LawPracticeTODAY
THE MONTHLY WEBZINE OF THE ABA LAW PRACTICE MANAGEMENT SECTION

Cyber Security for Attorneys: Understanding the Ethical Obligations

By David G. Ries

March 2012

As attorneys continue to embrace the latest technology, it is critical to understand and address the ethical obligations that go with it—from SmartPhones and cloud computing to laptops and USB drives—at the core is a duty of confidentiality.

As attorneys continue to embrace the latest technology, it is critical for them to understand and address the ethical obligations that go with it. This applies to the very latest technology, like SmartPhones and cloud computing, as well as other current technology, like laptops, remote access, wireless networks, and USB drives, that attorneys have been using for a number of years. At the core of these obligations is the duty of confidentiality.

Threats to data in computers, mobile devices, and information systems used by attorneys are at an all-time high. They range from lost or stolen laptops or mobile devices, to dishonest, disgruntled, or untrained insiders, to sophisticated hacking attacks. There have been numerous recent reports about these threats to attorneys in the news media, legal press, and information security publications. A recent article reported that 80 law firms were hacked during 2011. In November of 2011, the FBI met with major law firms to deal with the rising number of law firm computer intrusions, warning them that hackers see attorneys as a back door to the valuable data of their corporate clients. Attorneys' ethical obligations include understanding and dealing with these threats.

Ethics Rules

Attorneys' use of technology presents special ethics challenges, particularly in the areas of competence and confidentiality. Attorneys also have common law duties to protect client information and may have contractual and regulatory duties. For these other areas, see, Safeguarding Confidential Data: Your Ethical and Legal Obligations, Law Practice (July/August 2010).

The duty of competence (ABA Model Rule 1.1) requires attorneys to know what technology is necessary and how to use it. The duty of confidentiality (ABA Model Rule 1.6) is one of an attorney's most important ethical responsibilities. Together, these rules require attorneys using technology to take competent and reasonable measures to safeguard client data. This duty extends to all use of technology, including computers, mobile devices, networks, technology outsourcing, and cloud computing.

Model Rule 1.1 covers the general duty of competence. It provides that "A lawyer shall provide competent representation to a client." This "requires the legal knowledge, skill, thoroughness and

preparation reasonably necessary for the representation." It includes competence in selecting and using technology. It requires attorneys who lack the necessary technical competence for security (many, if not most attorneys) to consult with qualified people who have the requisite expertise.

Model Rule 1.6 generally defines the duty of confidentiality. It begins as follows:

> A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b). . . .

Rule 1.6 broadly requires protection of "information relating to the representation of a client;" it is not limited to confidential communications and privileged information. Disclosure of covered information generally requires express or implied client consent (in the absence of special circumstances like misconduct by the client).

The Ethics 2000 revisions to the Model Rules added Comment 16 to Rule 1.6. This comment requires reasonable precautions to safeguard and preserve confidential information:

> Acting Competently to Preserve Confidentiality
>
> [16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

The Comment references Model Rule 5.1 (Responsibilities of a Partner or Supervisory Lawyer) and Model Rule 5.3 (Responsibilities Regarding Nonlawyer Assistant), which are also important in attorneys' use of technology. Partners and supervising attorneys are required to take reasonable actions to ensure that those under their supervision comply with these requirements.

Model Rule 1.4, Communications, also applies to attorneys' use of technology. It requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology. It requires keeping the client informed and, depending on the circumstances, may require obtaining "informed consent." It requires notice to a client of compromise of confidential information relating to the client.

Ethics Opinions

A number of state ethics opinions have addressed professional responsibility issues related to security in attorneys' use of various technologies. It is important for attorneys to consult the rules, comments, and ethics opinions in the relevant jurisdiction(s).

An early example is State Bar of Arizona, Opinion No. 05-04 (July 2005) (Formal Opinion of the Committee on the Rules of Professional Conduct). It requires "competent and reasonable steps to assure that the client's confidences are not disclosed to third parties through theft or inadvertence" and "competent and reasonable measures to assure that the client's electronic information is not lost or destroyed." It further notes that "an attorney must either have the competence to evaluate the nature of the potential threat to the client's electronic files and to evaluate and deploy appropriate computer hardware and software to accomplish that end, or if the attorney lacks or cannot reasonably obtain that competence, to retain an expert consultant who does have such competence."

