Technology Competence is Now an Ethical Issue

By Kirsten H. Spira and Rebekah H. Lee

Kirsten Spira is partner in Jenner & Block LLP, Chair of the Los Angeles County Bar Association's Professional Responsibility and Ethics Committee and a State Bar certified Legal Malpractice Specialist. Rebekah Lee is a law student at The University of California, Berkeley, School of Law, class of 2022. The opinions expressed here are their own.

In February 2021, California became the 39th state to adopt a duty of technology competence when it added Comment 1 to Rule 1.1 ("Competence") of the California Rules of Professional Conduct. That comment explains that the duty of competence set forth in Rule 1.1 requires that all California attorneys "keep abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology."[1] This change places California in sync not only with the majority of states, but also with the American Bar Association ("ABA"), whose Model Rules of Professional Conduct require attorneys to keep up with the ever-evolving uses of technology in the practice of law.[2]

Even before California formally recognized a duty of technology competence as part of the competence requirement, the state and its local bar organizations strongly recommended that attorneys understand the basic risks and benefits of technology to ensure client confidentiality and virtual safety. But what qualifies as technology competence remains unclear, as the general language in Rule 1.1 leaves ample room for interpretation. Prior to the adoption of Rule 1.1, the State Bar of California's Standing Committee on Professional Responsibility and Conduct ("COPRAC") suggested that an attorneys' duty of competence required them to assess, among other things, their ability to assess the level of security afforded by technology, the degree of sensitivity of information, and the appropriate steps that they must take to ensure that client information remains secure.[3] When addressing attorneys' ethical duties in handling discovery of electronically stored information ("ESI"), COPRAC took the position that "a lack of technological knowledge . . . may render an attorney . . . incompetent to handle certain litigation matters involving e-discovery."[4] Similarly, in 2012, the San Diego County Bar Association ("SDCBA") released an opinion stressing the vast amount of information that is digitally stored and the new burdens of competence that come with technological advancements.[5]

The duty of technology competence is more relevant now than ever, as the pandemic has forced many attorneys into a completely virtual workspace. Nearly eight months after

[1] Cal. Rules of Professional Conduct, rule 1.1, cmt. 1.
[2] MODEL RULES OF PROF'L CONDUCT r. 1.1 (AM. BAR ASS'N 2021).
[3] Cal. State Bar Formal Opn. No. 2010-179.
[4] Cal. State Bar Formal Opn. No. 2015-193.
[5] San Diego County Bar Assn. Formal Opn. No. 2012-1 (2012).

California's stay-at-home order went into effect, the Orange County Bar Association ("OCBA") emphasized the need for technology competence as a part of attorneys' ethical duties during COVID-19.[6] The OCBA stated that attorneys using their own Wi-Fi and Zoom accounts for videoconferencing must do so effectively and with the risks of those technologies in mind.[7] It encouraged attorneys who lack the technical competence to do so to seek help from someone who does.[8]

In addition to the guidance set forth by various state organizations, other legal publications, such as JD Supra and the ABA Journal, laid out their own opinions of what technology competence might entail. After California officially recognized a duty of technology competence, JD Supra suggested that attorneys should demonstrate general competence in video conferencing tools, secure file transfer, research and brief-writing tools, and word-processing and email tools.[9] Similarly, the ABA Journal encouraged all attorneys practicing virtually to install security-related updates and use strong passwords, antivirus software, encryption, and VPNs.[10]

While the scope of the duty of technology competence is far from settled, one thing is certain: the use of technology in the practice of law is here to stay. The most recent legal blog posts and opinions about the importance of keeping abreast with technology during and after the pandemic are not overdramatic warnings. As of March of 2021, Zoom had 300 million participants using its videoconferencing platform and over 450,000 business customers—including many (if not all) of America's major law firms.[11] The true number of people and businesses using videoconferencing tools is even higher considering alternative platforms such as Skype and Microsoft Teams each have several million regular users as well.[12]

With increased use of videoconferencing tools comes brand new risks that can compromise attorneys and their clients. Zoom bombing, a phenomenon where uninvited participants intrude meetings, has become commonplace.[13] Intruders often share inappropriate images, comments, and other offensive content. Many of these incidents could be prevented with

