News, cases, companies Search

Advanced Search

Take a Free Trial | Sign In

Sign In

News, cases, companies

- Take a Free Trial
- Sign In

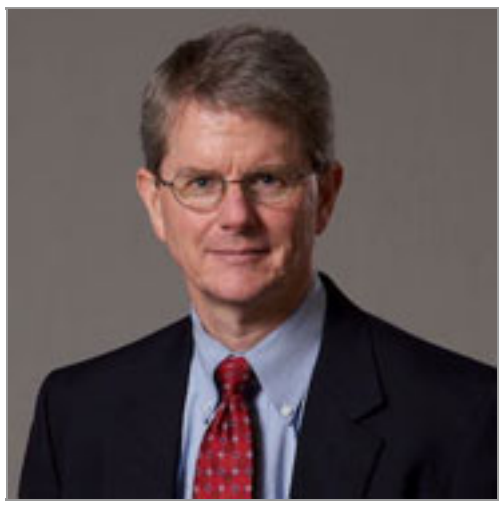
News, cases, companies

Advanced Search

Close

- Adv. Search & Platform Tools
- **Browse all sections**
- Banking
- Bankruptcy
- Class Action
- Competition
- Employment
- Energy
- Insurance
- Intellectual Property
- Product Liability
- Securities
- Rankings
- Glass Ceiling Report
- Global 20
- Law360 400
- Minority Report
- Practice Group Partner Rankings
- Practice Groups of the Year
- Pro Bono Firms of the Year
- Rising Stars
- Trial Aces
- Site Menu
- Join the Law360 team
- Search legal jobs

Ethics In The Tech Age: What Every Lawyer Should Consider



J.S. “Chris” Christie Jr.

Law360, New York (April 1, 2015, 12:00 AM ET) -- In light of recent changes to the ABA Model Rules of Professional Conduct, what are a lawyer’s ethical duties arising from new technology? And what should a lawyer know about technology?

Model Rules’ Technology and Confidentiality Amendments

In light of new technology and evolving security concerns, the ABA Commission on Ethics 20/20 submitted to the ABA House of Delegates a Resolution and Report on Technology and Confidentiality.[1] To guide lawyers regarding the use of technology, the commission proposed, and the ABA House of Delegates approved, amendments to the Model Rules of Professional Conduct. The amendments changed Model Rules 1.6 (Confidentiality of Information) and 1.1 (Competence).

As to Model Rule 1.6, the amendments add a new paragraph and change two comments. The commission recognized that existing 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. The commission concluded that, in light of the pervasive use of technology to store and send confidential client information, this existing obligation should be stated explicitly in the black letter of Model Rule 1.6. The commission also concluded that the comments should be 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 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 has a duty to keep up with technology; the amendment emphasizes that duty. 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.").

As a practical matter, few lawyers today are governed by the technology-related changes to the Model Rules. Lawyer conduct is governed by state rules, not the ABA Model Rules. While states except California have adopted a version of the ABA Model Rules, based on a chart on the ABA website, only 13 states as of March 2015 have adopted the August 2012 amendments to the Model Rules (22 states report they are "studying" the amendments).[2] Yet, the Commission on Ethics 20/20 addressed technology issues that concern every lawyer practicing today. And lawyers who do not adequately address technology might find themselves embarrassed, if not worse.

Ethics and Technology: Practical Considerations for Lawyers

So, in light of these amendments to the Model Rules, what are some of the technology risks in 2015 for lawyers? In addition to computer system security, every lawyer should consider password fundamentals, mobile security and scam avoidance.

Lawyers and Computer System Security

How to protect computer systems is generally beyond the scope of this paper. Unless one is the rare lawyer with the technical skills, finding someone with expertise to help is advisable. According to an ABA Legal Technology Survey Report published in September 2014, viruses, spyware, or malware infected nearly half of law firms' computer systems last year. Yet, only one-fourth of law firms had any kind of encryption available for their lawyers to use.[3]

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. Therefore, the key to protecting data can be encryption, the key to accessing encrypted data is having the key, and the key to safeguarding encrypted data is protecting the key.

A lawyer should consider what data might need to be encrypted. Some email programs automatically encrypt data when sent. Data can be encrypted when at rest, but such steps complicate the user experience. Encrypting all electronic information interferes with using the information efficiently. If data relating to the representation of a client is on a hard drive, a thumb drive, a mobile device, or attached to an email — whether it should be encrypted depends on a number of factors. Many free encryption tools are available.

Lawyers and Password Fundamentals

Every lawyer should consider password fundamentals for client information that is confidential. Good passwords are a simple precaution 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 someone can research and discover might create a risk.

First, what are bad passwords? The website SplashData released its list of the most popular internet passwords for 2012. As the most common passwords, they are also the most vulnerable. Topping the list was "password," with "123456" as runner-up, followed by the slightly more inventive "12345678."[4] Any password that someone could guess is a bad (weak) 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 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 passwords kept there.

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, required authorization before downloading applications, and automatic wiping if access is attempted

incorrectly a certain number of times.

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 predominate smartphone platform 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."[5]

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 drunken lawyer lost his smartphone?

For any mobile device that has information relating to the representation of a client, a lawyer should consider having a PIN or 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 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 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.[6] 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 securely deploy new applications from a law firm's "app store." MDM can also remote-wipe the mobile device.

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.

Wi-Fi Interception and Security for Lawyers

If a lawyer uses Wi-Fi, especially in a café or hotel hot spot, someone 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, emails 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 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. On the other hand, a lawyer can have a Gmail account that is secure. In the website address header (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.

