New York County Lawyers Association Professional Ethics Committee

Formal Opinion 749

February 21, 2017

TOPIC: A lawyer's ethical duty of technological competence with respect to the duty to protect a client's confidential information from cybersecurity risk and handling e-discovery when representing clients in a litigation or government investigation.

DIGEST: A lawyer's ethical duty of competence extends to the manner in which he provides legal services to the client as well as the lawyer's substantive knowledge of the pertinent areas of law. The duty of competence expands as technological developments become integrated into the practice of law. Lawyers should be aware of the disclosure risks associated with the transmission of client confidential information by electronic means, and should possess the technological knowledge necessary to exercise reasonable care with respect to maintaining client confidentiality and fulfilling e-discovery demands. Further, a lawyer's duty of competence in a litigation or investigation requires that the lawyer have a sufficient understanding of issues relating to securing, transmitting, and producing electronically stored information ("ESI"). The duty of technological competence required in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of technological competence if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge before performance is required, or associates with one or more persons who possess the requisite technological knowledge.

RULES OF PROFESSIONAL CONDUCT: 1.1, 1.6, 5.1, 5.3

OPINION

A lawyer has a duty to "provide competent representation to a client," which requires that the lawyer demonstrate "the legal knowledge, skill, thoroughness and preparation necessary for the representation." New York Rules of Professional Conduct ("RPCs"), RPC 1.1. A comment to the rule notes that "[t]o 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." RPC 1.1, Cmt. [8]. RPC 1.6 provides that a lawyer "shall not knowingly reveal confidential information, as defined in this RPC, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person." RPC 1.6(c) further requires a lawyer to "exercise reasonable care to prevent disclosure of information related to the representation by employees, associates and others whose services are utilized in connection with the representation."

Duty of Competence and Protection of Electronically Transmitted Client

Information

Compliance with RPC 1.6 requires that lawyers who use technology to store or transmit a client's confidential information, or to communicate with clients, use reasonable care with respect to those uses. The lawyer must assess the risks associated with the use of that technology to determine if the use is appropriate under the circumstances. *See, e.g.*, N.Y. State 709 (1998) ("an attorney must use reasonable care to protect confidences and secrets"); N.Y. City 94-11 (lawyer must take reasonable steps to secure client confidences and secrets). Lawyers should be aware that the storage and transmission of a client's confidential information electronically carries a risk of disclosure if the stored or transmitted data is hacked, or if human, software or hardware error results in an inadvertent disclosure.

Attacks on computer systems by those trying to gain confidential, proprietary, or other sensitive information for personal or political gain (including so-called "hacktivists") are reported with alarming frequency. Corporate clients have become proactive in attempting to ensure that its outside vendors—including lawyers—who have access to sensitive corporate information sufficiently protect that information from disclosure through inadvertence or cyber-attack. Individual clients are increasingly sensitive to the potential harm from widely reported data breaches, and similarly expect their lawyers to use appropriate measures to avoid unauthorized disclosure of personal data. In response to these concerns, at least 25 states have adopted rules regarding maintaining technological competence, including most recently Florida's rule, which mandates continuing legal education on the subject. *See, e.g.*, Florida Rules of Professional Conduct, Rule 6-10.3(b) (effective January 1, 2017, a Florida lawyer's CLE requirements will include 3 credit hours in approved technology programs); California Standing Committee on Professional Responsibility and Conduct Formal Op. 2015-193 (concluding that an attorney lacking the required e-discovery competence must either acquire the requisite skill before performance is required, associate with technical consultants or competent counsel, or decline the representation). An overwhelming majority of lawyers recently surveyed who work in firms ranging from solo practitioners to over 500 attorneys believed training in the firm's technology is important.[1]

Additionally, lawyers who represent clients who are located outside of New York may, in certain instances, be subject to laws in those other states that require a heightened level of protection of electronic communications. *See, e.g.*, Mass. Gen. L. Ch. 93H, 201 C.M.R. 17 (requiring, where technically feasible, the encryption of personal information stored on portable devices and personal information transmitted across public networks or wirelessly); Nevada Senate Bill 227 (amending Nev. Rev. Stat. § 597.970 and requiring that data collectors who conduct business in the state encrypt data storage devices – including computers, cell phones and thumb drives – that contain personal information that are moved outside the secured physical and logical boundaries of the data collecting

[1] "2016 Legal Technology Survey Report," American Bar Association (2016).

entity).

