It's 2024, Are You Technology Competent?

By Heather L. LaVigne
Assistant Bar Counsel
March 2024

Introduction and Brief History of Technology Competence

In March 2018, the Office of Bar Counsel published an article discussing a lawyer's duty of technology competence.[1] While we have published several articles related to technology and ethics in the meantime, this article provides a more fulsome update of the broad duty of technology competence, and is intended to further assist lawyers in assessing and developing their capabilities in this area. It does so by presenting a survey of selected decisions issued by disciplinary authorities and courts of various jurisdictions that imposed sanctions or discipline on attorneys who had failed to become competent in the use of various critical technologies.

The phrase, "duty of technology competence," is often used to refer to the language adopted in 2012 by the American Bar Association ("ABA") as comment 8 to Model Rule 1.1 (competence). Specifically, comment 8 requires lawyers to "keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*" (emphasis added). To date, at least 40 states have adopted language relating to the duty of technology competence.[2] In 2015, Massachusetts adopted the ABA's model language in comment 8 to Mass. R. Prof. C. 1.1. While Comment 8 did not create the duty to be competent in technology (it was already encompassed by Rule 1.1), it certainly has emphasized that such a duty is an integral part of competent lawyering.[3]

What Do You Need to Know to Be Technology Competent?

The cases that follow are grouped by common aspects of practice for which failures to properly adopt or use technology have resulted in disciplinary, civil, or other consequences for a lawyer or a client.[4] These include electronic filing; electronic discovery; security of client files, funds, and information; and practice technology and remote work. These cases show that technology missteps can result in failures to comply with almost any other ethical duty underscoring the fact that technology competence is built into all the other ethical rules.

---

[1] Heather L. LaVigne, *From Technophobe to Technolawyer A Lawyer's Duties Related to Technology Competence and Prevention of Inadvertent Disclosure* (March 2018).
[2] Robert Ambrogi, *LawSites,* https://www.lawnext.com/tech-competence
[3] *ABA Commission on Ethics 20/20 Revised Proposal—Technology and Confidentiality,* at 3-4 (September 19, 2011) https://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20110919_ethics_20_20_technology_and_confidentiality_revised_resolution_and_report_posting.pdf
[4] The article does not purport to address all potential practice areas in which technology issues can result in violations of ethical rules. For example, it will not address artificial intelligence. For a discussion of a lawyer's duties with regard to AI, see Assistant Bar Counsel Afton Pavletic's recent article, *The Wild West of Artificial Intelligence: Ethical Considerations for the Use of A.I. in the Practice of Law* (Jan. 2024). As cited throughout this article, the Office of Bar counsel has several other technology-related articles available on our website.

Electronic Filing

Electronic filing ("e-filing") can be fertile ground for costly and harmful mistakes. Luckily, many courts and government agencies have gone to great lengths to assist e-filers in understanding their obligations. These generally include enacting rules, publishing guides, and making staff available for questions. To take advantage of these resources, however, you must plan ahead. You should review the requirements, register for the system, practice with the system, and pursue any clarifications you may need long before a filing deadline. The stakes are high. For example, the Massachusetts Rules of Electronic Filing (R.E.F.), which govern electronic filing in the state trial and appellate courts make clear that filings can be rejected for "any technical nonconformance" with the rules, that a rejection does not extend the filing deadline, and that user errors will not excuse untimely filings. *See* S.J.C. Rule 1:25 - Massachusetts Rules of Electronic Filing (Effective June 1, 2020). The following cases from around the country demonstrate the risks of failing to master electronic filing.

