Competency, Confidentiality, Conflicts, and Technology

David Hricik
Professor of Law
Mercer University School of Law

33rd Annual Technology Law Conference
May 2020

TABLE OF CONTENTS

1. The Baseline Ethical Duties of Competency and Confidentiality

Most state rules are similar to the American Bar Association Model Rules of Professional Conduct (the "Model Rules"). The Model Rules impose an affirmative obligation on lawyers to be competent. Model Rule 1.1. States generally require lawyers to maintain all information relating to the representation of a client, unless disclosure is permitted or required. *See* Model Rule 1.6. Most often, this includes not just privileged information but all information gained in the professional relationship, whatever its source. *E.g., id.*.

While the duties of competency and confidentiality have long existed and indeed exist in the common law in the form of the standard of care, the technological changes driven inexorably by Moore's Law has made it easier for lawyers to violate these duties, both because technology is advancing rapidly and because information can be shared much more easily. Today, a lawyer can inadvertently send confidential information to opposing counsel – or a reporter – not just instantly, but in such vast amounts that would have been impossible to have done just a few years ago. One gigabyte of information translates to a small truck load of paper. *See* Doug Austin, *eDiscovery Best Practices: Perspective on the Amount of Data Contained in 1 Gigabyte* (March 5, 2012) (available at https://cloudnine.com/ediscoverydaily/electronic-discovery/ediscovery-best-practices-perspective-on-the-amount-of-data-contained-in-1-gigabyte/).

Reflecting the significance of technology to the practice of law and these core duties, several years ago, the ABA amended the Model Rules to specifically identify the need for lawyers to be competent with technology and to be aware of the risks that the use of technology poses to client confidences. For example, the ABA added Model Rule 1.6(c), which provides in full: "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." It also added a comment emphasizing the scope of this duty and its importance:

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to

> forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].
>
> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Model Rule. 1.6, cmts. 18-19. *See also* Model Rule 1.8, cmt. 8 ("a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology….").

This no doubt explains why that, as of mid-2018, thirty-one states had adopted the ABA's amendments requiring technical competency. *See* Robert Ambrogi, *31 States Have Adopted Ethical Duty of Technology Competence*, LawSites (Mar. 16, 2015) (available at https://www.lawsitesblog.com/2015-01/11-states-have-adopted-ethical-duty-of-technology-competence.html).

2. Anticipation of Litigation and the Duty of Preservation.

Model Rule 3.4 emphasize the lawyer's obligation not to obstruct access to evidence, emphasizing that a lawyer shall not "unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value." A comment to Georgia's counterpart emphasizes the technological reach of the rule, stating in part:

> Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for purpose of impairing its availability in a pending

Title search: Competency, Confidentiality, Conflicts, and Technology

Also available as part of the eCourse
Answer Bar: Maximizing Technology in Your Law Practice

First appeared as part of the conference materials for the
33rd Annual Technology Law Conference session
"Competency, Confidentiality, Conflicts, and Technology"