Mobile devices are easier to use if information is stored on 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 and should consider whether that data is secure, encrypted and backed-up. Ala. Ethics Op. 2010-2. Often, using a cloud service is more secure than what a lawyer might be able to have on the lawyer’s own network and systems. Examples of file storage or sharing services include Dropbox, Box by Box Inc. and Citrix’s ShareFile.[7]

Dropbox might be the most popular cloud file storage and sharing service, with more than 100 million users, including many lawyers. On the Dropbox homepage, it says that it uses “256-bit AES encryption” (the strongest normal standard today) and two-step verification, so that “your stuff is always safe in Dropbox.” Nonetheless, putting aside user misuse, perfect security is not possible, with two recent articles raising security concerns with regard to Dropbox.[8] For whatever reasons, Dropbox has been identified as the app that employers ban more than any other app.[9]

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 today’s reasonable safeguards to protect the lawyer’s mobile devices.

Lawyers and Scam Avoidance

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 they were deceived into allowing access to their computer or to their passwords.

A hacker can gain computer access when a user responds to phishing or spoofing emails; downloading games or apps with malware; or downloading malware by opening infected email attachments, infected thumb drives, or questionable websites. Some malware records keystrokes, which can reveal even the most complicated passwords. Separating use of computers for work and personal purposes can reduce the risks. Common sense can help, too.

What Risk-Reducing Steps Should a Lawyer Take?

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, what a lawyer should do depends on many factors and requires sound judgment.

For discussion, accept that the U.S. Post Office, Federal Express and UPS all have in the past lost and misdirected lawyers' packages with information relating to the representation of a client. Instead of sending a letter by mail, a lawyer might pay a professional courier, a runner or a paralegal to hand-deliver the package to reduce the risk of such a problem. Most lawyers would agree that such effort is rarely, if ever, required. On the other hand, a lawyer would want to make sure the package was sealed properly, was addressed correctly, and did not have see-through wrapping. Which of the technology safeguards mentioned above are comparable to ensuring a package is sealed properly and which are comparable to hand-delivery by a paralegal?

Conclusion

The Commission on Ethics 20/20 intended the 2012 amendments to the Model Rules not only to help lawyers consider the risks arising from using technology, but also to encourage lawyers to wisely take advantage of technology to increase the quality of legal services and to provide services more efficiently. As the commission intended and as a matter of legal ethics, lawyers should understand the reasonable steps that can reduce technology risks, should reasonably safeguard information relating to the representation of a client, and should use technology consistent with the applicable ethical rules.

—By J.S. "Chris" Christie Jr., Bradley Arant Boult Cummings LLP

Chris Christie is a partner with Bradley Arant Boult Cummings LLP's Birmingham, Alabama, office. He is chairman of the firm's insurance litigation group and co-chairman of its pro bono committee. He served as a Peace Corps Volunteer, teaching law at the University of Yaoundé School of Law and Economics.

Parts of this paper were in an article Christie wrote that was published as Ethics and Technology, 75(1) Ala. Law. 31 (2014).

[1] The Commission's Resolution and Report.

[2] The chart of "State by State Adoption of Selected Ethics 20/20 Commission Policies."

[3] Read "Viruses are More Common at Law Firms than Encryption, ABA Survey Shows."

[4] Read the "Top 25 Worst Passwords Revealed."

[5] Read the ABA Journal's article, "New hacker technology threatens lawyers' mobile devices" and the TechRepublic's article, "Security policies must address legal implications of BYOD."

[6] View an MDM demo.

[7] Read The Cyber Advocate's "Four Alternatives to Dropbox to Meet Your Firm's Storage Needs."

[8] Read "Looking inside the (Drop) Box," a whitepaper coauthored by Dhiru Kholia of the University of British Columbia and Przemyslaw Wegrzyn of Code Painters; Read TechRepublic's "DropSmack: Using Dropbox to steal files and deliver malware."

[9] Read Inc.com's "Top 10 Apps Banned in the Office."

Related Articles

- Lawyers And Email: Ethical And Security Considerations
- Check The Forecast Before Using Cloud-Based Storage
- How Lawyers Can Avoid Ethical Problems In The Cloud
- Clouds, Mobile Devices And The Workplace
- How To Protect Your Device From Data Disasters

View comments

Related

Sections

- Banking
- Bankruptcy
- California
- Capital Markets
- Class Action
- Commercial Contracts
- Competition
- Consumer Protection
- Corporate
- Employment
- Energy
- Environmental
- Florida
- Food & Beverage
- Government Contracts
- Health
- Hospitality
- Immigration
- Insurance
- Intellectual Property
- International Trade
- Legal Ethics
- Life Sciences
- Media & Entertainment
- Mergers & Acquisitions
- Native American
- New Jersey
- New York
- Pennsylvania
- Privacy
- Private Equity
- Product Liability
- Project Finance
- Public Policy
- Real Estate
- Retail & E-Commerce
- Securities
- Sports
- Tax
- Technology
- Telecommunications
- Texas
- White Collar

Law Firms

- Bradley Arant

Companies

- Box Inc.
- Microsoft Corporation
- Research In Motion Limited
- United Parcel Service Inc.

Government Agencies

- Peace Corps

Most Popular

- 1 Why It's Not So Bad To Be A Nonequity Partner
- 2 Why BigLaw's New 'Big Brother' Program Won't Be All Bad
- 3 DLA Piper Atty's Killer Gets 24 Years
- 4 Libor MDL Judge Throws Unprepared Lawyer Out Of Court
- 5 USPTO Unveils Reforms After Examiner Golfed On The Job

DEWEY LIVE BLOG

Follow our exclusive coverage of the trial of the year:

Catch up on the Dewey trial here

×

Add this article to my briefcase

Ethics In The Tech Age: What Every Lawyer Should Consider

Create new folder:

Name required

OR

Select a folder to add to:

Add Now Cancel

Visit Our Site Map