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?

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] The amendments changed Model Rules 1.1 (competence) and 1.6 (confidentiality of information).

Generally, state ethical rules, not the ABA Model Rules, govern lawyer conduct. Nonetheless, all states except California have adopted a version of the ABA Model Rules, with 31 states as of December 1, 2016, having adopted the 2012 Model Rules technology amendments and another 11 states reporting they are "studying" the amendments.2 Even for lawyers in a state that has not adopted these amendments, ethics and technology issues concern every lawyer practicing today. And lawyers not adequately addressing technology might find themselves embarrassed, if not worse.

As to Model Rule 1.1, by adding the following phrase beginning with "including" to its comment [8], the 2012 technology amendments stress that competent lawyers should be aware of basic features of technology: "a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*." Without the amendment to comment [8], a lawyer already had a duty to keep up with technology; the amendment emphasizes that duty.[3]

As to Model Rule 1.6, the 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 preexisting obligation is now stated explicitly in the black letter of Model Rule 1.6. The comments were also amended to offer lawyers more guidance about how to comply with this obligation.

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." As examples, a lawyer should make reasonable efforts to avoid sending a letter or an e-mail to the wrong person, posting confidential client information on social media, or allowing the law firm's computer network to be "hacked."

Comment [16] to Model Rule 1.6, now comment [18], was rewritten to add a list of possible factors to be considered in determining the reasonableness of a lawyer's efforts to prevent disclosure or access: "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)." To comply with Model Rule 1.6(c), instead of risking misdelivery by sending a package by mail, a lawyer might pay a paralegal to hand deliver the package. But 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?

Comment [17] to Model Rule 1.6, now comment [19], 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,[4] Gramm-Leach-Bliley (GLB),[5] and other laws intended to protect data privacy.

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.[6]

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, smartphones, 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.

PHOTO: ISTOCK

TIP

As a lawyer using technology, your ethical duties require competence; use good judgment to reduce risks and safeguard information.

A lawyer should consider regularly updating software and replacing software that is no longer being updated. For example, 10 percent of the lawyers responding to the ABA's 2015 Legal Technology Survey responded that they still use Windows XP.[7] Windows XP has not been updated or patched since April 2014.[8] 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 an *ABA Legal Technology Survey Report* published in September 2014, viruses, spyware, or malware infected nearly half of law firms' computer systems in 2013. Yet, only one-fourth of law firms had any kind of encryption available for their lawyers to use.[9]

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. As discussed below, some e-mail 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 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 e-mail, whether it should be encrypted requires more thought and depends on a number of factors. Many free encryption tools are available.[10]

A lawyer should consider whether his or her safeguards are HIPAA and GLB compliant. Even if the lawyer does not represent health care 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.

A lawyer should consider the risks a vendor (third-party service provider) presents to data security. "Vendors are consistently cited as a primary cause of data breaches."[11] Just like other businesses, a lawyer should exercise reasonable due diligence selecting vendors, have contracts with vendors requiring them to safeguard data, and monitor vendors to confirm that they are complying.

Another issue involves the cloud, which 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 whether lawyers can use the cloud.

Twenty states have considered the issue and advised that lawyers can use cloud computing, if they exercise reasonable care.[12] Often, using a cloud vendor is more secure than what a lawyer might be able to have on the lawyer's own computer systems. A cloud vendor is also likely to have better backup capability. If considering a cloud vendor, a lawyer might ask or investigate the following questions:

Viruses, spyware, or malware infected nearly half of law firms' computer systems in 2013.

J.S. "Chris" Christie Jr. *is a Birmingham, Alabama, partner of Bradley Arant Boult Cummings LLP, where he serves as chair of its Insurance Practice Group and cochair of its Pro Bono Committee. He may be reached at jchristie@bradley.com. Parts of this article were published as "Ethics and Technology," 75* Ala. Law. *31 (2014).*

- 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 back up data?
- Does the vendor back up 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 the lawyer 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, Google Drive, Box, and Microsoft OneDrive for Business.[13] Dropbox is the most popular cloud file storage and sharing service, with more than 300 million users, including many lawyers. Whether Dropbox, even Dropbox for Business, is secure enough for businesses has been questioned.[14] In 2016, Dropbox apparently responded to these concerns, publishing "Dropbox Business Security: A Dropbox Whitepaper."[15] For whatever reasons, Dropbox has been identified annually since 2013 as the app that companies ban more than any other app.[16]

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.[17]

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 gain access by deceiving someone. Generally, hackers use two deceptive methods: (1) sending phishing and spoofing e-mails, which urge the e-mail recipient to respond; or (2) using malware that a recipient downloads with games or other apps or by opening infected e-mail attachments, infected thumb drives, or unsafe websites that infect a computer visiting it.

