Legal Competence and the Role of Technological Expertise

By Julia Brickell

Provided in conjunction with panel presentation at Lawyers for Civil Justice Membership Meeting: December 6-7, 2018 in New York City

Technological developments continue to change the way we do business as corporate counsel. The ways in which the companies we work for utilize technology to collect data and analyze data is ever changing. The challenge for the corporate counsel is to stay sufficiently familiar with this rapidly changing environment to know when outside expertise is required. The rules of professional conduct call upon us as lawyers to recognize these moments in time when it is necessary to enlist outside help.

The breathtaking volume of data that is being generated, the speed of advances in the uses of artificial intelligence to interpret this data, and the risks associated with misuse of this data are beyond the scope of this paper. The focus is instead on the foundational ethical obligations that we have as lawyers and how those obligations come into play in this dynamic environment.

Most states have adopted some version of the 2013 ABA Model Rule 1.1 that requires a lawyer to competently represent a client. The commentary to that rule makes clear that lawyers need to be aware of "the changes in the law and its practice, including the benefits and risks associated with relevant technologies."

A lawyer's lack of awareness of "relevant technologies" creates ethics issues beyond simple competence. How can a lawyer lacking technological expertise fulfill the communication requirements of RPC 1.4 to "promptly inform the client of any decision or circumstances with respect to which the client's informed consent . . .is required by these Rules" and "reasonably consult with the client about the means by which the client's objectives are to be accomplished"? Can a lawyer support the reasonableness of a fee under RPC 1.5 when she lacks "the skill requisite to perform the legal service properly" because of unfamiliarity with the "relevant technologies" implicated in the area in which the legal advice is being given? How is a lawyer to ensure she has fulfilled her obligations under RPC 3.4 to be fair with opposing counsel by not "unlawfully obstruct[ing] another party's access to evidence or unlawfully alter[ing], destroy[ing] or conceal[ing] a document or other material" of evidentiary value if she is unfamiliar with the "relevant technologies" available to locate and isolate that evidence? How can a lawyer who lacks awareness of the "relevant technologies" fulfilled his managerial responsibilities for lawyers under supervision (RPC 5.1) and for nonlawyer assistants under supervision (RPC 5.3) that are utilizing these same technologies? And ultimately, how can a lawyer unfamiliar with the "relevant technologies" demonstrate full candor toward the tribunal (RPC 3.3) and not "knowingly . . . make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer"?

From chain of custody to retrieval and production of the intended information, choosing, using, and explaining the impact of litigation technologies requires specialized knowledge on the part of lawyers that is not taught in law school. For example, document review technologies vary greatly in what they do well, and results vary according to the expertise with which they are deployed. Mapping a client's network of data can be a complex undertaking. And for lawyers who seek safety for their client data by moving that data to the cloud, technical expertise is critical. Fully understanding the implications of cloud contracts, including the

impact on security responsibilities, requires in-depth knowledge of cloud operations. To benefit the client, meet the obligation to communicate and conform to ABA rules of competence, candor, and fairness, the lawyer is responsible for acquiring—or hiring—the knowledge to assess strengths and weaknesses of available technology, measure efficacy in implementation, and defend the chosen approach. Courts have grown weary of litigators who are ignorant of their clients' data sources. They will likely soon tire of those who use technology ineptly or not at all.

Cyber security risks are at the forefront for every company—even private law firms—given their tempting stores of confidential information. The California Attorney General's 2016 Data Breach Report, by way of example, takes the position that unless an organization is implementing the applicable CIS Top 20 Security Controls, it is not meeting reasonable security standards for protection of personal information. And for lawyers inside and out, ethical rules mandate that the lawyer maintains confidentiality of client information (ABA Model Rule 1.6). That in turn necessitates that the lawyer ensures the company has reasonable security protections. Lest it seem that a company could be too small to attract attention, consider the case of *Millard v. Doran*, brought in New York in April 2016 to recover money lost when the Millards made a nearly $2 million real estate down payment to a scammer. That person had hacked into the unsecure AOL email account of the sole practitioner representing the Millards, had read about the deal, and set up the scam. Not aware of a breach? Consider *Shore v. Johnson & Bell, LTD,* filed in federal court in Illinois in April 2016. Plaintiffs alleged that the mere existence of law firm security vulnerabilities, even in the absence of a breach, put client data at risk and constituted negligence and thus malpractice.

What is the way forward for lawyers in light of these ethical obligations and the rapid changes in technologies impacting their companies? The State Bar of California Standing Committee on Professional Responsibility and Conduct delineated a hypothetical parade of horribles for an attorney in a 2015 formal opinion. Written in the context of an e-discovery issue, the committee suggested that "the duty of competence may require a higher level of technical knowledge and ability" than the lawyer possessed, advising that the lawyer either acquire the skills, hire someone possessing the skills, or decline the engagement. The ABA Cybersecurity Handbook, which identifies technology-related security issues and suggests best practices for addressing them, includes the recommendation that "[i]f a lawyer is not competent to decide whether use of a particular technology allows reasonable measures to protect client confidentiality, the ethics rules require that the lawyer must get help, even if that means hiring an expert information technology consultant to advise the lawyer." The bottom line is that technological expertise can be hired rather than solely acquired.

Staying current on your company's and clients' technologies is vital. Ensure that inside and outside counsel have enough access to business clients to understand the technologies on which they advise. Learn the data environment. Understand the scope and content of applicable regulatory schemes and interview the owners of the data associated with those schemes. Find out if the company (or firm) has done a risk assessment. Undercover technology and data-oriented policies and procedures and learn what they mean: determine if they address current realities and if they are closely followed. Assess the training and auditing and consider if it should be enhanced to comport with that expected for an effective compliance and security program. Open lines of communication with the CIO and heads of IT and security (they are indeed different competencies). Become informed on what competencies might be required to maximize the value of a particular technology for the client. Assess the users of that technology to see if they are trained in the field that the technology seeks to address. Be systematically engaged.

When it comes to engaging outside experts, find those with deep background in the underlying activity, not just those who can use a technology. Interview the purported expert. The mark of competence

for the lawyer—the core tenet of RPC 1.1—often lies in knowing when and how to engage the right experts to address the technology challenges that inevitably lie ahead.

As we enter an era of increasingly “smart” devices and “sophisticated” tools in which opaque AI is embedded, the challenges will only grow. The privacy and security aspects of the legal inquiry grow more profound. Measuring the output of an algorithmic tool to evaluate completeness and bias requires knowledge not taught in law school. Understanding the choices engineers are making as they design products – in order to identify and advise on risk and on proper disclosures to customers – requires increasing knowledge outside the legal realm.