In *Matter of Gareth David DeSantiago-Keene*, Docket No. DRB 21-06 (Aug. 30, 2021) upheld by 250 N.J. 185 (2022) a New Jersey lawyer received a three-month suspension when he delegated his e-filing duties to a client who was not a lawyer. Specifically, the lawyer was not sufficiently "computer savvy" to create an e-filing account for a client, so the client created it for him and maintained complete control over it. The client then used the account to make filings in a second matter unrelated to the case in which she was represented by the lawyer. After the lawyer agreed to represent the client in the second matter, the client made filings in which she purported to be the lawyer. The lawyer then lied to the court about why he did not appear on an order to show cause why sanctions should not be issued against him. The lawyer was found to have assisted in the client's unauthorized practice of law, engaged in dishonesty, and failed to maintain a client file. For this misconduct, aggravated by prior discipline, the lawyer was suspended for three months.

In *Matter of Jonathan David Esten*, 2017 WL 475660 (Va.St.Disp.) (Oct. 31, 2012), a Virginia lawyer received a public reprimand when he did not e-file a brief, resulting in the client being barred from presenting oral argument. While he emailed his brief, the court rules required that he use the court's e-filing system. He then failed to e-file the brief despite having received significant assistance and reminders from the court staff as well as extensions of time to e-file it. He was found to have violated Virginia's diligence rule. For this and other misconduct, the lawyer received a public reprimand with probation and a legal education requirement.

In *People v. Chuck Odifu Egbune*, 15PDJ025, 2015WL6178409 (Oct. 5, 2015), an Ohio lawyer failed to establish an account with the e-filing vendor. As a result, he did not receive communications about his client's case, did not respond to the opposing party's motion to dismiss, and did not know that the court dismissed the case. He was found to be in violation of Ohio's competence rule. For this and other misconduct, the lawyer received a public censure. Similarly, in *Cleveland Metropolitan Bar Association* v. *Rudolf Gusley*, 133 Ohio St.3d 534 (2012), an Ohio lawyer failed to register for an e-filing system resulting in summary judgment being granted against his client. Once he became aware of the motion and outcome, the lawyer failed to notify the client or seek relief. The lawyer was found to have violated Ohio's diligence and communication rules and received a public reprimand.

Lawyers have also been disciplined for failing to comply with redaction rules, which are increasingly important in the age of electronic access to court records. In *Matter of John A. Goudge*, 2012PR00085 (Jan. 29, 2013), an Illinois lawyer directed a non-lawyer assistant to e-file documents in federal court in a case relating to student loan delinquencies. Several defendants' personal identifying information and financial account numbers had not been redacted, in violation of the Federal Rules of Civil Procedure. One defendant called the court with concerns that her information was viewable by the public. The lawyer was found to have violated Illinois rules regarding supervision of non-lawyers and prohibiting conduct prejudicial to the administration of justice. The lawyer received a public reprimand.

Similarly, in a Massachusetts matter, a lawyer violated court orders requiring the redaction of an alleged assault victim's identifying information and also sent the unredacted pleadings to a blogger. *Matter of Stacy Elin Rossi*, 36 Mass. Att'y Disc. R. 415 (2020). The lawyer was found to have violated Mass. R. Prof. C. 1.1 (competence); 1.3 (diligence); 3.4(c) (failure to comply with obligations under the rules of a tribunal); 8.4(a) (misconduct through the acts of others); 8.4(d) (conduct prejudicial to the administration of justice); and 8.4(h) (fitness to practice). For this and other misconduct, some of which was mitigated, the lawyer received a three-month suspension with two months stayed on conditions of entering into a mentoring arrangement.

While the board in *Rossi* did not focus on the method of filing, and it was the lawyer herself who disseminated the filing to a blogger, the importance of properly redacting documents cannot be overstated in our increasingly online world. In addition to traditional media outlets monitoring court dockets to report on cases of public interest, there are countless bloggers and vloggers who disseminate court documents to vast audiences. Although a court may reject a filing for a failure to redact, lawyers cannot rely on court staff to notice redaction failures. Once the document is online, it may stay in the public realm forever.

Electronic Discovery

Electronic discovery ("e-discovery") mishaps can result in violations of many ethical rules as well as monetary and other sanctions against attorneys and clients. The vast scope of electronic discovery obligations is far beyond the scope of this article. There is a robust body of rules and case law relating to e-discovery that has evolved since the 2006 adoption of the federal civil procedure rules pertaining to e-discovery. Below are just a few examples of electronic discovery issues that have resulted in ethical violations or court sanctions.