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

If a cursor is hovered over (do not click) an e-mail sender's name, the sender's e-mail address and its domain name is shown. For an e-mail with links, if a cursor is

PHOTO: ISTOCK

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 e-mail might have names that are close to those being spoofed, but with slight differences; for example, "bradllley" with two *l*s, rather than "bradley" with one *l*. If an e-mail's sender's domain names or link URLs make one suspicious, the e-mail is probably a phishing e-mail.

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.[18] E-mails with an attachment spread this computer virus. After a Melissa virus e-mail recipient opens the attachment, the virus replicates itself by creating e-mails 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 e-mail systems with the huge number of e-mails.

Today, probably the most serious malware risk is ransomware.[19] 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") to the hacker.[20] Ransomware can encrypt files making them unusable, prevent access to Windows, or stop certain apps from working.

In 2016, ransomware attacks in the United States averaged 4,000 per day, costing over $200 million in the first three months of 2016.[21] 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.[22] A September 2016 article reported that two-thirds of ransomware-infected companies in the United Kingdom pay ransomware demands, but not all get their data back.[23]

When considering safeguards to protect against malware, the types of computers at risk include servers, desktops, laptops, tablets, smartphones, and any other device that can download data or access the Internet. Lawyers should be able to reduce malware risks,[24] including ransomware risks, with the following steps:

- Do not open risky e-mails or e-mail attachments;
- Do not click on risky links in e-mails or websites;
- Do not download games or nonwork 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;[25] and
- Backup important files in a remote, unconnected facility.

Lawyers have recently been targets of scams, including one based on phishing e-mails with a link to view a business complaint that opens a website that installs ransomware.[26] In the first quarter of 2016, PhishMe reported that 93 percent of phishing e-mails were related to ransomware.[27] What are red flags indicating that an e-mail is risky?

- Asks for login and password;
- Purports to be from the IRS, a court, or other government entity;
- Purports to be from a financial institution or health care provider;
- Requests personal information like account numbers;
- Has suspicious or misspelled sender e-mail 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; or
- Requests to download a file, especially an .exe file.

The red flag of an e-mail's asking for login and password information should be the most obvious one. Providing another with one's login and password is always very risky, but replying to an e-mail with that information is bad—but people must do it, because phishing e-mails 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 e-mail scams are even more sophisticated. "Social engineering" refers to psychologically manipulating people into performing actions or disclosing confidential information.[28] 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" e-mail 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 e-mails. 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 e-mail 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 e-mail safeguard is to have a warning, such as "External E-mail," added as the top line of the message for every e-mail received from an outside sender. The warning should highlight internally any attempt at spoofing the lawyer's own e-mails, as well as remind the lawyer and his or her staff to be careful.

but also train his or her staff and make sure they follow the steps too.

Password Fundamentals

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

Strong passwords can sometimes interfere with a 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

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

Even stronger passwords combine

An easy way to remember good passwords is to borrow from leetspeak (or l33tspeak), replacing letters with other characters.

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.

Microsoft offers suggestions for removing ransomware.[29] The FBI also has a publication with suggestions.[30] 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.[31]

As to avoiding scams such as phishing e-mails and malware, a lawyer should decide what steps as technology safeguards are reasonable. Then, the lawyer must not only follow the steps consistently

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 2015, 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."[32] 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

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.

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, and smartphones) 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.

Mobile device security. 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; iPhone 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."[33]

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 e-mail, e-mail attachments, or accessed documents? What access to the firm e-mail 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 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.

In addition, a lawyer should consider having all possibly confidential data accessible through the mobile device 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 his or her e-mail 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.[34] 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 e-mail and associated content away from applications; can distribute applications, data, and configurations; and can even be used to securely deploy new applications from a law firm's "app store." MDM can also remote-wipe the mobile device.

Lawyers might consider mobile device management software, which can secure, monitor, and support all connected mobile devices.

For a mobile device used for work, a lawyer should consider what software (applications) are downloaded, because 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 e-mail attachments does not pose the same risks as a mobile device with thousands of e-mails with confidential client information in the text of the e-mails.

