Mound Cotton Wollan & Greengrass LLP
COUNSELLORS AT LAW

Law360

ABA Remote Work Guide Raises Bar For Atty Tech Know-How

By Jennifer Goldsmith and Barry Temkin
April 5, 2021, 3:19 PM EDT

On March 10, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued an opinion that contains timely guidance on ethical issues specific to working remotely, which many lawyers have found themselves doing during the coronavirus pandemic.[1]

ABA Ethics Opinion 498 outlines ethical issues specific to remote law practice, including lawyers' ethical duties of competence, confidentiality and supervision, which are imposed by Rules 1.1, 1.6, 5.1 and 5.3 of the ABA Model Rules of Professional Responsibility.

The new ethics opinion actually contains a relatively modest amount of new information, and synthesizes principles that have been articulated by both the ABA and state bar ethics committees over the past several years, including New York County Lawyers Association Formal Opinion 754-2020[2] and California State Bar Formal Opinion No. 2020-203,[3] both of which provide helpful guidance for lawyers seeking to maintain traditional ethical values of confidentiality and competence in an era of rapid technological change.

As will be seen, the concept of professional competence increasingly encompasses technological knowhow. Twenty-first century technology is quite literally becoming mandatory training for lawyers.

Duty of Confidentiality

Perhaps the most important obligation for lawyers working remotely is the duty of confidentiality under Rule of Professional Conduct 1.6, which provides that lawyers "shall not reveal information relating to the representation of a client," and must "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[4]

Rule 1.6 is a disciplinary rule that is broader than the attorney-client privilege, which is an evidentiary principle. Instead, Rule 1.6 broadly applies to "information relating to the representation of a client," which often includes information that the client has requested to keep confidential, or which might be embarrassing to the client, regardless of whether it emanated from an attorney-client communication.[5]

Lawyers' duty of competence is embodied in Rule 1.1, which provides that a "lawyer shall provide competent representation to a client."[6] New York's counterpart is similar, and further provides, in a comment, that: "To maintain the requisite knowledge and skill, a lawyer should … 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."[7]

Lawyers working remotely may confront more confidentiality challenges than were posed in the relatively controlled and sterile office environment. Remotely working lawyers may find it difficult to maintain the security or integrity of their working space, as other family or household members may pass through or even share the same room.

Portions of client meetings or depositions might be audible to other household members in different rooms. Parents may need to leave a screen unattended in order to assist a child with school or homework, or to prepare a meal, thereby potentially exposing confidential information.

Moreover, other family members may have access to lawyers' devices, which could be left unattended in the home. Such devices should be fully encrypted and subject to dual factor authentication in order to be sure they can be secured.
The ABA has recommended that lawyers adhere to a panoply of measures to preserve the confidentiality of client information when working remotely, including:

- Avoiding use of unsecured Wi-Fi systems when accessing or transmitting confidential client information;
- Utilizing virtual private networks that encrypt information and shield online activity from third parties;
- Implementing multifactor authentication to access firm hardware and networks;
- Ensuring that computer systems are up to date, with appropriate firewalls and anti-malware software;
- Backing up data stored remotely;
- Ensuring that portable devices can be remotely scrubbed;
- Requiring strong passwords to protect data access in devices;
- Creating a written work-from-home protocol that specifies procedures to safeguard confidential information; and
- Training employees on security protocols, data privacy and confidentiality policies.[8]

In addition, lawyers conducting meetings, depositions or court proceedings via Zoom, Microsoft Teams or other videoconferencing software should be cognizant of their risks and limitations, and "should review the terms of service (and any updates to those terms) to ensure that using the virtual meeting or videoconferencing platform is consistent with the lawyer's ethical obligations."[9]

In a relatively new development, the ABA also advises lawyers to review the terms of service applicable to hardware devices and software systems "to assess whether confidentiality is protected,"[10] a measure that relatively few lawyers have hitherto followed.

As mentioned, the ABA committee also recommends that lawyers secure the integrity and security of their internet connection by using virtual private networks. In addition, the ethics committee recommends unplugging or disabling the listening capacity of Amazon Echo, Alexa, Apple Homepod or other smart speakers or virtual assistants, in order to prevent electronic eavesdropping on confidential client communications.[11]

Thus, lawyers who use electronic smart speakers — even for taking dictation, scheduling meetings or putting on background music — should be careful to disable the listening aspects of these devices in order to preserve client confidentiality.[12]

Finally, law firms should ensure that any portable devices can be remotely wiped, so that confidential client information can be erased in the event that a laptop or smartphone is stolen, or inadvertently misplaced.