E-discovery violations are common when attorneys fail to understand how their client stores electronic information and what types of electronic information must be preserved to comply with court orders and the various laws and rules pertaining to electronic evidence. A lawyer's lack of understanding of these systems can result in spoliation of evidence, failure to properly respond to discovery requests, and false representations to courts and opposing parties. For example, in *Matter of Reisman*, 29 Mass. Att'y Disc. R. 556 (2013), a Massachusetts lawyer improperly advised his client to delete files from a laptop during litigation. Because of his inexperience with electronic discovery, he wrongly believed that the files could be deleted. The

court found that the client had engaged in spoliation of evidence. In a resulting disciplinary matter, the lawyer was found to have violated Mass. R. Prof. C. 1.1 (competence); 1.4 (communication); and 3.4(a) (unlawful obstruction of party's access to evidence). The lawyer received a public reprimand and was required to attend continuing legal education courses. In *Admonition No. 20-24,* 36 Mass. Att'y Disc. R. 527 (2020), a Massachusetts lawyer represented a client against allegations that she had stolen confidential documents from her employer. While the client gave the lawyer flash drives containing the content she had taken from the employer, she did not accurately explain the contents of drives. The lawyer did not know how to review the content and relied on the client's representations, which resulted in him making negligent misrepresentations to opposing counsel and the court. The lawyer received an admonition for violations of Mass. R. Prof. 1.1 (competence) and 1.3 (diligence).

Electronic discovery mistakes can also result in a lawyer inadvertently producing documents and information that were intended to remain confidential. This was recently on display in the highly publicized Alex Jones defamation case brought by families of victims of the Sandy Hook school shooting. Many lawyers have seen the viral video of Attorney Mark Bankston, who represented some of the plaintiffs, questioning Alex Jones about his lawyer's inadvertent production of electronic information, and Jones exclaiming that Bankston got his "Perry Mason moment." What did not end up in a viral video was the sanctions proceeding relating to Jones' lawyer, Andino Reynal. *See Lafferty, Sherlach, and Sherlach v. Alex Jones*, 2023 WL 415602 (Jan. 17, 2023). Reynal was in possession of medical records belonging to other plaintiffs who Bankston did not represent, and which were subject to a protective order. Reynal's paralegal inadvertently produced some of these materials to Bankston by sending a link to a different set of documents than was intended for production. As most jurisdictions require attorneys who receive inadvertently produced material to notify the sender, Bankston informed Reynal that he found in the production what he believed to be inadvertently produced documents. Under the applicable law, there was a 10-day claw-back period for Reynal to pursue protection of the inadvertently produced documents, which he did not do. The court found that Reynal had violated Connecticut rules relating to competence and safekeeping property[5] when he failed to take steps to retrieve and protect the inadvertently produced medical records. The lawyer was sanctioned.

For ethical obligations when you are on the receiving end of an inadvertent production, Massachusetts attorneys should review Mass. R. of Prof. Conduct 4.4(b), and Richard C. Abati, *Inadvertent Disclosure: When Your Opponent Has Let the Cat Out off the Bag* (April 2016).[6] Lawyers on the receiving end of inadvertent productions may face sanctions and discipline. For example, in January 19, 2024, an Alabama lawyer was publicly reprimanded when he obtained privileged emails between his client's wife and her attorney and failed to notify the wife's counsel.[7] He then used those emails to gain an unfair advantage in the proceeding. For this and other misconduct the lawyer received a public reprimand.

---

[5] This author posits that several other rule violations could be charged under these circumstances.

[6] Available on our website.

[7] Discipline summary Available at https://www.alabar.org/office-of-general-counsel/disciplinary-history/

As technology used by clients and lawyers will continue to change, attorneys should participate in continuing legal education, and, where appropriate, consult with the growing community of electronic discovery experts. When associating with others, lawyers must be especially cognizant of their confidentiality and supervision obligations.

