- Do not click on risky links in emails or websites
- Do not download games or non-work apps
- Do not open risky thumb drives or CDs
- Do not visit unsafe, suspicious or fake websites
- Block unsafe, suspicious or fake websites
- Install up-to-date antivirus and security software
- Update software, replacing if no longer updated
- Separate work and personal computer use[27]
- Backup important files in a remote, unconnected facility

In the first quarter of 2016, PhishMe reported that 93% of phishing emails were related to ransomware.[28] For emails, what are red flags indicating that an email is risky?

- Asks for login and password
- Purports to be from the IRS, a court, or other government entity

---

[22] https://www.cryptocoinsnews.com/fbi-now-says-dont-pay-bitcoin-ransomware-extortionists/.
[23] http://www.latimes.com/business/technology/.
[24] J. Tashea & V. Li, "Large Law Firms' Secret Information from Big-money Clients, Entices Cyberthieves," ABA Journal (January 2018) http://www.abajournal.com/magazine/article/large_law_firms_cybertheft_risk; DLA Piper, "WannaCry ransomware attack was just the tip of the iceberg," https://www.dlapiper.com/en/uk/insights/publications/2017/06/wannacry-ransomware-attack/.
[25] D. Palmer, "Two-thirds of companies pay ransomware demands: But not everyone gets their data back," http://www.zdnet.com/article/two-thirds-of-companies-pay-ransomware-demands-but-not-everyone-gets-their-data-back/.
[26] *See* https://www.microsoft.com/en-us/security/portal/mmpc/shared/prevention.aspx.
[27] If separate computers are not possible, at least have separate accounts (especially if a child is using it) on the same computer.
[28] http://phishme.com/q1-2016-sees-93-phishing-emails-contain-ransomware/.

- Purports to be from a financial institution or healthcare provider
- Requests personal information like account numbers
- Has suspicious or misspelled sender email address or domain
- Has links with suspicious URL addresses
- Requests clicking on unfamiliar links
- Has generic, unusual or incorrect name in greeting
- Makes an urgent request with a short deadline like 24 hours
- Requests to download a file, especially an .exe file

The red flag of an email's asking for login and password should be the most obvious one. Providing another with one's login and password information is always very risky, but replying to an email with that information is bad – but people must do it, because phishing emails keep asking for that information.

Most of the above red flags can apply to considering whether a link, website or social media post is risky. Common sense can help, too.

Some email scams are even more sophisticated. "Social engineering" refers to psychologically manipulating people into performing actions or disclosing confidential information.[29] Victims are often motivated by wanting to help. In this context, social engineering might entail the hacker learning enough about a law firm to pose as the managing partner and send a "spear phishing" email to the firm's controller. Avoiding sophisticated scams may require slowing down, research, and common sense before action.

A lawyer should consider having a technology risks training program for all who have access, through the lawyer's computer systems, to the internet or to emails. While a cliché, a chain is only as strong as its weakest link. A hacker usually has as much access to a lawyer's computer system through a staff member's responding to a phishing email as when a lawyer does so. An important safeguard can be staff training and checking to see if staff is complying with what they have been trained to do.

Another email safeguard is to have a warning, such as "External Email," added as the top line of the message for every email received from an outside sender. The warning should highlight internally any attempt at spoofing the lawyer's own emails, as well as remind the lawyer and his or her staff to be careful.

Once a ransomware or other computer infection is detected, a lawyer should, like any other business, quickly assess what happened, determine what is affected, and contain and limit the damage. A lawyer also should consider communications to clients, courts, and the public.

[29] "What is Social Engineering?" https://www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering.

As part of "How do I remove ransomware from my PC," Microsoft offers suggestions for removing some ransomware.[30] The FBI has a publication with suggestions.[31] If backup data is available, that can provide another alternative after being infected. The FBI used to advise paying the ransom if no other alternatives were available, but as of April 29, 2016, changed its position, and now says do not pay bitcoin ransom to extortionists.[32]

As to avoiding scams such as phishing emails and malware, a lawyer should decide what steps as technology safeguards are reasonable. Then, the lawyer must not only follow the steps consistently, but also must train his or her staff and make sure they follow the steps too.

