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, the ABA Model Rules of Professional Conduct were amended in August 2012. The amendments changed Model Rules 1.1 (competence) and 1.6 (confidentiality of information).

Amended Model Rule 1.1, comment [8], stresses 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.

The amendment to Model Rule 1.6 adds a new paragraph and changes 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.

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."

In light of these amendments, what are technology risks in 2017 for lawyers?

> MOBILE TECHNOLOGY POSES RISKS THAT LAWYERS SHOULD CONSIDER MORE CAREFULLY.

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 anti-virus software and other security software, including a firewall. A lawyer should consider regularly updating software and replacing software that is no longer being updated. For all electronic data, a lawyer should consider whether the data should be encrypted.

A lawyer should consider what data might need to be encrypted. Some e-mail programs automatically encrypt data when sent. Another issue is whether to encrypt data at rest. 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.

A lawyer should consider whether his or her safeguards are HIPAA or 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.

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 risks a vendor presents to data security. A lawyer should exercise reasonable due diligence selecting vendors, have contracts with vendors requiring them to safeguard data, and monitor vendors' compliance.

Another issue involves the cloud. Because cloud computing places client data on remote servers not in a lawyer's direct

J.S. "Chris" Christie Jr. (jchristie@bradley.com.) is a Birmingham, Alabama, partner of Bradley Arant Boult Cummings LLP. Parts of this article were published as "Ethics and Technology," *Alabama Lawyer,* January 2014 (75:1).

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. Often, a cloud vendor offers greater security than what a lawyer might have on the lawyer's own computer systems. A cloud vendor is also likely to have better backup capability.

Avoiding scams. Hackers often attempt to gain access by deceit. 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.

Lawyers should be able to reduce malware risk 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 non-work apps; do not open risky thumb drives or CDs; do not visit unsafe, suspicious, or fake websites; install up-to-date anti-virus and security software; update software; separate work and personal computer use; and backup important files in a remote, unconnected facility.

Mobile security. Mobile technology poses risks that lawyers should consider more carefully. These risks include WiFi interception and the loss of computers that are mobile devices. Risk reducers include passwords, encryption, two-factor identification, inactivity time-outs, authorization before downloading applications, remote wiping, and automatic wiping if access is attempted incorrectly a certain number of times.

Mobile device security. An overwhelming trend in mobile devices is "bring your own device" (BYOD). Years ago, many law firms allowed only firm-approved and firm-owned mobile devices. With advances in smartphones and tablets, BYOD has become the accepted norm. 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" (tinyurl.com/l8z45ks).

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 strong 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.

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

WiFi interception and security. If a lawyer uses WiFi, 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.

Packets can be sent as "clear text" (unencrypted) or on an encrypted connection. A lawyer using a general webmail service such as Gmail 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, look for an "S" after the HTTP, which indicates that the site uses encryption.

When using WiFi, 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. ■