Maintaining Client Files

Maintaining client files in electronic form is essentially a standard practice in 2024, so lawyers must ensure that electronic files are maintained securely to avoid permanent loss or unauthorized access by third parties.

In *People v. Jennifer K. Mrachek*, 23PDJ06520, 23WL8869762 (Dec. 4, 2023), a Colorado lawyer represented an incarcerated client in a resentencing matter for over 7 years. During that time, she performed a significant amount of work which was maintained on her computer and an external hard drive. She lost the entire file when her computer and external hard drive were damaged. She stopped communicating with her client and never told the client that the file was lost. The lawyer was found to have violated Colorado's rules regarding diligence, communication, and retention of client files and received a public censure. *See also Columbus Bar Assn. v. Bulson*, Slip Opinion No. 2023-Ohio-4258 (2023) (Ohio lawyer failed to finalize client's work in part because he could not recover lost computer files, and then failed to communicate with his client).

Similarly, in *Matter of Doyle*, 26 Mass. Att'y Disc. R. 143 (2010), a Massachusetts lawyer failed to properly preserve a client's electronic file, did not maintain a back-up, lost all the documents, and thereafter, neglected the case. He was found to have violated Mass. R. Prof. C. 1.3 (diligence). The lawyer received a public reprimand.

As these cases show, lawyers must use appropriate back-up procedures and if client files are lost, lawyers cannot just throw up their hands. It may be possible to retrieve the lost files or recreate some of the file. At the very least you must communicate with your client and act to protect their interests while the file issue gets sorted out. Additionally, lawyers must take measures to prevent the unauthorized receipt of or access to client information, property, and money in their possession. *See, e.g.,* Mass. R. Prof. C. 1.6, cmt. 18-19 (requiring lawyer to act competently to safeguard against unauthorized access by third parties to confidential information and communications). The next sections discuss instances in which lawyers have been scammed or hacked resulting in funds being improperly disbursed or information being disclosed.

Securing Client Funds and Information

The North Carolina State Bar has been ahead of the pack when it comes to disciplining lawyers whose lack of competence or diligence causes them to fall victim to wire fraud scams.[8] In *Matter of Michelle Vereckey*, 21G0973 (Sept. 6, 2022), a North Carolina lawyer initiated multiple wires pursuant to fraudulent wiring instructions without verifying the wiring

[8] Discipline resulting from a lawyer's knowing involvement in any sort of fraud or scam is beyond the scope of this article.

instructions. The grievance committee stated that the lawyer had failed to recognize numerous "red flags" which should have raised her suspicions about the fraud. By failing to verify the wiring instructions prior to the disbursements, the lawyer was found to have violated North Carolina's rule on safekeeping of trust property. The lawyer received a public reprimand. Similarly, in *Matter of David Hands*, 21G0668 (Feb. 16, 2022), a North Carolina lawyer fell victim to a wire fraud scam when his paralegal received an email purporting to be from a party to the transaction, stating that corrected wire instructions would be sent via fax. When she received the fax, the paralegal did not verify the changed wire instructions, in violation of the firm's protocols. The lawyer received a public reprimand for violating North Carolina's rules on safekeeping of trust property and supervision of non-lawyer assistants. *See also Matter of Anthony Donato*, 19G0239 (Aug. 17, 2019) (public reprimand when neither lawyer or paralegal reviewed or verified the wire instructions); *Matter of James W. Kirkpatrick*, 19G0191 (Aug. 7, 2019) (same).

