THERE'S NO PLACE LIKE HOME: ETHICAL CONSIDERATIONS FOR LAWYERS CONTINUING TO WORK REMOTELY AND USE SOCIAL MEDIA

Date: 22 June 2021

Investigations, Enforcement, and White Collar Alert

By: Clifford C. Histed

There's no place like home. Now, more than any time in history, lawyers are working from home, supervising other lawyers who are also working remotely, and weighing options to integrate this change permanently in a post-pandemic world. Lawyers continue advising clients who are also working remotely and supervising others. According to PwC's U.S. Remote Work Survey published in January 2021, “remote work has been an overwhelming success for both employees and employer” and less than twenty percent of executives say that they want to return to the office environment as it was before the COVID-19 pandemic.[1] Seventy-five percent of executives believe that at least half of their employees will be back in the office by July 2021, while sixty-one percent of employees expect to spend half of their time in the office by that time.[2] While a “return to normal” is uncertain, one thing is certain—for the “foreseeable future” lawyers will spend a substantial amount of their time working from home. This article addresses some ethical implications of this important shift in the practice of law.

I. PROTECTING THE CONFIDENTIALITY OF CLIENT INFORMATION

On 10 March 2021, the American Bar Association's Standing Committee on Ethics and Professional Responsibility issued Formal Opinion 498 called “Virtual Practice” (the Opinion). The Opinion broadly addresses the areas of lawyer competence, confidentiality of client information, and supervision. We focus here on confidentiality and supervision.

Under Model Rule of Professional Conduct 1.6, lawyers have a duty of confidentiality to their clients and “shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [an enumerated exception].”[3] Of course this means that, “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.”[4] Relatedly, and as discussed in the Opinion, lawyers with managerial authority have ethical obligations to establish policies and procedures to ensure compliance with the ethical rules and a duty to make reasonable efforts to ensure that subordinate lawyers and non-lawyer assistants comply with the applicable Rules of Professional Conduct.[5] Specifically, lawyers must “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.*”[6] The duty to supervise non-lawyers extends to those outside the law firm.[7] Therefore, the duties described above apply to lawyers and also to the junior lawyers, experts, investigators,

©2005-2026 K&L Gates LLP. All Rights Reserved.

consultants, and non-lawyer assistants who support a lawyer's practice. With these principles in mind, we now examine certain issues specific to the remote practice of law.

A. Client Confidentiality and Virtual Meeting Platforms

1. Securing Videoconferences

The Opinion makes clear what probably is intuitive—"any client-related meetings or information should not be overheard or seen by others in the household, office, or other remote location, or by third parties who are not assisting with the representation, to avoid jeopardizing the attorney-client privilege and violating the ethical duty of confidentiality."[8] In March 2020, the FBI issued a press release warning the public that it had received several reports of "Zoom-bombing" in which outsiders intruded into Zoom classroom settings.[9] The FBI recommended taking these steps to mitigate teleconference hijacking:

- Do not make meetings or classrooms public.
- Require a meeting password or use other features that control the admittance of guests.
- Do not share a link to a teleconference on an unrestricted, publicly available social media post.
- Provide links only to specific people.
- Manage screen sharing options. In Zoom, change screen sharing to "host only."

These recommendations are good starting points for lawyers for whom protecting confidential client information is an ethical imperative. Recognizing this, the Pennsylvania Bar Association Committee on Legal Ethics and Professional Responsibility incorporated the FBI's guidance into its own formal opinion.[10] Perhaps lawyers should do even more. Here we present additional guidance on protecting client information during video conferences:

- Use virtual background features if your work environment contains information that others should not see, including notes and calendars on the wall, or labeled files.
- Before screen sharing, close all applications, emails, and documents that you will not use during the session to ensure that they are not visible during the presentation.
- Before screen sharing, turn off system notifications so that they do not pop up on your computer screen during your conference.
- Always assume that you have a hot microphone. If you have a connected monitor and you close your laptop, your microphone may still be on.
- Take great care to avoid being overheard. Children and teenagers often pay attention more often than we give them credit for and many of them share information learned in the home on social media.
- Do not have confidential conversations in the vicinity of smart home listening devices. Big Brother is listening.
- Do not reuse meeting access codes.
- Monitor participant lists for unknown attendees, and do not be shy about asking people to identify themselves. Some platforms allow the host to lock the meeting after it begins. Do that.