Additional examples include New Jersey Advisory Committee on Professional Ethics, Opinion 701, "Electronic Storage and Access of Client Files" (April, 2006), State Bar of Arizona, Opinion No. 09-04 (December, 2009): "Confidentiality; Maintaining Client Files; Electronic Storage; Internet" (Formal Opinion of the Committee on the Rules of Professional Conduct); State Bar of California, Standing Committee on Professional Responsibility and Conduct, Formal Opinion No. 2010-179; and Pennsylvania Bar Association, Committee on Legal Ethics and Professional Responsibility, Formal Opinion 2011-200, "Ethical Obligations for Attorneys Using Cloud Computing/Software as a Service While Fulfilling the Duties of Confidentiality and Preservation of Client Property" (November, 2011). In addition to this Pennsylvania opinion, there are now several ethics opinions on attorneys' use of cloud computing, which involves cyber security, outsourcing, and a number of additional ethical considerations.

The key professional responsibility requirements from these opinions are competent and reasonable measures to safeguard client data, including an understanding of limitations in attorneys' competence, obtaining appropriate assistance, continuing security awareness, and ongoing review as technology, threats, and available security evolve over time.

Ethics 20/20

The ABA Commission on Ethics 20/20 is currently in the process of reviewing the ABA Model Rules of Professional Conduct and the U.S. system of lawyer regulation in the context of advances in technology and global legal practice developments. One of its areas of focus is technology and confidentiality. It released Revised Draft Resolutions in this area in February of this year.

The Revised Draft proposes adding the underlined language to the Comment to Model Rule 1.1 Competence:

> [6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, …

It proposes adding the following new subsection (underlined) to Model Rule 1.6 Confidentiality of Information:

> (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.

The draft recommends the following changes to Comment [16] to this rule:

> Acting Competently to Preserve Confidentiality
> [16] Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include 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). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

These proposed revisions are clarifications rather than substantive changes. They add additional detail that is consistent with the present rules and comments, ethics opinions, and generally accepted information security principles.

Information Security Basics

Information security is a process to protect the confidentiality, integrity, and availability of information. Comprehensive security must address people, policies and procedures, and technology. While technology is a critical component of effective security, the other aspects must also be addressed. As explained by Bruce Schneier, a highly respected security professional, "[i]f you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[i] The best technical security is likely to fail without adequate attention to people and policies and procedures. Many attorneys incorrectly think that security is for the IT department or

consultants. While IT has a critical role, everyone, including management, all attorneys, and all support personnel, must be involved for effective security.

An equally important concept is that security requires training and ongoing vigilance and attention. It must go beyond a onetime "set it and forget it" approach.

Security starts with a risk assessment to identify anticipated threats to the information assets, including an inventory of information assets to determine what needs to be protected. The next step is development and implementation of a comprehensive information security program to employ reasonable physical, administrative, and technical safeguards to protect against identified risks. This is the most difficult part of the process. It must address people, policies and procedures, and technology. It needs to include assignment of responsibility, training, ongoing security awareness, monitoring for compliance, and periodic review and updating.

The requirement for lawyers is reasonable security, not absolute security. New Jersey Ethics Opinion 701 states "'[r]easonable care,' however, does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible…" Recognizing this, the Ethics 20/20 proposal includes "…[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure."

Security involves balancing and trade-offs to determine what risks and safeguards are reasonable under the circumstances. The analysis includes the sensitivity of the information, the risks, and available safeguards (including their cost, difficulty of implementation, and effect on usability of the technology). There is frequently a trade-off between security and usability. Strong security often makes technology very difficult to use, while easy to use technology is frequently insecure. The challenge is striking the correct balance among all of these often competing factors. This aspect of security is also recognized by the Ethics 20/20 proposal.

Reasonable Safeguards

The greatest challenge for lawyers in establishing cyber security programs is deciding what security measures are necessary and then implementing them. Determining what constitute "competent and reasonable measures" can be difficult. The Ethics 20/20 proposal, discussed above, provides some high level guidance. It includes the following factors:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include 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).

The Commission is exploring the use of a central ABA resource to advise attorneys on reasonable security. The Law Practice Management Section currently provides helpful resources on cyber security, including this webzine, *Law Practice* magazine, ABA TECHSHOW and other continuing legal education programs.

Conclusion

Attorneys have an ethical obligation to take competent and reasonable measures to implement cyber security to safeguard information relating to clients. This includes approaching information security as a process, understanding limitations in attorneys' competence, obtaining appropriate assistance, continuing security training and awareness, and ongoing review as technology, threats, and available security evolve over time.

David G. Ries *is a partner in the Pittsburgh, PA, office of Thorp Reed & Armstrong, LLP, where he practices in the areas of environmental, commercial and technology litigation. He is a member of the ABA Law Practice Management Section Council and regularly speaks and writes on technology law and ethics issues, including a new book, with Sharon Nelson and John Simek, Locked Down: Information Security for Lawyers (American Bar Association 2012).*

---

[i] *Bruce Schneier, Secrets and Lies - Digital Security in a Networked World (John Wiley & Sons, Inc. 2000) at p. xii.*