In a somewhat different set of circumstances, an Iowa lawyer was disciplined when he failed to recognize an obvious scam and lost funds of several clients. *Iowa Disciplinary Bd. v. Wright*, 840 N.W.2d 295 (2013). The lawyer represented a client in pursuing a purported inheritance from a long-lost Nigerian relative. Instructions received by the client directed him to pay certain taxes and obtain an "anti-terrorism certificate" from the Nigerian government so that the inheritance could be released to him. To pay these expenses, the lawyer solicited and negotiated loans from several of his other clients. The lawyer spoke on the phone to various people claiming to be agents of the Nigerian government and then disbursed the funds to them, losing thousands of his client's funds that could not be retrieved. The Iowa board credited that the lawyer believed the inheritance to be legitimate but found that he failed to verify any of the identities of the people he spoke to, and that a cursory internet search for "anti-terrorism certificate" would have revealed that this was a common scam. The lawyer was found to have violated Iowa's rules regarding competence, business transactions with clients, and dishonesty (for failing to fully disclose information to clients from whom he obtained loans), and he received a one-year suspension.

Lawyers may fall victim to wire fraud scams because of a data breach of their own systems or the systems of anyone involved in the transactions. Scams in which a fraudster gains access to a lawyer's email account and takes advantage of knowledge that the lawyer is expecting wire instructions are referred to as business email compromise scams.[9] While not all of these situations implicate a violation of ethical rules,[10] the scams have become sufficiently widespread that lawyers; as a matter of competence, diligence and the duty to safeguard client funds; are expected to take reasonable precautions against them. Discipline is especially likely when attorneys: (a) do not properly confirm wire instructions; (b) ignore typical signs of a wire fraud scam; (c) fail to employ sufficient measures to prevent wire fraud; (d) fail to communicate

[9] *See, e.g.,* https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise; https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident; https://www.bbb.org/all/scamstudies/bec_scams/bec_scams_full_study

[10] *For more information on wire fraud scams and ethical considerations, see, e.g., 2020 NC Formal Ethics Op. 5 (Jan. 15, 2021); 2021 NC Formal Ethics Op. 2 (Jul. 16, 2021); 2015 NC Formal Ethics Op. 6 (Oct. 25, 2015); 2011 NC Formal Ethics Op. 7 (Jan. 27, 2012); NYCBA Formal Op. 2015-3 (April 22, 2015)*

with their clients in the aftermath of an incident; and (e) take insufficient actions to mitigate consequences of the errant disbursal. Discipline is particularly likely when harm results. The next section discusses cases relating to more general cybersecurity incidents and data breaches at law firms.

In 2023 the New York Attorney General's office investigated a New York Law firm after a data breach involving confidential health records of the firm's medical provider clients.[11] The firm entered into an agreement to resolve the matter by paying the state $200,000. While the firm did not admit wrongdoing, the Attorney General's allegations appear in the agreement. The firm is said to have failed to implement available fixes to known vulnerabilities in its information technology systems, which permitted a hacker to access the firm's systems, deploy ransomware,[12] and steal a significant amount of data and information. Once alerted to the intrusion, the firm hired a forensic cybersecurity provider, and the firm paid a $100,000 ransom to the attackers in exchange for return of the files and a promise to delete them. The Attorney General alleged that the firm failed to comply with federal privacy and security laws and failed to provide timely notice of the breach to clients and others affected. The agreement required the firm to implement several practices and procedures to improve its cybersecurity.

In 2019, an immigration client sued his former Washington D.C. law firm for malpractice, breach of fiduciary duty, and breach of contract, after the firm's information technology systems were breached by someone assumed to be targeting the client.[13] The client, who was seeking political asylum in the U.S., claimed that he informed the firm that he had been the target of cyber-attacks by the Chinese Communist Party and that the firm misrepresented its ability to protect his data from such cyber-threats. The firm ultimately settled the matter for $499,000.[14]

Lawyers are fiduciaries who are entrusted with highly confidential information and funds. Accordingly, lawyers are expected to take measures to prevent and mitigate cyber-threats. Discipline is especially likely when attorneys: (a) ignore known vulnerabilities and risks; (b) employ insufficient measures to prevent data breaches; (c) fail to communicate with their clients in the aftermath of a breach; and (d) take insufficient actions to mitigate consequences of a breach. Discipline is particularly likely when harm results. There is a growing community of cybersecurity experts to consult, as well as opportunities for continuing legal education. The internet abounds with information about cybersecurity.[15] Many professional liability carriers also provide educational information and insurance coverage relating to cybersecurity. Lawyers

---

[11] Investigation of Heidell, Pittoni, Murphy, & Back, Assurance No. 23-011 (March 10, 2023) available at https://ag.ny.gov/sites/default/files/aod_-_final_hpmb.pdf

[12] For a discussion of Ransomware, see Terrence D. Pricher, *Ransomware 101: An Introduction for Small Firms and Title Insurance Agents* (July 2017); *See also* https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/ransomware.