©2005-2026 K&L Gates LLP. All Rights Reserved.

- Turn off any “join before the host” function so that unwelcome participants cannot join before the meeting begins.
- Remember, not every meeting needs to be a video conference. Telephone calls are not yet obsolete.

2. Recording Videoconferences

Hosts should always inform attendees in advance or at the start of the meeting if they are going to record the meeting. In some states, recording a conversation without the consent of all of the meeting participants can be a criminal offense. Hosts may also choose to explicitly require consent to be recorded via Zoom. Hosts should consider giving participants the option to participate without having their image or voice recorded by allowing them to mute their microphone and turn off their camera, and submit questions using a chat function. Finally, because hosts can start and stop recording at any time, they should consider recording only those parts of a meeting that truly must be recorded and leaving the rest of the meeting unrecorded.

B. Client Confidentiality and Social Media Platforms

Lawyers comment on legal topics in many different formats, including through articles made available online (like this article) and webinars and other presentations (like the webinar for which this article was prepared). Lawyers who communicate about legal topics in public commentary must take great care to protect the confidences of their clients. As noted above, and worth repeating here, a lawyer “shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by [an enumerated exception].”[11] Rule 1.6 “applies not only to matters communicated in confidence by the client but also to *all information relating to the representation, whatever the source*.”[12] Thus, the scope of protection provided by Rule 1.6 is far wider than the scope of the attorney-client privilege. Unless one of the exceptions found in Rule 1.6 applies, a lawyer is prohibited from commenting publicly, including through social media platforms, about any information related to a representation. Depending on the circumstances, even the identity of a client may be protected under Rule 1.6.[13] For example, even information about a client's representation found in a public court order is not exempt from the scope of Rule 1.6 because the duty of confidentiality extends to information related to a representation regardless of its source, even if others may be aware of or have access to such knowledge.[14] “Rule 1.6 does not provide an exception for information that is 'generally known' or contained in a 'public record.'”[15] ABA Formal Opinion 480 forcefully and clearly sums up the issue in this way:

At least since the adoption of the ABA Canons of Ethics, the privilege of practicing law has required lawyers to hold inviolate information about a client or a client's representation beyond that which is protected by the attorney-client privilege. Indeed, lawyer ethics rules in many jurisdictions recognize that the duty of confidentiality is so fundamental that it arises before a lawyer-client relationship forms, even if it never forms, and lasts well beyond the end of the professional relationship. It is principally, if not singularly, the duty of confidentiality that enables and encourages a client to communicate fully and frankly with his or her lawyer.[16]

Whether speaking in a private setting or a public one, and whether speaking virtually or on a social media platform, the duty of protecting client confidences is paramount.

©2005-2026 K&L Gates LLP. All Rights Reserved.

II. USE OF SOCIAL MEDIA IN DISCOVERY AND INVESTIGATIONS

Social media evidence has become a central feature of modern litigation, just as social media affects virtually every other aspect of our lives. Lawyers can summon and use social media instantly with smart phones—devices the Supreme Court recently called "almost a feature of human anatomy."[17] Given social media's pervasiveness in our culture, and the frequency with which people use it compared to other forms of communication, social media evidence is a broader and deeper trove of courtroom evidence than has ever been available before.[18] But lawyers must be careful in how they obtain and use information from social media platforms.

Before there was social media, and even before the Internet, lawyers would have been wise to advise their clients not to talk about their cases, and to preserve evidence, and not to contact parties and witnesses by pretext.[19] These principles still hold true, and are embodied in these twelve helpful tips gleaned from the ABA Center for Professional Responsibility and numerous state and local bar ethics committees:

1. Attorneys may not contact a represented person through social networking websites.
2. Attorneys may not contact a party or a witness by pretext. This prohibition applies to other parties and witnesses who are either identified as a witness for another party or are witnesses the lawyer is prohibited from contacting under the applicable Rules of Professional Conduct.
3. Attorneys may contact unrepresented persons through social networking websites, but may not use a pretextual basis for viewing otherwise private information on those websites.
4. Attorneys may advise clients to change the privacy settings on their social media page. In fact, lawyers *should* discuss the various privacy levels of social networking websites with clients, as well as the implications of failing to change these settings.
5. Attorneys may instruct clients to make information on social media websites "private," but may not instruct or permit them to delete/destroy relevant photos, links, texts, or other content, so that it no longer exists. This rule is no different from the obligation not to destroy physical evidence, i.e., evidence is evidence, regardless of how it was created.
6. Attorneys must obtain a copy of a photograph, link, or other content posted by clients on their social media pages to comply with requests for production or other discovery requests.
7. Attorneys must make reasonable efforts to obtain photographs, links, or other content about which they are aware if they know or reasonably believe it has not been produced by their clients.
8. Attorneys should advise clients about the content of their social networking websites, including their obligation to preserve information, and the limitations on removing information.
9. Attorneys may use information on social networking websites in a dispute or lawsuit. The admissibility of the information is governed by the same standards applied to all other evidence.
10. Attorneys may not reveal confidential client information in response to negative online reviews without a client's informed consent. Thus, responses should be proportional and restrained.
11. Attorneys may review a juror's Internet presence.

©2005-2026 K&L Gates LLP. All Rights Reserved.

12. Attorneys may connect with judges on social networking websites provided the purpose is not to influence judges in carrying out their official duties.[20]

Social media evidence is both an evidentiary bounty and an ethics minefield. Careful lawyers will find great opportunity, and careless lawyers will find jeopardy.

This article is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author and not necessarily those of K&L Gates clients.

FOOTNOTES

[1] *U.S. Remote Work Survey*, PwC (January 12, 2021) https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html.

[2] *Id.*

[3] Model Rules of Professional Conduct § 1.6(a) (2020) (AM. BAR ASS'N).

[4] Model Rules of Professional Conduct § 1.6(c) (2020) (AM. BAR ASS'N).

[5] ABA Comm. on Ethics & Pro. Resp., Formal Op. 498 (2021), p. 3.

[6] Model Rules of Professional Conduct § 1.6 cmt. [18] (2020) (AM. BAR ASS'N) (emphasis added).

[7] *See* ABA, supra note 6, p. 4.

[8] *Id.*, p. 5.

[9] Kristen Seterea, *FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic*, FBI (March 30, 2020) https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[10] Pennsylvania Bar Ass'n Comm. on Legal Ethics and Prof'l Responsibility, Formal Op. 2020-300 (2020).

[11] Model Rules of Professional Conduct § 1.6(a) (2020) (AM. BAR ASS'N).

[12] Model Rules of Professional Conduct § 1.6 cmt. [3] (2020) (AM. BAR ASS'N) (emphasis added).

[13] *See* ABA Comm. on Ethics & Professional Responsibility, Formal Op. 480 (2018), p. 2, note 7 (collecting ethics opinions from several jurisdictions).

[14] *Id.*, p. 3.

[15] *Id.*, p. 4.

[16] *Id.*, p. 5 (internal citations omitted).

[17] *United States v. Carpenter*, 585 U.S.—, 138 S. Ct. 2206 (2018).

[18] *See, generally*, Clifford C. Histed, Desiree F. Moore, and Daniel Charles (DC) V. Wolf, *Bot or Not? Authenticating Social Media Evidence at Trial in the Age of Internet Fakery*, K&L GATES (November 10, 2020) https://www.klgates.com/Bot-or-Not-Authenticating-Social-Media-Evidence-at-Trial-in-the-Age-of-Internet-Fakery-

©2005-2026 K&L Gates LLP. All Rights Reserved.

11-10-2020.

[19] *See* Daniel J. Siegel, *Ethics Corner: 12 Rules for Ethically Dealing with Social Media*, AM. BAR ASS'N, BUSINESS LAW TODAY, (February 16, 2017) https://www.americanbar.org/groups/business_law/publications/blt/2017/02/ethics_corner/.

[20] *Id*.

KEY CONTACTS



CLIFFORD C. HISTED
PARTNER

CHICAGO
+1.312.807.4448
CLIFFORD.HISTED@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.