

Chapter 2

Technological Competence

The technological change lawyers have witnessed brings in its wake an obligation to know enough about that change and its consequences, if they can be reasonably anticipated, to have an impact upon the client's business and the representation to be provided.

Model Rule of Professional Conduct 1.1 requires that a lawyer provide competent representation to a client. "Competent representation" is said by the Rule to require "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation." *Id.*

The Comment to the Rule indicates that whether the lawyer has that skill is a function of a comparison between the nature of the matter with the lawyer's training and experience in handling such matters and the feasibility of associating with a lawyer who has "established competence" in the area. Model Rule of Professional Responsibility 1.1, Comment 1: the clear inference of the Rule is that if the lawyer cannot provide "competent representation" she should decline the representation.

For present purposes, the most significant modification of the accompanying comments is the one generated by the American Bar Association Formal Opinion in 2012. Its president had urged the committee responsible for the Rules to bring them kicking and screaming into the technological world in which lawyers live. The product was a modification of Comment 8, "Maintaining Competence," which required a lawyer to "keep abreast of changes in the law and its practice" by adding the words "*including the benefits and risks associated with relevant technology.*"

A moment's thought indicates obvious instances where lawyers' behavior can and will be tested by this standard. Take a discovery dispute where lawyer A demands a certain production of electronically stored information and lawyer B tells the judge, considering a motion to compel, that the production would be difficult and cost hundreds of thousands of dollars. If it turns out that that lawyer B's assertion is false and uttered by him without any effort to understand how available technology could have lessened those costs substantially and that knowledge was easily accessible and well known by other lawyers who litigate eDiscovery cases, lawyer B may well have violated this rule.

Take another lawyer who uses a computer or tablet to work while not in his office. He does not encrypt the contents of the device he uses, and uses as his password, giving access to the contents, “1234.” When he does log on, he uses a public network, available “for free” in a retail store or an airport, to transmit highly confidential and privileged material back to his office. If his computer or tablet is stolen, or if his transmittal is hacked and diverted to a third party, breaching the privilege, and exposing his client’s confidential trade secrets to its competitors, he may well have violated his ethical responsibility to be competent.

Recently, the Standing Committee on Professional Responsibility and Conduct issued Formal Opinion No. 2015-193 (hereafter, “Op.”) which gives the most detailed and precise advice to date on the specific ethical obligations that are imposed upon a lawyer who is involved in what the Committee calls “the handling of discovery of electronically stored information.” Op. at 1.

Presented to the Committee was a hypothetical where after an unsuccessful effort to resolve their differences concerning eDiscovery, counsel, at a judge’s direction, meet again. One lawyer proposes a joint search of the other lawyer’s client’s network, based upon a jointly agreed search term list. This lawyer offers the other a “claw back” agreement which permits the client to retrieve (“claw back”) any inadvertently produced electronically stored information that is protected by the attorney-client or work product privileges. Op. at 1. The attorney for the other side mistakenly believes that this agreement will permit his client to claw back anything it produces, whether or not privileged. He agrees with the proposal and the agreement is made a part of the judge’s case management order.

This attorney exchanges his search terms with opposing counsel and they agree that both sets will be used.

The CEO of his client, known to be a large company with an information technology department, tells the lawyer that there is no other electronically stored information in its possession that has not been already provided to counsel. The lawyer accepts that representation, assuming that the client’s IT department knows how to search a network and directs the client to make the network accessible to other side on the date agreed upon for the search, using the agreed upon search terms. The lawyer does nothing more; he never reviews what he has been given but instead assumes that the network search will not yield anything more than what the client has already given him. When the search is conducted, its results are provided him in electronic form but he does not review, apparently, because he is busy with other matters.

A week later, however, the lawyer gets a letter from opposing counsel accusing him of destroying evidence. When the attorney cannot open the electronic results of the network search, he hires an expert who accesses the data, conducts a forensic search, and tells the lawyer that: (1) potentially responsive electronically stored information has been routinely deleted from the client’s computers as part of its normal document retention (or destruction) policy, resulting in gaps in the production; (2) due to the breadth of the agreed upon search terms, both privileged and irrelevant but highly proprietary information about the client’s upcoming revolutionary product were provided to its chief competitor; (3) an IT professional, with

litigation experience, would have recognized the overbreadth of the search and prevented the retrieval of the proprietary information. *Id.* at 2.

The Committee began its Opinion by explaining that, while lawyers are required to be competent, a mere failure to act competently does not trigger discipline, unless it was reckless, intentional or repeated. Nevertheless, the reality was that nearly every case potentially involves eDiscovery. Therefore, the ethical duty of competence requires the lawyer to assess at the commencement of every case what eDiscovery issues will arise. If they will, the lawyer must assess his own skills and, if he lacks them to associate or consult with someone who has the expertise he lacks.

The Committee then specified that lawyers handling eDiscovery must have the following skills.

- (1) initially assess eDiscovery needs and issues, if any;
 - (2) implement/cause to implement appropriate ESI preservation procedures;
 - (3) analyze and understand a client's ESI systems and storage;
 - (4) advise the client on available options for collection and preservation of ESI;
 - (5) identify custodians of potentially relevant ESI;
 - (6) engage in competent and meaningful meet and confer with opposing counsel concerning an eDiscovery plan;
 - (7) perform data searches;
 - (8) collect responsive ESI in a manner that preserves the integrity of that ESI; and
 - (9) produce responsive non-privileged ESI in a recognized and appropriate manner
- Op. at 3–4.

The lawyer failed in obvious ways to meet these obligations. He began by failing to evaluate how eDiscovery would impact discovery in the case and his own capabilities to meet the consequential obligations that would be imposed upon him if there was to be eDiscovery. This attorney, however, made no assessment of either, and made the situation worse by not consulting with another attorney or eDiscovery expert prior to reaching the agreements he did. Similarly, he agreed to search terms without any understanding of how that could operate to permit the disclosure that occurred.

He also failed abysmally to instruct his client in how to conduct or supervise the search of the network. He did not pre-test the search terms or review the client's data before the search, seeming only to rely on his assumption that client would know what to do, and, in any event, that the claw back agreement would protect his client from the disclosure that occurred.

According to the Committee, all of this could and should have been avoided by the lawyer's consulting those who knew what he did not who could have informed him and steered him away from his improvident agreement and helped him to structure the search to avoid the consequences this search engendered.

The Legal Technology Guidebook

Williams, K.; Facciola, J.M.; McCann, P.; Catanzaro, V.M.

2017, XI, 142 p. 3 illus. in color., Hardcover

ISBN: 978-3-319-54522-6