[13] *Guo Wengui v. Clark Hill*, PLC, 440 F.Supp.3d 30 (2020).

[14] *Guo Wengui v. Clark Hill*, PLC, 338 F.R.D. 7 (2021); *Ho Wan Kwak, et. al*, Case No. 22-50073 (May 4, 2023).

[15] https://www.americanbar.org/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/ https://www.fbi.gov/investigate/cyber

should also review ABA opinions that provide guidance to lawyers regarding protecting client information.[16]

Law Practice Technology

Lawyers in all practice areas are using technology in their law practice. Failure to understand the risks and benefits of those technologies can result in harm to clients and professional discipline for lawyers.

In *Disciplinary Counsel v. Valenti*, 165 Ohio St.3d 49 (2021), an Ohio lawyer made several errors for multiple clients resulting in the court removing her as appointed counsel for criminal defendants. Among other errors, she filed incoherent briefs, missed filing deadlines, and failed to show up at a hearing due to a scheduling conflict. She defended her actions by stating that she had accidentally filed a draft brief, failed to save the final version, and missed a filing deadline because the flash drive containing the filing had broken. The court found that the lawyer was not "sufficiently technologically competent" and found that she violated Ohio's rules on competence, diligence, and conduct prejudicial to the administration of justice. The lawyer was suspended for six months, stayed on condition that she receive six hours of continuing legal education in criminal appellate law, and six hours of continuing legal education in law-office management with a focus on calendar management and law-office technology.

In *Matter of Hochman*, 31 Mass. Att'y Disc. R. 295 (2015), a Massachusetts lawyer used a commercially available software program to prepare bankruptcy documents for his clients and failed to ensure that output totals were accurate. As a result of his failure to review the totals, the lawyer generated an unfeasible bankruptcy plan resulting in dismissal of the client's bankruptcy petition. The lawyer also failed to communicate with the client regarding the denial. The lawyer was found to have violated Mass. R. Prof. C. 1.1 (competence); 1.2(a) (pursuit of client's objectives), 1.3 (diligence), and 1.4 (communication). For this and other misconduct, he received a public reprimand.

In *Matter of O'Dougherty*, GC No. 14-0520 (2015), a Connecticut lawyer repeatedly failed to communicate with a client by phone, text, or email. The lawyer said she did not understand texting, among other excuses. The lawyer was found to have violated Connecticut's communication rule. The lawyer was ordered to take continuing legal education courses.

Remote Work

While technology and remote work[17] have opened many doors for attorneys to enhance their practice, taking advantage of remote settings to commit misconduct will result in discipline.

---

[16] *See* ABA Formal Opinion 483 – Lawyers' Obligations After an Electronic Data Breach or Cyberattack (2018) and ABA Formal Opinion 477R – Securing Communication of Protected Client Information (2017).

[17] For more information about remote practice, see Stacey A.L. Best, Lawyers in Crisis: Ethical Guidelines for Remote Work and Dealing with COVID-19 (April 2020).

In *Matter of Rosin*, 39 Mass. Att'y Disc. R. ___ (2023), a Massachusetts lawyer was disciplined for coaching a client while he was testifying at a remote deposition. The lawyer and the client were in the same room wearing masks. After the deposition, opposing counsel reviewed the video and heard about fifty instances of the lawyer feeding his client answers. The lawyer was found to have violated Mass. R. Prof. C. 3.4(c) (fairness to opposing parties); 8.4(d) (conduct prejudicial to the administration of justice); and 8.4(h) (fitness to practice). The Board issued a public reprimand but made clear that future similar cases may not be viewed "as indulgently."

