"REMOTE" LAWYERING

Overcoming privacy and confidentiality challenges for attorneys.

WRITTEN BY **ELIZABETH ROGERS**

There arrived a particular hour on a particular weekend after "spring break" 2020, or maybe it wasn't until the end of March, when a wave of anxiety washed away the bliss of working at home in sweatpants. For many lawyers, maybe it was the day we learned that we could not work in the office buildings where our law firms are located or that we could not make a live appearance at a hearing in the courthouse. And so it began, at different times, for different reasons, and in different ways that we established our "new norms."

The new remote lawyering norm creates novel challenges because many of us have been forced to quickly and significantly change our workplace and the ways we interact with clients, courts, colleagues, and each other. Lawyers who are inexperienced with maintaining a law practice from home have developed a sudden need to know how to not only use technology effectively but also how to use it in a way that complies with legal and ethical obligations toward clients and their information. To help bridge the gap between the number of questions about how to do it right and the available answers, this article sets forth some guidelines and best practices to help lawyers navigate the regulatory and ethical challenges of working from home, arising in the context of privacy and confidentiality.

The Reasonable Security Requirement

Privacy and the duty of confidentiality require reasonable security. Therefore, lawyers working at home should provide reasonably appropriate technical, administrative, and physical security for all client confidential information. Taking these steps not only aids productivity, but also ensures compliance with certain data privacy regulations as well as ethics and professional responsibility requirements. For example, maintenance of a reasonable security program under the California Consumer Privacy Act, or CCPA, is a defense in a personal data breach lawsuit.

Some steps lawyers can take to provide reasonable security include maintaining secure remote access and the consolidation of case information into one well-organized electronic space. Further, the ability to encrypt sensitive client or employee information, control where it is stored, and monitor who can access it will not only mitigate security vulnerabilities but also provide other advantages. Specifically, many states' data breach notification laws include a safe harbor provision to reward businesses for encrypting their data. This provision would, for example, allow a law firm to portray a security event as an "incident" instead of declaring it had a "breach" and relieve it from the expense and humiliation of having to send out breach notifications.

The Ethical Challenge

Under the Duty of Confidentiality

Because certain privacy regulations are closely related to a lawyer's ethical duty to safeguard a client's confidential information, there are overlapping duties regarding a lawyer's responsibility to safeguard personal data when using technology solutions. Specifically, the duty of confidentiality broadly requires the lawyer to not reveal a client's confidential information to anyone not authorized by the client. This duty includes avoiding a data breach or other inadvertent disclosure or unauthorized access to a client's confidential information.[1]

Lawyers must, for example, use a heightened standard for who, how, and when remote access to client confidential data will be allowed. To achieve a heightened standard, a law firm might establish policies that limit remote access to highly sensitive client data to only a single team member or to only the few team members who have critical roles to play in the management of the case. Additionally, law firms might consider providing limited or redacted information to those workers who do not usually work from home and may not have access to secure IT or other adequate equipment, if they deem the duty of confidentiality warrants such a restriction under the circumstances.

The heightened duty of confidentiality, under remote lawyering circumstances, also requires the legal community to consider whether and under what circumstances Zoom (or any other videoconferencing solution) is an appropriate forum for engaging in confidential client communications and, if so, what measures should be taken to ensure confidentially. Recent events involving the Zoom videoconferencing platform—leading to the term "Zoom-bombing"[2] —provide an ideal case study to illustrate how use of these technologies can give rise to a violation of duty of confidentiality (and potentially, the ethical duty of technology competence, discussed below).

The answer to whether the use of Zoom satisfies the heightened duty of confidentiality for conducting client meetings involves considerations similar to those arising under various international and state privacy laws. Whether or not use of Zoom would be considered to satisfy the requirements of a reasonable security program will depend on the specific circumstances of the communication, the audience, and the availability of other forums for transmission.

Even with that being said, to comfortably use Zoom as a tool for confidential communications with clients, attorneys must ensure basic security functions are enabled[3] to limit exposure and the risk of compromised communications. Establishing basic controls, however, will not ensure categorical compliance with the duty of confidentiality or of privacy regulations. The key is to establish the right balance between the level of sensitivity of the information being transmitted with the most appropriate security option available to protect it, under all of the circumstances. Clients always have the right to insist on greater security.

Under the Ethical Duty of Technology Competence

On February 26, 2019, the Texas Supreme Court amended Paragraph 8 of the comment to Rule 1.01 of the Texas Disciplinary Rules of Professional Conduct,[4] which deals with competent and diligent legal representation. Under the amended comment, maintaining proficiency and competence in the practice of law includes knowing "the benefits and risks associated with relevant technology."[5]

Attorneys who work remotely are increasingly turning to a variety of videoconferencing platforms to provide legal services to clients, both inside and outside the courtroom.[6] While these technologies have proven benefits in ensuring a continuity of legal services, lawyers must, nevertheless, exercise their heightened ethical duty to be aware of the risks of these platforms and technologies.

For example, a serious privacy and confidentiality risk arising from the use of videoconference platforms includes software vulnerabilities or problems in the codebase that might allow criminals to exploit the platform to compromise its end users. Zoom provides yet another case study that, this time, illustrates vulnerabilities and potential ethical violations that arise because of security flaws in the software. The New York Attorney General's Office investigated, after which a settlement agreement with Zoom was reached, and required Zoom to make cybersecurity enhancements to its technology.[7] To be fair, software vulnerabilities exist in many applications. The process of identifying them, patching them, and updating them is not only an inherent part of the life cycle of any application but also part of the Texas lawyer's heightened duty of technology competence.