C. Lawyers and Password Fundamentals

Every lawyer should consider password fundamentals for client information that is confidential. Good passwords are a simple safeguard to protect client information.

A lawyer's strong passwords can sometimes interfere with the lawyer's efficiently using a computer. A password needs to be remembered, but easy passwords can create risks. Hiding a password under the telephone may not be as bad as putting it on a post-it note on the computer screen, but an unauthorized person wanting to access a computer might look around for passwords written down. Moreover, using the same password for every purpose or not changing passwords periodically can increase risk.

In addition, some sites have password prompt questions such as "What is your mother's maiden name?" If security matters, using a prompt that a hacker can research and discover creates a risk.

What are bad (weak) passwords? In 2017, SplashData released its annual most used and thus worst passwords list. Topping the list was "123456," with "password" as runner-up, followed by the slightly more inventive "12345678."[33] Any password that a hacker could guess is a bad password.

Good (strong) passwords include uppercase and lowercase letters, numbers, symbols, and spaces. For many purposes, an eight-digit password with some combination of several types of these characters should be plenty strong.

An easy way to remember good passwords is to borrow from leetspeak (or l33tspeak). With l33tspeak, one replaces letters with other characters. For example, password can become P@55w0rD. The longer a password is, the harder it is to crack. Not only are passwords with characters that are not letters and numbers difficult to guess, but

---

[30] https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx#faq.
[31] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.
[32] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise; https://www.cryptocoinsnews.com/fbi-now-says-dont-pay-bitcoin-ransomware-extortionists/.
[33] For 2017's worst passwords, see https://13639-presscdn-0-80-pagely.netdna-ssl.com/wp-content/uploads/2017/12/Top-100-Worst-Passwords-of-2017a.pdf.

programs that try every possible password (brute-force attacks) have great difficulty breaking long passwords using these types of characters.

Even stronger passwords combine l33tspeak with phrases ("passphrases"). More than 15 characters can currently make a passphrase too difficult to crack for almost any hacker. For example, M0unt@in M@n 4321 5treet is not impossible to remember, but would be much harder to hack than any eight-character password.

Applications called password managers are available. One service is called LastPass. It helps generate secure passwords and helps the user remember them. Using this type of tool, however, is difficult to manage for a law firm network and might create a risk of a hacker's breaking into the service and then having all of the lawyer's passwords.

Like other safeguards, good passwords are for all who access the lawyer's computer systems. A lawyer should require staff to have good password fundamentals, train staff on those password fundamentals, and find ways to ensure staff compliance with good password fundamentals.

D. Lawyers and Mobile Security

Mobile security might be the security risk many lawyers should consider more. Among the risks are losing computers that are mobile devices (laptops, tablets, smart phones) and Wi-Fi interception. Among the risk-reducers might be passwords, remote wiping, encryption, two-factor identification, inactivity timeouts, authorization before downloading applications, and automatic wiping if access is attempted incorrectly a certain number of times.

1. Mobile Device Security for Lawyers

An overwhelming trend in mobile devices is BYOD or Bring Your Own Device. Years ago, many law firms only allowed firm approved and owned mobile devices (usually BlackBerry smartphones). With advances in smartphones and tablets, BYOD has become the accepted norm; iPhones and Android have been the predominant smartphone platforms for several years now. Even new BlackBerry models have similar security issues as iPhones and Androids. Nonetheless, a September 2013 article in the *ABA Journal* called BYOD "a nightmare" from a security perspective and quoted a security firm executive as follows: "We strongly believe that lawyers should connect to law firm networks only with devices owned and issued by the law firms."[34]

[34] J. Dysart, "New hacker technology threatens lawyers' mobile devices," Sept. 1, 2013, http://www.abajournal.com/magazine/article/new_hacker_technology_threatens_lawyers_mobile_devices. Since 2013, employers have generally adapted to BYOD. "BYOD Policies: What Employers Need to Know," https://www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx; M. Dhingra, "Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)," http://www.sciencedirect.com/science/article/pii/S1877050916000326.