Similarly, an Arizona lawyer was disciplined for coaching a client during testimony at a virtual hearing. *State Bar v. Claridge*, PDJ 2021-9068, 2022WL2837857 (AZ.Disp.Com.) (Jan. 21, 2022). After the hearing, the court discovered that the lawyer had used the chat function of the video conference software to provide answers to the client on cross-examination. The lawyer was found to have violated Arizona's rules on fairness to opposing parties, dishonesty, and conduct prejudicial to the administration of justice. The lawyer was suspended for 60 days and put on probation for two years.

A Florida attorney was disciplined when he coached a witness during a telephone deposition without video. *Florida Bar v. James*, 329 So.3d 108, 109-112 (Fla. 2021). Specifically, the lawyer and his client were in separate locations while the lawyer texted his client answers to questions posed to her. When the opposing counsel questioned the lawyer about typing sounds, the lawyer falsely stated that he was texting his daughter. After stating that he would put his phone away, the lawyer inadvertently sent opposing counsel several text messages meant for his client containing answers to questions. The lawyer was found to have violated Florida's rules regarding dishonest conduct, obstructing another party's access to evidence, and conduct that is prejudicial to the administration of justice. He was suspended for thirty days.

In *Florida Bar v. Oscar Antonio Hotusing*, SC2022-0944, 2023 WL 6314606 (September 28, 2023), a Florida attorney took advantage of the availability of remote practice to engage in the unauthorized practice of law in another state. He used the Maryland Court's electronic filing system to assist a client in a Maryland divorce proceeding without authorization to practice law in Maryland. The lawyer registered under his client's name, indicating that she was *pro se*, but used his own email address. He submitted filings stating that she was *pro se*, without stating that they were prepared with the assistance of counsel, and requested a remote hearing which ultimately did not occur. The respondent was found to have engaged in the unauthorized practice of law, and conduct involving dishonesty. For this misconduct, aggravated by prior discipline, the lawyer was suspended for 91 days. [18]

[18] The ethical implications of remote practice while physically located in a state in which the lawyer is not authorized to practice law is beyond the scope of this article. For more information on cross-border remote practice, see David Kluft, What You Should Know About Cross-Border Remote Practice (March 2023).

Of course, feeding answers to someone who is providing testimony under oath is unethical under any circumstance. [19] Likewise, any manner of deceiving a court to practice before it without authorization is discipline worthy. These cases show that lawyers who take advantage of remote situations and leverage technology to commit misconduct may subject themselves to serious discipline.

Conclusion

At least three important lessons emerge from these cases. First, lawyers and their staff must prioritize ongoing technology-related education, training, and communication. This includes creating a culture of security and compliance in which no one is exempt from participation. In other words, no employee's pay grade is above or below learning the benefits and risks of relevant technology and how to appropriately employ it in their work. It also means setting expectations for and developing a climate that supports forthright communication about technology, professional development, and mitigation of mistakes.

Second, lawyers who find themselves enmeshed in a technology-related blunder must take reasonable steps to mitigate the consequences of the error. This requires that lawyers timely and truthfully communicate with their clients, courts, and others affected. When measures can be taken to ameliorate the error, lawyers must take those steps. As many of the above cases show, lawyers who compound fixable or mitigatable errors by neglect, lack of communication, or dishonesty are likely to subject themselves and their clients to greater harm, costly sanctions, or discipline.

Third, while this article does not intend to suggest that all technology-related mistakes rise to a violation of the duty of competence, lawyers practicing in Massachusetts should be aware that technology missteps can rise to the level of ethical misconduct warranting discipline. Staying abreast of technology is therefore a critical element of being an ethical lawyer.

[19] For more information on this topic and witness preparation in general, see ABA Formal Opinion 508 – The Ethics of Witness Preparation (2023).