New York Law Journal

An Update on Lawyers' Duty of Technological Competence: Part 1

By Anthony E. Davis and Steven M. Puiszis
New York Law Journal
March 1, 2019

As published on Page 3

In this Professional Responsibility column, Anthony E. Davis and Steven M. Puiszis write: The duty of competence requires lawyers to be aware of the benefits and risks of emerging technologies that can be used to deliver legal services and how advances in existing technologies can impact the security of information in their possession. Because of the speed at which technology is advancing, the lawyer's duty of competence must evolve with the technologies.

In 2012 Rule 1.1 of the ABA's Model Rules—the duty of competence—was modified in Comment 8 to require that lawyers know and understand "the benefits and risks and associated with relevant technology." Consistent with that change, Comment 8 to New York Rules of Professional Conduct (RPC) 1.1 states: "To maintain the requisite knowledge and skill, a lawyer should … (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information." As early as 2004, N.Y. State Bar Association Ethics Opinion 782 opined that a lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology.

In our Jan. 8, 2016 column "The Ethical Obligation to Be Technologically Competent," we explored the meaning of this duty in connection with using technology in a manner consistent with lawyers' duty to preserve clients' confidences and secrets in the light of the growing threats to data security. In this article we will consider the much broader implications of this duty in the era of Artificial Intelligence and other critical developments in the high tech world in which lawyers now operate (willingly or not).

There are six realms of technological competence reasonably necessary for today's lawyers: data security; the technology used to run a law firm and practice law; social media competence; technology used by clients to build products or offer services that lawyers have to defend; electronic discovery; and technology used to present information in court. In this first of two articles we will consider the first two realms. The remainder will be covered in the next article.

Data Security

The Jan. 8, 2016 article focused on this topic, and the threats identified there continue unabated, albeit with ever increasing sophistication, including phishing, social engineering attacks, data breaches and Internet scams. And as the threats have increased in intensity and severity, the duty to understand and protect clients and law firms themselves has expanded commensurately.

But the duty is broader than creating walls against invaders. It requires that in complying with their duties to preserve client confidences under RPC 1.6, lawyers take reasonable care to ensure that only authorized individuals have access to electronic files. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but although not adopted in the Comments to New York's RPC's, Comment 18 to Model Rule 1.6 lists factors to consider in assessing what constitutes ″reasonable efforts″ to protect against the inadvertent or unauthorized disclosure of, or access to client information including:

- The sensitivity of the information.
- The likelihood of disclosure if additional safeguards are not taken.
- The cost of employing additional safeguards.
- The difficulty of implementing the safeguards.
- The extent to which the safeguards adversely affect a lawyer's ability to represent a client.
- Whether the client requires special security measures be taken or provides informed consent to forgo security measures that might be required under this rule.

Data security is thus a relative concept. What might be reasonable and appropriate safeguards for one firm may be completely inadequate for another. The nature of a law firm's practice area(s), its size, geographic locations, office footprint, clientele, and the technological sophistication of its lawyers and staff are all relevant factors. The increasing use by clients of outside counsel guidelines containing data security requirements makes Comment 18's final factor critical in any such analysis.

The use of the cloud implicates the lawyer's duty of competence under Rule 1.1, as well as 1.6 duties to preserve confidential information. Because use of the cloud means that client information will be stored on a third party's servers, it poses a different set of security risks, as third parties may be permitted to have some form of access to client information.

A lawyer's duty to safeguard information under its control cannot be transferred or delegated to a third party, nor is it lessened simply because the lawyer stores client information with a cloud provider. A lawyer must evaluate whether a cloud provider's terms of use, policies, practices and procedures are compatible with the lawyer's professional obligations.

N.Y. State Bar Association Ethics Opinion 842 (2010) suggested that exercising "reasonable care" in this context "may" require:

- Verifying the cloud storage provider has an enforceable obligation to preserve confidentiality and will notify the lawyer if served with process requiring the production of client information.

- Investigating the adequacy of the cloud provider's security, policies, recoverability methods, and other procedures.

- Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored.

- Investigating the cloud provider's ability to purge any copies of the data, and to move the data to a different host for any reason.