Lawyers must have a sufficient understanding of the technology – either directly or through associating with persons possessing such knowledge – to determine how to satisfy the lawyer's duty of reasonable care. Reasonable care will vary depending on the circumstances, including the subject matter, the sensitivity of the information, the likelihood that the information is sought by others, and the potential harm from disclosure. *See* NYCLA Op. 738 (2008) (lawyer may not ethically search metadata made available through an adversary's inadvertent disclosure of client confidential information through metadata); N.Y. State 782 (2004) (addressing the exercise of reasonable care to prevent the disclosure of client confidential information through metadata).

Duty of Competence and Electronically Stored Information

Lawyers who represent client in litigations, or in government or regulatory investigations, are well aware that often a significant aspect of the representation of the client is the collection, preservation and production of ESI. The ethical duty of competence requires an attorney to assess at the outset of e-discovery issues that may arise in the course of the representation, including the likelihood that e-discovery will or should be sought by either side, identification of likely electronic document custodians, and preservation and collection of potentially relevant ESI in an appropriate database that will permit the lawyer to search for responsive ESI during e-discovery.

A lawyer's obligations with respect to ESI will be governed by applicable state or federal law. *See, e.g.*, Fed. R. Civ. P. Rules 16, 26 and 37 (outlining a federal court litigant's obligations with respect to the presentation and production of ESI); Rules 202.12(b) and 202.70(g) of New York's Uniform Trial Court Rules (requiring all attorneys be sufficiently versed in matters relating to their client's technological systems to be competent to discuss all issues relating to electronic discovery at preliminary conferences). In addition, a lawyer's ethical duty of competence requires the lawyer to assess his or her own e-discovery skills and resources in order to meet these ESI demands. E-discovery needs in a particular matter may include (i) assessing e-discovery needs and ESI preservation procedures; (ii) identifying custodians of potentially relevant ESI; (iii) understanding the client's ESI system and storage; (iii) determining and advising the client on alternatives for the collection and preservation of ESI and associated costs; and (v) ensuring that the collection procedures, software and/or databases created will permit the lawyer to provide responsive ESI in an appropriate manner. If a lawyer lacks the requisite skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate with another attorney or expert who possess these skills. RPC 1.1 (b) & Cmt., 1,Cmt. 8.

Where a lawyer satisfies his or her duty of technological competence by associating with another lawyer or expert, the lawyer remains responsible for fulfilling the duty of

competence, and must satisfy himself or herself that the work of the associated lawyer or expert is being done properly. The lawyer must understand the pertinent legal issues and the e-discovery obligations imposed by law or court order and the relevant risks associated with the e-discovery tasks at hand, and satisfy himself or herself that everyone involved in the e-discovery process on behalf of the client is conducting themselves accordingly. *See* RPCs 5.1, 5.3.

CONCLUSION

A lawyer's ethical duty of competence extends to the manner in which he or she provides legal services to the client as well as the lawyer's substantive knowledge of the relevant areas of law. Lawyers must be responsive to technological developments as they become integrated into the practice of law. A lawyer cannot knowingly reveal client confidential information, and must exercise reasonable care to ensure that the lawyer's employees, associates and others whose services are utilized by the lawyer not disclose or use client confidential information. The risks associated with transmission of client confidential information electronically include disclosure through hacking or technological inadvertence. A lawyer's duty of technological competence may include having the requisite technological knowledge to reduce the risk of disclosure of client information through hacking or errors in technology where the practice requires the use of technology to competently represent the client.

A lawyer's competence with respect to litigation requires that the lawyer possesses a sufficient understanding of issues relating to securing, transmitting, and producing ESI. The duty of competence in a specific engagement will vary depending on the nature of the ESI at issue and the level of technological knowledge required. A lawyer fulfills his or her duty of competence with respect to technology if the lawyer possesses the requisite knowledge personally, acquires the requisite knowledge in a timely manner and before performance is required, or associates with one or more persons who possess the requisite technological knowledge. If a lawyer is unable to satisfy the duty of technological competence associated with a matter, the lawyer should decline the representation.