The Regulatory Challenge

Under the Americans with Disabilities Act of 1990

Some law practices and law firms that are offering the hybrid option—either working from the office building or virtual lawyering—have implemented medical screening programs before lawyers can work in the law firm's office. Ordinarily, the Americans with Disabilities Act, or ADA, forbids an employer from asking medical questions, requiring an employee to submit to medical exams, or from disclosing confidential medical information, including an employee's identity. However, because the World Health Organization and the Centers for Disease Control have declared COVID-19 to be an international pandemic, in April 2020, the Equal Employment Opportunity Commission said COVID-19 meets the ADA's direct threat standard that allows employers to ask screening questions, take the temperatures of, and test workers prior to permitting those workers onsite. For example, law firms may ask applicants or current employees whether they have specific symptoms currently associated with COVID-19 but also may ask about any additional symptoms that evolve as more information is learned about the effects of the virus.

Best Practices

Law firms that implement medical screening solutions should also implement notice and consent requirements. For example, the CCPA requires covered employers who employ California residents to provide those employees with a "notice at or before the time of collection" when collecting personal information, even though employees are exempt from other provisions in the law until 2022. Even where not legally required to do so, covered law firms should consider providing all employees with a notice for the sake of preserving positive employee relations.

At other points during the screening process, ADA- and CCPA-covered law firms also will need to consider whether and how long to retain the data collected. If answers to screening questions and test results are going to be kept, then they should be treated like a confidential record of a serious health condition, under the ADA, and retained as a medical record, separate from the employee's other personnel records.

Under the General Data Protection Regulations ((EU) 2016/679 ("GDPR"))

Compliance with the GDPR, in a remote working world, requires extra thought and forward thinking because not everyone who is handling client matters from home understands what personal data is protected[8] and how to protect it. For example, recorded audio files of conversations with clients contain personal and confidential data that not only must satisfy the requirements of Texas' ethical rules for safeguarding confidential client data, but also must satisfy the GDPR's requirements for a legal basis of processing the personal data.[9] An example of a simple step that law firms can take is to remove the recording functionality, which will prevent employees from inadvertently creating audio files that contain personal and/or confidential client data.

Conclusion

The answers and solutions for the novel challenges associated with remote lawyering are still evolving and will probably continue to do so. Despite the uncertainties, attorneys must always consider not only the implications of using a specific method of communication but also the availability and plausibility of methods. For attorneys, there is not only the duty to comply with established and newly enacted privacy laws but also the duty to consider how emerging technologies impact their practices and implicate their ethical duties to clients, a duty that always should come first. **TBJ**

NOTES

1. Tex. Prof. R. of Disc. Conduct 1.05(b) provides that: Except as permitted by paragraphs (c) and (d), or as required by paragraphs (e), and (f), a lawyer shall not knowingly: (1) *Reveal confidential information of a client or a former client to:* (i) a person that the client has instructed is not to receive the information; or (ii) *anyone else,* other than the client, the clients representatives, or the members, associates, or employees of the lawyer's law firm. (Emphasis added.)
2. Defined loosely as the practice of bad actors hijacking legitimate confidential client sessions and either conducting espionage or disrupting the normal course of events.
3. These controls include: (a) enabling meeting passwords; (b) disabling join before host; (c) enabling lobby with approval; (d) locking Zoom room when the correct attendees have joined; (e) disabling guest chat; and (f) disabling guest screen sharing.
4. Texas Supreme Court Misc. Docket No. 19-9016, available at https://www.txcourts.gov/media/1443638/199016.pdf.
5. Comment 8 to the Texas Disciplinary Rules of Professional Conduct, Rule 1.01 provides: Because of the vital role of lawyers in the legal process, each lawyer should strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology. To maintain the requisite knowledge and skill of a competent practitioner, a lawyer should engage in continuing study and education. If a system of peer review has been established, the lawyer should consider making use of it in appropriate circumstances. Isolated instances of faulty conduct or decision should be identified for purposes of additional study or instruction.
6. Subrat Patnaik, *Zoom's daily participants jumped from 10 million to over 200 million in 3 months,* VentureBeat (Apr. 2, 2020 7:43 AM), https://venturebeat.com/2020/04/02/zooms-daily-active-users-jumped-from-10-million-to-over-200-million-in-3-months/. For example, Zoom grew from 10 million to 200 million active users between March and June 2020.
7. Email from Kim A. Berger, Chief of Bureau of Internet and Tech., N.Y. State Office of the Atty. Gen., to Travis LeBlanc, Zoom Video Communications, Inc. (May 7, 2020), available at https://ag.ny.gov/sites/default/files/nyag_zoom_letter_agreement_final_counter-signed.pdf.
8. Gen. Data Protection Regs. ("GDPR"), Art. 4 (1). Personal data are any information that are related to an identified or identifiable natural person.
9. *See* GDPR, Recital 40. In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis.

ELIZABETH ROGERS
is a partner in the nationwide law firm Michael Best & Friedrich based in Austin. Focusing her practice on privacy and cybersecurity matters, Rogers routinely advises clients on issues including breach responses, privacy risk assessments, and enterprise-wide cybersecurity compliance frameworks across industries such as retail, health care, financial services, retail electric providers, education, and state and local governments.