The opinion also points out that a highly relevant inquiry is whether the cloud provider has ever suffered a security breach, and if so, how the breach (or breaches), occurred and what steps have been taken to prevent a reoccurrence.

Given the increasing importance of encryption to data security, lawyers should inquire if the cloud provider encrypts information both in transit and at rest.

Finally, law firms should consider rules and policies that prohibit the use of public clouds that have not been carefully evaluated and approved by the firm. This would include the use of mobile technology and applications that store sensitive or confidential client information in public clouds without the firm's prior express authorization.

Although the N. Y. State Bar Association Ethics Committee took the position in Formal Opinion 1019 that client consent is unnecessary when a law firm is able to make a determination that the security measures in place are reasonable in connection with technology used for remote access to client files, the risk exists that a client may later second guess that determination. Accordingly, even if not required to do so, lawyers should consider addressing the use of the cloud in their engagement letters, explaining how they use the cloud and its potential ramifications in terms that clients can understand.

More generally, law firms need to consider addressing the sensitivity of client information at the outset of any engagement. The client can be asked at the file opening stage if the engagement will involve any highly sensitive information or information warranting special security measures. Additionally, the file intake process can be set up to identify any categories of information that state or federal law treat as highly sensitive in nature or that the firm believes should be treated as highly sensitive. Examples could include personally identifying information, protected health information, non-public financial information, proprietary information, source code, patents, trademarks, trade dress, trade secrets, a merger and acquisition or a high stake business deal. A firm can then take any steps it deems necessary and appropriate to protect that information, including limiting who is permitted to access that information and how it may be transmitted.

Finally, record retention policies cannot be ignored. Given today's level of data breach risk, records and data should be kept no longer than necessary. Data protection also requires careful and proper disposal of client records.

Technology Used to Run a Law Firm and Practice Law

Computer research has made law libraries and hard copy of texts obsolete. Tools are now available that can identify relevant decisions that were not cited in a party's brief. Software programs can generate a wide variety of basic legal documents. This second realm includes communication technologies, technologies for transmitting information, running conflicts checks, or opening new engagements, as well as applications for document generation, electronic research, electronic calendaring, and docketing. Emerging technologies in this realm include blockchain, knowledge management and data analytics. Knowledge management and data analytics are forms of augmented or artificial intelligence (AI).

There is a growing recognition that different AI tools or applications can potentially lead to differing, inaccurate or even biased results depending on the choices made in developing the algorithm, or the data used to train the algorithm. An algorithm that is trained on a dataset that is incomplete or is the product of unacceptable

human choices and biases will likely produce biased results. Rather than eliminating human bias, the use of AI may reinforce it. These are issues that lawyers will need to consider in deciding which technologies to use, rather than simply relying on so-called blackbox technologies.

Ideally an algorithm or AI tool should be able to explain its output. The persons who created the algorithm and trained it, as well as their background, experience and expertise are questions that should be considered. Equally, the dataset or information used to train the algorithm is should be considered and should be available for review.

Lawyers subject to the EU's General Data Privacy Regulation (GDPR) should be aware that Article 15(h) of the GDPR, requires data controllers to provide "meaningful logic" about any automated decision-making tools that produce "legal effects" on EU data subjects. Because a lawyer qualifies as a data controller under the GDPR, he or she may need to obtain that information from the developer of an AI tool or application, depending on its purpose and how it is used by the lawyer.

In sum, if an attorney lacks a basic understanding of how to use an available technology, or the risks inherent in the technologies used to provide legal services, how can the attorney take "reasonable steps" to competently guard against those risks? The duty of competence also requires lawyers to be aware of the benefits and risks of emerging technologies that can be used to deliver legal services and how advances in existing technologies can impact the security of information in their possession. Because of the speed at which technology is advancing, the lawyer's duty of competence must evolve with the technologies.

Anthony E. Davis *and* ***Steven M. Puiszis*** *are partners of Hinshaw & Culbertson. Anthony E. Davis is a past president of the Association of Professional Responsibility Lawyers. Steven M. Puiszis is Hinshaw's General Counsel—Privacy, Security & Compliance.*