Wi-Fi interception and security. 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 captures packets of information sent through the air between the device and the hot spot. These packets can be passwords, e-mails, or whatever is sent. Software to packet sniff (a packet analyzer) is readily available. Wireshark sells a number of packet capture devices.

Packets can be sent as "clear text" (unencrypted), which means anyone can read them as plain English, or 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 e-mail interception problem, because the e-mails 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.[35] On the other hand, a lawyer can have a Gmail account that is secure. In the website address header (the URL), 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 e-mail 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 e-mail system can require a VPN connection to connect to e-mail.

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 e-mail encryption as part of today's reasonable safeguards to protect the lawyer's mobile devices.

Conclusion

As emphasized by the Model Rules 2012 technology amendments, 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 also train his or her staff to do the same. ■

Notes

1. For background on these ABA Model Rules amendments, see the reports of the ABA Commission on Ethics 20/20, filed May 7, 2012, for the ABA Annual Meeting in August 2012, available at www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html.

2. *State by State Adoption of Selected Ethics 20/20 Commission Policies, Guidelines for an International Regulatory Information Exchange, and Amendment to Model Rule 8.4*, ABA Center for Prof. Resp. Pol'y Implementation Committee, www.americanbar.org/content/dam/aba/administrative/professional_responsibility/state_implementation_selected_e20_20_rules.authcheckdam.pdf (last updated Dec. 1, 2016).

3. *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466, at 2 n.3 (Apr. 24, 2014) (discussing whether a lawyer should research a juror's Internet presence, saying "we are also mindful of the recent addition of Comment [8] to Model Rule 1.1"); Fla. Bar Prof'l Ethics Comm., 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.").

4. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, and HIPAA's implementing regulations, 45 C.F.R. §§ 160–164, regulate the collection, use, and disclosure of medical information by health care providers and their business associates (entities that do business with health care providers; i.e., lawyers with doctors as clients).

5. 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 nonpublic financial information by financial institutions and entities that receive nonpublic financial information from financial institutions (i.e., lawyers with banks as clients).

6. 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 valuable resources on legal ethics relative to other aspects of technology, including social media and metadata, see the ABA Legal Technology Resource Center (LTRC) at www.americanbar.org/groups/departments_offices/legal_technology_resources/resources.html.

7. David Ries, *Security*, ABA TECHREPORT 2015, *available at* www.americanbar.org/publications/techreport/2015/Security.html.

8. Catherine Sanders Reach, *Arsenic and Old Lace: Technology Competency*, Addendum (Ala. State Bar), Oct. 2016, www.alabar.org/assets/uploads/2016/10/Addendum-Oct-2016.pdf.

9. Robert Ambrogi, *Viruses Are More Common at Law Firms Than Encryption, ABA Survey Shows*, L. Sites (Sept. 12, 2014), www.lawsitesblog.com/2014/09/viruses-much-common-law-firms-encryption-aba-survey-shows.html.

10. Casper Manes, *The Top 24 Free Tools for Data Encryption*, GFI Talk (June 12, 2015), www.gfi.com/blog/the-top-24-free-tools-for-data-encryption/.

11. John Thomas A. Malatesta III & Sarah S. Glover, *A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses*, 17 Sedona Conf. J. 761 (2016). For any business considering data security, this article has numerous action items and

considerations when evaluating existing or potential vendors.

12. *See Cloud Ethics Opinions around the U.S.*, ABA LTRC, www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Jan. 5, 2017).

13. *Dropbox Alternatives: 10 Best Cloud Storage Services*, Beebom, http://beebom.com/best-dropbox-alternatives-for-cloud-storage/ (last updated Mar. 1, 2016).

14. Mike Batters, *Security Comment: Why Are People Still Using Dropbox for Business?*, Legal IT Insider (Apr. 14, 2016), www.legaltechnology.com/latest-news/security-comment-why-are-people-still-using-dropbox-for-business/.

15. *Available at* https://cfl.dropboxstatic.com/static/business/resources/dfb_security_whitepaper-vflDw-Ksl.pdf.

16. James Bourne, *MobileIron Security Report: iOS Increases Dominance, Dropbox Most Banned Consumer App*, Enterprise AppsTech (Aug. 2, 2016), www.appstechnews.com/news/2016/aug/02/mobileiron-security-report-ios-increases-dominance-dropbox-most-banned-consumer-app/.

17. *HHS Settles with Health Plan in Photocopier Breach Case*, HHS.gov, www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html (last visited Jan. 5, 2017).

