Inexcusable Incompetence

The Duty to "Keep Abreast" of Technology

By Alyssa A. Johnson

As lawyers, our duty of competence is paramount and fundamental to our practice. As explained in the Model Rules, "[c]ompetent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." Model Rules of Prof'l Conduct R. 1.1. Before lawyers and their clients began using internet-based technology to store confidential information and communicate with each other, "competency" was a straightforward concept.

In 2012, comment 8 was added to Model Rule 1.1. It reads: "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 relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." (emphasis added). Twenty-six states have adopted comment 8. Robert Ambrogi, *Another State Adopts Duty of Technology Competence; Makes It 26*, (Dec. 28, 2016), available at http://www.lawsitesblog.com.

Recently, Florida became the first state to take comment 8 one step further. As of January 1, 2017, Florida requires members of the Florida bar to take three hours of continuing legal education credits geared toward understanding the risks and benefits of technology. *In re: Amend. to Fla. Bar Rules 4-1.1 and 6-10.3*, Case No. S.C.16-574 (Fla. Sept. 29, 2016) (amending Fla. Bar R. 6-10.3). But if you don't hold a license to practice in Florida, and your state has not adopted comment 8, a lawyer's duty of competence arguably extends to having a proficiency in technology. But what exactly are the requirements that attorneys must meet to keep abreast of the "benefits and risk associated with relevant technology"? The key in Model Rule 1.1 is in the definition of preparation: the proficiency level is that which is "reasonably necessary" for the representation. You don't have to be an IT expert, but you have to know enough or have access to enough information to be able to represent your client competently and to make informed decisions about your client's representation.

Two important tech aspects that every attorney should understand are (1) e-discovery, and (2) how to protect your client's data and confidences. If you know that significant e-discovery will be an issue, it is a good practice to hire an outside consultant to assist you. Otherwise, you may risk unknowingly disclosing client confidences that may not be subject to a claw-back provision. You may also risk disclosure of your client's propriety information, causing irreparable harm. *See* Cal. State Bar Formal Op. 2015-193 (discussing the pitfalls of e-discovery in detail).

Obviously, this creates exposure to sanctions and malpractice suits. One court, in interpreting comment 8, sanctioned a defendant's attorney after he claimed that he was "not computer literate." The court noted that "[p]rofessed technological incompetence is not an excuse for discovery misconduct." *James v. Nat'l Fin. LLC*, No. CV 8931-VCL, 2014 WL 6845560, at *12 (Del. Ch. Dec. 5, 2014). The court said, "if a lawyer cannot master the technology suitable for that lawyer's practice, the lawyer should either hire tech-savvy lawyers tasked with responsibility to keep current, or hire an outside technology consultant who understands the practice of law and associated ethical constraints." *Id.* (citing Judith L. Maute, *Facing 21st Century Realities*, 32 Miss. C. L. Rev. 345, 369 (2013)).

Protecting your client's data and confidences also requires the competent use of technology. Model Rule 1.6 requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or *unauthorized access to*, information relating to the representation of a client." (emphasis added). You cannot protect against unauthorized access to your client's information without being aware of your technology, which threats to the technology could arise, and which methods you have or could have in place to mitigate any unauthorized access to your client's information.

As one FBI agent noted,

> Law firms are a rich target. They don't have the capabilities and the resources to protect themselves. Within their systems are a lot of the sensitive infor-

Ethics, continued on page 74

■ Alyssa A. Johnson is an associate with Hinshaw & Culbertson LLP, practicing from the firm's Milwaukee office. She focuses her practice in professional liability defense litigation. Ms. Johnson also has experience with litigation involving real estate, property, workers' compensation, and ERISA claims. She has also handled appeals and amicus briefs on behalf of clients. She received her J.D. degree from Marquette University Law School in 2012. Ms. Johnson is admitted to practice in Wisconsin.

Ethics, from page 72

> mation from the corporations that they represent. And, therefore, it's a vulnerability that the bad guys are trying to exploit, and are exploiting.

Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, (Sept. 13, 2014), available at http://triblive.com.

Cyber-attacks are no longer just a problem for Alicia Florrick on the *Good Wife*; they pose serious issues for every firm. Because attorneys are on notice of cyber-attacks, every lawyer must think of his or her own practice and vulnerabilities. How is your computer, tablet, phone, or another device protected? Just as you would keep a lock on your office door to protect your paper files, your electronic data should be locked down. With the rapid evolution of cyber-crime, it's easier to hack your data than it would be for a person to steal your paper files.

If you are left clueless about e-discovery or how to protect your client's data from a cyber-threat such as ransomware, it is your duty to educate yourself or to hire or associate with someone who can help you understand and mitigate technology risks. When hiring a third-party IT vendor, your duty to protect client confidences extends to the vendor, as well. Not only can being aware of the risks and benefits of technology prevent you from being on the wrong end of a malpractice suit, but you can also use your knowledge, or your consultant's knowledge, to your advantage to attract clients that are likely also dealing with the change of the times. FD