The initial concern is easy to understand. Imagine a lawyer's leaving a smartphone at a bar. What client information is on the smartphone in email, email attachments, or accessed documents? What access to the firm email system or other systems can a hacker find through the smartphone? How long before the law firm learns that its drinking lawyer lost his smartphone?

For any mobile device that has information relating to the representation of a client, a lawyer should at least consider having a PIN and should consider having a stronger password. For smartphones with a swipe pattern as the password, a lawyer might consider changing the password periodically to avoid a wear pattern on the screen. A lawyer might also consider remote wiping and other risk-reducing steps.

For any mobile device that has information relating to the representation of a client, a lawyer should consider having all possibly confidential data encrypted. Laptops, tablets and smartphones can be stolen, regardless of how careful a lawyer tries to be.

For heightened mobile device security, a lawyer might consider two-factor identification to access a lawyer's email or other systems. Two-factor identification can require a password and other information, a password and a telephone call to a specific number, or a password and any other factor that can be used to identify the user. On the other hand, plowing through current two-factor identification can seem like a barrier to using technology.

Lawyers might consider Mobile Device Management (MDM) software, which can secure, monitor, and support all connected mobile devices.[35] Through a remote MDM console, using commands sent over the air, an administrator can update any mobile device or group of mobile devices. MDM can separate email and associated content away from applications; can distribute applications, data, and configurations; and can even be used to deploy securely new applications from a law firm's "app store." MDM can also remote-wipe the mobile device.

For a mobile device used for work, a lawyer should consider what software (applications) are downloaded, since some might compromise the device. If a child plays with a work mobile device, a lawyer should consider the risks of the child's deleting documents, sending documents to the wrong people, or downloading malware.

For simpler mobile device security, instead of (or in addition to) the above considerations, a lawyer might manage risks by not having or limiting the confidential information on the device. A mobile device that only has confidential client information in encrypted email attachments does not pose the same risks as a mobile device with thousands of emails with confidential client information in the text of the emails.

2. Wi-Fi Interception and Security for Lawyers

If a lawyer uses Wi-Fi, especially in a café or hotel hot spot, a hacker could theoretically intercept what is sent, sometimes called "packet sniffing." Packet sniffing

[35] To view Citrix's MDM video, see https://www.youtube.com/watch?v=oUYYZdSXQTQ.

captures packets of information sent through the air between the device and the hot spot. These packets can be passwords, emails, or whatever is sent. Software to packet-sniff (a packet analyzer) is readily available. Wireshark sells a number of packet capture devices.[36]

Packets can be sent as "clear text" (unencrypted), which means anyone can read them as plain English, or packets can be sent on an encrypted connection, which means even though people can intercept them, they cannot read them. If a lawyer uses Microsoft Exchange and has encrypted connections, the lawyer should not have an unencrypted email interception problem, because the emails are encrypted during transmission.

If a lawyer uses a general webmail service like normal Gmail, the lawyer might be sending clear text and have an avoidable risk.[37] On the other hand, a lawyer can have a Gmail account that is secure. In the website address header (the URL for uniform resource locator), look for an S after the HTTP. In other words, "HTTPS:" in the URL indicates that the site uses encryption.

When using Wi-Fi, an alternative to using an encrypted email system might be to use a VPN connection to a firm network. A VPN connection provides a secure tunnel that funnels web activity, encrypted, through the secure connection. This connection is a secure way to work on Wi-Fi. A lawyer's email system can require a VPN connection to connect to email.

Perhaps in the future, the advances in quantum computing will make today's encryption look easy to break. In the not-so-distant future, perhaps a new mode of security is likely to be needed. Until then, a lawyer should consider email encryption as part of today's reasonable safeguards to protect the lawyer's mobile devices.

IV. Conclusion

As the Model Rules' 2012 Technology Amendments and the ABA's 2017 Formal Opinion 477R emphasize, an ethical lawyer should have reasonable technological competence. A lawyer should use good judgment, taking reasonable steps to reduce technology risks and to safeguard information. And a lawyer should not only consistently safeguard confidential data, but should also train his or her staff to do the same.

[36] https://www.wireshark.org/.

[37] For a general discussion of lawyers' communicating confidential information by email and risks lawyers should consider, see Texas State Bar Op. No. 648 (2015), http://www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx.