CHAPTER FIVE

THE ETHICS OF VIRTUAL LAWYERING

Vincent J. Syracuse, Esq.
Maryann C. Stallone, Esq.
Alyssa C. Goldrich, Esq.*

* Vincent J. Syracuse, Esq. is the founder of Tannenbaum Helpern Syracuse & Hirschtritt LLP's ("Tannenbaum Helpern") Litigation & Dispute Resolution practice and is currently its Co-Chair. Mr. Syracuse has authored the monthly Attorney Professionalism Forum in the NYSBA Journal since 2012 and has chaired NYSBA's program on ethics and civility for more than 20 years. He is a member of the Executive Committee of NYSBA's Commercial and Federal Litigation Section and former Chair of that Section, as well as a member of NYSBA's Committees on Attorney Professionalism and Continuing Legal Education.

Maryann C. Stallone, Esq. is a Partner and commercial litigator in Tannenbaum Helpern's Litigation & Dispute Resolution practice. Ms. Stallone co-authors the monthly Attorney Professionalism Forum in the NYSBA Journal and regularly lectures and writes on the topics of restrictive covenants, business break-ups, professional responsibility and cybersecurity.

Alyssa C. Goldrich, Esq. is an Associate in Tannenbaum Helpern's Litigation and Dispute Resolution practice and Co-Chair of the New York County Lawyers Association's Supreme Court Committee. Ms. Goldrich also co-authors the monthly Attorney Professionalism Forum in the NYSBA Journal.

[5.0] I. INTRODUCTION

The ubiquity of modern technology has made it possible, and in many cases, relatively easy, for lawyers to practice law from remote locations away from their "brick and mortar" offices. While innovations in technology have, to be sure, eliminated many of the practical challenges historically faced by lawyers when working remotely, there are many ethical challenges that still accompany the remote practice of law.

[5.1] II. TAKING MEASURES TO PROTECT CONFIDENTIALITY

One of the most fundamental challenges that lawyers face when working from a remote location is the need to protect client confidences. Rule 1.6 of New York's Rules of Professional Conduct (RPC) governs a lawyer's duty of confidentiality, which applies in all settings and at all times. RPC 1.6(a) states that "a lawyer shall not knowingly reveal confidential information . . . or use such information to the disadvantage of a client." Confidential information is defined as "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."[1] So as to not run afoul of an attorney's duty of confidence to clients, attorneys should be wary of falling into the trap of adopting casual practices when working at home.

When working in close proximity to other members of the household, attorneys must take extra precautions to safeguard client confidences. For example, an attorney's "remote office" should be as autonomous as possible. It is best practice to avoid working in commonly used areas of the home where you often do not have the ability to close a door, such as the kitchen table or the living room. However, if the attorney's personal circumstances do not permit such autonomy, it is important to set clear boundaries with children, partners and other members of the household as to how the attorney's workspace and work files should be treated. For example, attorneys should try to take confidential client-related communications behind, if possible, a locked door, and let their family members know in advance that they should not be disturbed. Attorneys should also take practical steps to secure their work devices such as not letting children or significant others use or access work devices for personal use and setting up strong and unique passwords for those devices (i.e., laptops,

1 *See* RPC 1.6.

smartphones, tablets, etc.). Those devices should also be programmed to implement a screensaver and require a password after a certain period of time has lapsed that the attorney has not been using that work device. To the extent practical, attorneys may also want to consider having a private, password-protected Wi-Fi network specifically for professional work separate and apart from their home Wi-Fi. Attorneys also may want to consider investing in a locked filing cabinet to store sensitive client information. If an attorney is unable to obtain locked storage, attorneys should endeavor to store work-related materials somewhere only the attorney can access them. Sensitive client information should not be left on the kitchen table or counter for everyone to see.

Additionally, before communicating with clients via email or phone, lawyers should take time to consider their surroundings. This includes considering whether someone might overhear the attorney's conversation with the client, including by voice-enabled smart speakers such as Amazon Alexa. According to a 2019 report by the Consumer Intelligence Research Partners, there were 76 million listening assistants installed in the United States, and the trend is continuing to grow exponentially.[2] The listening function of these devices is typically triggered by a "wake-up word" which tells the device to listen to, and often record, whatever follows the trigger word. However, there is evidence to suggest that voice assistants can be triggered by something other than the wake-up word, which can put confidential client information in serious jeopardy of being exposed.[3] While Google and Amazon continue to insist that inadvertent triggering of a listening assistant is rare, it is best to play it safe and err on the side of extreme caution, particularly when dealing with sensitive client information outside of a law firm's office. Therefore, it is a best practice to remove at home listening devices situated near an attorney's home workspace.

[5.2] III. BECOMING PROFICIENT IN THE TECHNOLOGY NEEDED TO PERFORM LEGAL SERVICES FOR CLIENTS

In today's world, the documents and information relevant to the practice of law often exist in digital form and are stored on cloud-based platforms that cannot be located or navigated without a basic understanding

2 Kerrie Spencer, *Why Lawyers Should Mute Alexa*, Bigger Law Firm, April 24, 2020, https://www.biggerlawfirm.com/why-remote-lawyers-should-mute-alexa.

3 *Id.*

of modern technology. For this reason, it is of critical importance that each attorney become "tech-savvy" or, at the very least, competent in the use of technology. In 2014, the NYSBA Committee on Professional Ethics (the "Committee") opined that an attorney should only use technology that he or she is competent to use.[4] While it is axiomatic that in today's day and age an attorney's technological proficiency plays an important role in their practice, irrespective of their office location, such aptitude is essential when working remotely. Accordingly, before a lawyer transitions to a remote work environment, appropriate steps should be taken to ensure that the lawyer is familiar with the law firm's operating systems and computer programs, and the firm's policies concerning the use of those systems and programs outside of the office. While an attorney is certainly not expected to be an IT expert, at the very least, the attorney should have the firm's IT personnel's number handy and be prepared to contact the IT personnel with issues arising from their remote work environment.

Additionally, if the COVID-19 pandemic has taught our profession anything, attorneys should endeavor to be flexible to become proficient in other technology that will enable them to service their clients and meet their clients' objectives remotely, if and when necessary. For example, during the pandemic many litigators may have been compelled to perform depositions or mediations for the first time remotely, and transactional attorneys may have been required to conduct closing remotely. It is critical that under such circumstances attorneys obtain training on how to perform those services in advance of the deposition, mediation, or closing. Our firm conducted several depositions and mediations utilizing videoconferencing platforms. Prior to engaging in those activities, we contacted the vendor providing the video platform to get a demo or watched a video concerning the technology (Zoom or Skype or any other platform) and practiced the video technology with our clients in anticipation of the actual deposition or mediation. We also tested the video platform to ensure that our Wi-Fi connectivity at our respective homes were sufficient, and used an Ethernet cable to secure our connections where necessary. Obtaining the training and practicing the video model in advance provided us with the ability to become proficient and comfortable with the technology.

4 *See* NYSBA Comm. on Prof'l Ethics, Op. 1025 (2014).

[5.3] IV. BEING COGNIZANT ABOUT AND PREPARED FOR CYBERSECURITY THREATS

Being technologically proficient, however, is only half the battle. Attorneys also should be cognizant of the heightened risk of cybersecurity threats when working remotely. The protection of client information from cybersecurity threats is an ethical issue of paramount importance. Attorneys and law firms have an ethical obligation to institute and maintain sound cybersecurity protocol, and to ensure that third-party vendors do the same.[5] Comment [8] to RPC 1.1 states: "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."

Indeed, it is of such recognized importance that on June 13, 2020, the House of Delegates approved the report of the NYSBA's Committee on Technology and the Legal Profession, which recommended that the mandatory 24-hour credit requirement for attorney continuing legal education CLE) be modified to require one credit on the topic of cybersecurity.[6] The credit would be considered under *Ethics and Professionalism* and it would be included within the existing biennial *Ethics and Professionalism* requirement. The requirement would exist for four years and would potentially be extended depending on the state of the legal profession at the time regarding cybersecurity, including the "hacking" of law firm electronically stored information.[7]

One example of a common cybersecurity threat to the practice of law are phishing scams. These scams include fraudulent emails that appear to be sent from a genuine source, such as a colleague, family member or personal banking institution, for the purpose of obtaining personal information, such as passwords and banking details, and defrauding attorneys or their firms. For this reason, attorneys should be extra vigilant when reviewing emails and downloading files. It is always a best practice to double check the email address of the sender and confirm the email is

5 See Vincent J. Syracuse, Maryann C. Stallone, Richard W. Trotter & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., June 2017, Vol. 89, No. 5.

6 New York State Bar Association, Report of the New York State Bar Association Committee on Technology and the Legal Profession Recommending That the Attorney Continuing Legal Education Biennial Requirement Be Modified to Require That the Ethics and Professionalism Requirement Include for Four Years One Credit on Cyber Security, January 27, 2020.

7 *Id.*

legitimate, as many hackers will create fake email accounts with only slight variations to that of the individual the hacker is purporting to impersonate. Attorneys also should avoid downloading files or clicking on links from an email that they are not expecting, and immediately bring emails that appear to be suspicious to the attention of the firm's IT department for further investigation.

Furthermore, attorneys should access their firm networks remotely through a Virtual Private Network (VPN), an encrypted connection over the internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted over the internet. Firms should always keep their VPNs current and deploy all patches with updated security configurations. It is critical to maintain proper multi-factor authentication for all VPN access to networks.

Cybersecurity threats also arise with the use of cloud-based file-sharing services to send and receive confidential client documents. A 2014 report by the Department of Homeland Security recognized that "online tools that help millions of Americans work from home may be exposing both workers and businesses to cybersecurity risks."[8]

In 2014, the Committee concluded that giving lawyers remote access to client files was not unethical, as long as the technology used provides reasonable protection to client confidential information, or the law firm informs the client of the risks and obtains informed consent from the client to proceed.[9] The Committee noted that "because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients."[10] However, the comments to RPC 1.6 instruct "[t]he key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure."[11]

8 Michael Roppolo, *Work-from-home remote access software vulnerable to hackers: Report*, CBS News, July 31, 2014, https://www.cbsnews.com/news/work-from-home-remote-access-software-vulnerable-to-hackers-report/.

9 *See* NYSBA Comm. on Prof'l Ethics, Op. 1019 (2014) and NYSBA Comm. on Prof'l Ethics, Op. 1020 (2014).

10 *Id.*

11 RPC 1.6, Comment [17].

To meet the reasonable care standard set forth in RPC 1.6, attorneys should consult with their firm's IT department or service provider to investigate whether their firm's file sharing services implement reasonable security measures to protect client confidences. Where possible, the firm should implement a two-factor authentication to access its work applications and software. If after speaking with the firm's IT provider/personnel an attorney continues to have doubts as to security, one should obtain the client's consent before sharing any files or documents. The failure to employ basic data-security measures can have severe consequences, including civil liability for professional malpractice. A security measure that law firms should consider implementing to protect client confidences is the encryption of files and emails sent both inside and outside the firm. Encryption is the process of converting digital information into a code, to prevent unauthorized access by outside parties.

The ABA Standing Committee on Ethics and Professional Responsibility has set forth additional best practices in addressing cybersecurity risks such as: (1) understanding and using reasonable security measures, such as secure internet access methods; when accessing files remotely, attorneys should avoid logging onto unsecure Wi-Fi networks or "hotspots," which can expose both the attorney and the firm's files to malware—software designed by hackers that can infiltrate remote desktops and whose capabilities include logging keystrokes, uploading discovered data, updating malware and executing further malware; (2) training non-lawyer support staff in the handling of confidential client information and to report suspicious activity; (3) clearly and conspicuously labeling confidential client information as "privileged and confidential"; and (4) conducting due diligence on third-party vendors providing digital storage and communication technology; (5) creating and implementing a data breach incident response plan; and (6) assessing the need for cyber insurance for data breaches.[12]

Another detrimental cybersecurity threat that attorneys should be aware of is a man-in-the-middle attack, or MITM attack, which occurs when the communication between two systems is intercepted by a third party, i.e., a Man-in-the-Middle. This can happen in any form of online communication, such as email, web browsing, and even social media. The MITM can use a public Wi-Fi connection to gain access to the attorney's browser, or even compromise an entire device. Once the MITM gains access to a device they have the ability to steal credentials, transfer data

12 *See* ABA Standing Committee on Ethics and Professional Responsibility, Formal Opinion No. 477 (May 2017).

files, install malware, or even spy on the user. To avoid the potentially significant and disastrous effects of a MITM attack, attorneys should work off a secure Wi-Fi network and avoid using "hotspots."

Additionally, when using video-conferencing platforms such as Zoom, lawyers should adopt the practice of password protecting meetings so they can avoid a type of cyberattack called "Zoom-bombing," where strangers hijack a private Zoom teleconferencing chat and draw offensive imagery onscreen, such as pornographic images, disclose personal information of the individuals in the chat, and even taunt them with hate speech and threats.

[5.4] V. THE CONTINUING DUTY TO SUPERVISE SUBORDINATE ATTORNEYS WHILE WORKING REMOTELY

Separately, attorneys working remotely must consider their ethical obligations of supervising subordinate attorneys, as required by RPC 5.1. Lawyers serving in a managerial or supervisory role are required to make reasonable efforts to ensure that all attorneys comply with their ethical obligations.[13] Specifically, RPC 5.1(b) requires lawyers with management or direct supervisory authority over other lawyers in the firm to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the RPC such as identifying dates by which actions must be taken in pending matters and ensuring that inexperienced lawyers are appropriately supervised.[14]

There are no bright line rules governing supervision. However, the comments to RPC 5.1 advise that each law firm should carefully consider the firm's structure and nature of its practice when adopting policies governing the supervision of subordinate attorneys.[15] For example, if the firm is relatively small and consists of mostly experienced lawyers, informal supervision and periodic review of compliance with the required policies will ordinarily suffice. Conversely, if the firm is much larger, and employs numerous junior attorneys, more elaborate measures may be necessary to place the firm in compliance with RPC 5.1.[16]

13 *See* RPC 5.1.

14 *See* RPC 5.1, Comment [2].

15 *See* RPC 5.1, Comment [3].

16 *Id.*

The degree of supervision required also varies on a case-by-case basis and is generally judged by what is reasonable under the circumstances. Factors that should be considered include: (i) the experience of the person whose work is being supervised, (ii) the amount of work involved in a particular matter, and (iii) the likelihood that ethical problems might arise while working on the matter.[17] Generally speaking, it is best practice for supervising attorneys to remain apprised of subordinate attorneys' workload, implement a system for review of the subordinate attorney's work product and ensure that the subordinate attorney understands that system.

Supervising attorneys also should establish an open line of communication with subordinate attorneys. In today's age, there are many mediums that allow for regular communication in this remote work environment including video conferencing, telephone calls, email and even text messages. Therefore, in addition to communicating via email, a supervising attorney should schedule regular calls with subordinate attorneys to check on their progress and review and discuss their work product and workload. How often the supervising attorney communicates with subordinate attorneys will depend on the complexity of the matter and issues, and the upcoming deadlines in those matters. This too is a matter of the lawyer's reasonable judgment and care.

Notably, RPC 5.1(d) articulates a general principle of personal responsibility for acts of other lawyers in the law firm and imposes such responsibility on a lawyer who orders, directs or ratifies wrongful conduct and on lawyers who are partners or who have comparable managerial authority in a law firm who know or reasonably should know of the conduct.[18] Thus, lawyers acting in a supervisory or managerial role should be aware that their failure to exercise diligence in reviewing the work of subordinate attorneys may result in personal liability under RPC 5.1(d).

[5.5] VI. THE CONTINUING DUTY TO DILIGENTLY REPRESENT CLIENTS

Whether working in the office or remotely, attorneys should always use their best efforts so that client communication and diligent representation continues uninterrupted. RPC 1.4 governs an attorney's obligations with respect to communicating with clients and states that attorneys are ethically obligated to promptly comply with reasonable requests for informa-

17 *See id.*

18 *See* RPC 5.1(d).

tion from clients.[19] To avoid noncompliance with RPC 1.4 while working remotely, attorneys should inform clients of the best way to reach them. If, for example, an attorney is able to forward calls from the office line to a personal cell phone, the attorney can tell clients that they may still use the office number. If attorneys do not have this ability, they need to advise their clients what alternate number they can be reached at. In some instances, this may require the attorney to provide the client a personal cell phone or home landline number. In addition, attorneys should regularly check their office voicemail and email and avoid large gaps in response time.

[5.6] VII. THE CONTINUING DUTY TO MAINTAIN PROFESSIONALISM AND DECORUM

Finally, attorneys must continue to maintain their professionalism and decorum despite working from the comfort of their homes. It is extremely important to dress appropriately when appearing in front of a tribunal; proper dress is part of basic professionalism and a sign of respect.[20] That standard still applies when participating in virtual court conferences, video arbitrations and mediations and virtual client meetings. Judge Dennis Bailey of Broward County Florida expressed his dismay that attorneys appeared inappropriately on camera for virtual court hearings: "It is remarkable how many attorneys appear inappropriately on camera," Bailey said. "We've seen many lawyers in casual shirts and blouses, with no concern for ill-grooming, in bedrooms with the master bed in the background, etc. One male lawyer appeared shirtless and one female attorney appeared still in bed, still under the covers. Putting on a beach cover-up will not cover up the fact that you are poolside in a bathing suit. So, please, if you don't mind, let's treat scheduled court hearings as court hearings, whether Zooming or not." If such a hearing or call was completely unplanned and unexpected, it is advisable that you ask to either reschedule the call or inform the court why you are not wearing appropriate attire (i.e., I'm on vacation with my family and received this call unexpectedly, if true).[21]

19 RPC 1.4(a)(4); Vincent J. Syracuse, Maryann C. Stallone & Carl F. Regelmann, Attorney Professionalism Forum, N.Y. St. B.J., July/August 2016, Vol. 88, No. 6.

20 *See* Vincent J. Syracuse & Matthew R. Maron, Attorney Professionalism Forum, N.Y. St. B.J., May 204, Vol. 86, No. 4.

21 Debra Cassens Weiss, Lawyers are dressing way too casual during Zoom court hearings, judge says, *ABA Journal,* April 15, 2020, https://www.abajournal.com/news/article/lawyers-are-dressing-way-too-casual-during-zoom-hearings-judge-says.

As always, the devil is in the details. What is deemed appropriate can be subjective and there may not always be agreement on what should be worn when participating in a virtual court or ADR proceeding. Certainly, going shirtless, wearing a bathing suit or video conferencing from your bed is never appropriate. You should use common sense, and when in doubt, it is best to err on the side of caution and overdress to avoid facing the risk of having your choice of clothing overshadow the needs of your client or what you might be saying.

[5.7] VIII. CONCLUSION

In short, although innovations in modern technology have given lawyers the freedom to operate their practice remotely, an attorney's ethical obligations must be at the forefront of their considerations regardless of their location. Close adherence to the aforementioned rules and procedures will allow lawyers to operate their remote practice easily, efficiently and in compliance with their ethical obligations.