Analysis and Implications

As mentioned, ABA Ethics Opinion 498 links the lawyer's duty to maintain client confidences with the overall ethical obligation of competence under Rule 1.1, thereby raising the stakes for lawyers who might have previously lagged in technology.

While Opinion 498 is neither groundbreaking nor earth-shattering, it should be viewed as part of a larger movement by which lawyers are being exhorted to develop competence in 21st century technology, on pain of professional discipline.

Opinion 498 wisely builds on principles discussed in earlier opinions, including an August 2020 NYCLA opinion and a September 2020 opinion of the California State Bar Association, which considers a lawyer's ethical obligations with respect to unauthorized access by third parties to electronically stored confidential information.[13]
The California State Bar Association wrote in that opinion that law firms should take reasonable steps to secure their electronic data storage systems from the risk of unauthorized access to client confidential information, and should provide for remote lockdown and scrubbing in the event a portable device is lost or compromised.

In the event of a breach, "lawyers have an obligation to conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."

Florida has gone even further, recently adopting a rule requiring all Florida lawyers to take three continuing legal education credit hours on technology in each three-year cycle, including use of encryption and other technology to preserve client confidential data.[14]

The cumulative effect of these recent ethics opinions is to elevate the bar for technological competence for lawyers.

Law firms that are subjected to cyber incidents, whether malicious or inadvertent, will find themselves scrutinized under these new developing standards, at risk of potential professional discipline or claims made by disgruntled clients whose confidential information was exposed or exfiltrated.

A lawyer whose data was penetrated may be expected to answer questions about compliance with Opinion 498. And while the ethics rules themselves eschew their use as the basis for civil lawsuits,[15] many courts have permitted their admissibility, and creative plaintiffs lawyers may seek to impose new standards based upon 21st century technology.

Moreover, whether or not used to fashion a lawsuit, Opinion 498 makes clear that attorneys working remotely must make reasonable efforts to secure client information as part of their obligation of confidentiality. Accordingly, lawyers who wish to keep up with the times — and avoid claims — should take note and learn from this new opinion.

Jennifer Goldsmith is vice president of professional liability claims at Ironshore Inc., a part of Liberty Mutual Insurance Co.

Barry Temkin is a partner at Mound Cotton Wollan & Greengrass LLP, an adjunct professor at Fordham University School of Law, and former chair of the New York County Lawyers Association Committee on Professional Ethics.

[1] ABA Formal Opinion 498 (March 10, 2021), https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf.

[2] https://www.nycla.org/pdf/NYCLA%20Op.%20754-2020%20-%20Ethical%20Obligations%20when%20Lawyers%20Work%20Remotely.pdf.

[3] https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/Formal-Opinion-No-2020-203-Data-Breaches.pdf.

[4] RPC 1.6(c); ABA Ethics Op. 498, at 2.

[5] See, e.g. New York Rule of Professional Conduct 1.6, https://www.nycourts.gov/ad3/AGC/Forms/Rules/Rules%20of%20Professional%20Conduct%2022NYCRR%20Part%201200.pdf.

[6] ABA Model Rule 1.1, Competence.

[7] New York Rules of Professional Conduct 1.1, comment 8.

[8] ABA Eth. Op. 498, at 6-7.

[9] ABA Eth. Op. 498, at 5.

[10] ABA Eth. Op. 498, at 4.

[11] ABA Eth. Op. 498, at 6.

[12] See, Barry Temkin and Brenda Dorsett, Lawyers' Digital Assistants Raise Ethics, Privacy Concerns, Law360 (May 23, 2019), https://www.law360.com/articles/1161964/lawyers-digital-assistants-raise-ethics-privacy-concerns.

[13] California State Bar Ethics Opinion 2020-203, https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/Formal-Opinion-No-2020-203-Data-Breaches.pdf.

[14] FL Rule 6-10.3(b), https://floridabar.org (requiring three credit hours of CLE in "approved technology programs" for every three-year/33 credit cycle).

[15] See, e.g., New York Rules of Professional Conduct, comment 12 ("Violation of a Rule should not itself give rise to a cause of action against a lawyer nor should it create any presumption in such a case that a legal duty has been breached.").