---

[6] Jeremy G. Suiter, *November 2020 Ethically Speaking – Complying With Your Ethical Duties During COVID-19*, ORANGE CTY. BAR ASSN., https://www.ocbar.org/All-News/News-View/ArticleId/3959/November-2020-Ethically-Speaking-Complying-With-Your-Ethical-Duties-During-COVID-19.
[7] *Id.*
[8] *Id.*
[9] Matthew Gurnick, *California Bar Requires Attorneys to Embrace Technology*, JD SUPRA, (Mar. 30, 2021), https://www.jdsupra.com/legalnews/california-bar-requires-attorneys-to-5727418/.
[10] David L. Hudson Jr., *New ABA Ethics Opinion Addresses Professional Responsibilities of Virtual Practice*, ABA JOURNAL (Mar. 10, 2021, 10:27 AM), https://www.abajournal.com/news/article/ethics-opinion-addresses-professional-responsibilities-of-virtual-practice.
[11] Brian Dean, *Zoom User Stats: How Many People Use Zoom in 2021?*, BACKLINKO.COM (Mar. 10, 2021), https://backlinko.com/zoom-users.
[12] Jordan Novet, *Skype is Still Around – It's Just Been Upstaged by Microsoft Teams*, CNBC (Oct. 10, 2020, 10:30 AM), https://www.cnbc.com/2020/10/10/skype-upstaged-by-microsoft-teams.html#:~:text=(In%20a%202019%20blog%20post,40%20million%20concurrent%20users.%E2%80%9D)
[13] https://www.nytimes.com/2020/04/09/technology/zoom-security.html.

simple security measures. For example, when hosting a videoconference meeting, attorneys should remember to use a meeting password, instruct attendees to refrain from circulating the meeting link, or consider using the "waiting room" feature that allows meeting hosts to permit or deny access to the meeting.

Chat features on videoconferencing tools pose another potential security risk. Attorneys should remember that messages that are not manually directed to another participant can be viewed by all attendees. Platforms like Zoom and WebEx allow meeting hosts to save transcripts of these chats for future reference.[14] Even the most basic features of videoconferencing tools can undermine confidentiality and negatively affect attorneys' ability to do their jobs effectively. Attorneys should be mindful of whether they are on mute or video. Disabling the audio and video functions as the default setting or habitually checking them at the beginning of a meeting can help attorneys maintain privacy, security, and sometimes even professionalism. Attorneys using their videoconferencing tools for personal and professional purposes should also be mindful of their virtual name tags.

In addition to the new growing popularity of videoconferencing tools, attorneys should continue to exercise caution while using everyday technology like email and shared cloud drives. Inadvertent email transmissions are commonplace, so much so that the State Bar of California adopted a rule about it.[15] To avoid this mistake, attorneys should consider writing the body of their message before entering a recipient's email address. Attorneys may also want to enable an "unsend" feature to quickly undo accidental transmissions. While none of these features or tips are new, they are effective in preventing unintentional breaches of confidentiality and help attorneys abide by their duty of technology competence.

Similarly, attorneys who work in the "cloud" can exercise simple precautions when uploading documents or other data into a potentially shared space. While platforms may vary in their security features, attorneys should question their use of the cloud for highly sensitive information. If it is absolutely necessary, attorneys should consider using encryption, pass codes, and access permission requests when using the cloud. And if an attorney is unfamiliar with these security and privacy features, they should obtain help from someone who is.

While technology has provided attorneys with tools to work faster and more efficiently, it has also created a new set of technical and ethical challenges. California's adoption of a duty of technology competence will play a critical role in forcing attorneys to ensure that they are equipped to handle these challenges.

---

[14] ZOOM, https://support.zoom.us/hc/en-us/articles/115004792763-Saving-in-meeting-chat#h_f352de7d-303d-4f5b-b791-928aebb8d41e (last visited Jul. 9, 2021).
[15] *See* Cal. Rules of Professional Conduct, rule 4.4.