18. *See* Jonathan Strickland, *10 Worst Computer Viruses of All Time*, HowStuffWorks Tech (Aug. 26, 2008), http://computer.howstuffworks.com/worst-computer-viruses1.htm.

19. *See Ransomware*, Microsoft Malware Protection Center, www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx (last visited Jan. 5, 2017).

20. For example, a Pennsylvania district attorney's office recently paid about $1,400 in bitcoin to a malware ring known as the Avalanche. Joe Mandak, *Prosecutor's Office Paid Bitcoin Ransom in Cyberattack*, ABC News (Dec. 5, 2016), http://abcnews.go.com/Technology/wireStory/feds-business-lost-387500-world-cybercrime-operation-43985864.

21. Rebecca Campbell, *FBI Now Says Don't Pay Bitcoin to Ransomware Extortionists*, Cryptocoins News (Aug. 9, 2016), www.cryptocoinsnews.com/fbi-now-says-dont-pay-bitcoin-ransomware-extortionists/.

22. Richard Winton, *$17,000 Bitcoin Ransom Paid by Hospital to Hackers Sparks Outrage*, L.A. Times, Feb. 19, 2016, www.latimes.com/business/technology/la-me-ln-17000-bitcoin-ransom-hospital-outrage-20160219-story.html.

23. Danny Palmer, *Two-Thirds of Companies Pay Ransomware Demands: But Not Everyone Gets Their Data Back*, ZDNet (Sept. 7, 2016), www.zdnet.com/article/two-thirds-of-companies-pay-ransomware-demands-but-not-everyone-gets-their-data-back/.

24. *See Help Prevent Malware Infection on Your PC*, Microsoft Malware Protection Center, www.microsoft.com/en-us/security/portal/mmpc/shared/prevention.aspx (last visited Jan. 5, 2017).

25. If separate computers are not possible, at least have separate accounts on the same computer (especially if a child is using it).

26. Debra Cassens Weiss, *Don't Click! Lawyers Get Fake Emails about a Complaint; Hyperlink Installs Malicious Software*, A.B.A. J. (Dec. 5, 2016), www.abajournal.com/news/article/dont_click_lawyers_get_fake_emails_about_a_complaint_hyperlink_installs_mal/?utm_source=internal&utm_medium=navigation&utm_campaign=most_read.

27. *Q1 2016 Sees 93% of Phishing Emails Contain Ransomware*, PhishMe (June 4, 2016), http://phishme.com/q1-2016-sees-93-phishing-emails-contain-ransomware/.

28. *What Is Social Engineering?*, Webroot, www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering (last visited Jan. 5, 2017).

29. *Ransomware: Frequently Asked Questions*, Microsoft Protection Center, www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx#faq (last visited Jan. 5, 2017).

30. FBI, Ransomware Prevention and Response for CISOs, www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Jan. 5, 2017).

31. Campbell, *supra* note 21; *Incidents of Ransomware on the Rise*, FBI (Apr. 29, 2016), www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/.

32. For 2015's worst passwords, see www.teamsid.com/worst-passwords-2015/.

33. Joe Dysart, *New Hacker Technology Threatens Lawyers' Mobile Devices*, A.B.A. J. (Sept. 1, 2013), www.abajournal.com/magazine/article/new_hacker_technology_threatens_lawyers_mobile_devices. Since 2013, employers have generally adapted to BYOD. Madhavi Dhingra, *Legal Issues in Secure Implementation of Bring Your Own Device (BYOD)*, 78 Procedia Computer Sci. 179, *available at* www.sciencedirect.com/science/article/pii/S1877050916000326; Paul G. Lannon & Phillip M. Schreiber, *BYOD Policies: What Employers Need to Know*, Soc'y for Hum. Resource Mgmt. (Feb. 1, 2016), www.shrm.org/hr-today/news/hr-magazine/pages/0216-byod-policies.aspx.

34. To view Citrix's MDM video, see www.youtube.com/watch?v=oUYYZdSXQTQ. To view Microsoft's MDM video, see www.youtube.com/watch?v=MUnCEPjZreY.

35. For a general discussion of lawyers' communicating confidential information by e-mail and risks lawyers should consider, see Tex. State Bar Prof'l Ethics Comm., Op. 648 (Apr. 2015), www.legalethicstexas.com/Ethics-Resources/Opinions/Opinion-648.aspx.