Cybersecurity Considerations for Environmental and Energy Lawyers Working Remotely in the Wake of the Coronavirus

Prepared by: ABA SEER Special Committee on Ethics
Pamela Esterman, Sive, Paget & Riesel, P.C., New York, NY
Claudia Rast, Butzel Long, Ann Arbor, MI
Irma Russell, University of Missouri - Kansas City School of Law

Date: March 26, 2020

Introduction

As we all navigate the COVID-19 virus pandemic, a quick review of the following practice pointers addressing a lawyer’s legal and ethical duties while working remotely may help avoid those pitfalls common to telework. The US Department of Homeland Security Cybersecurity and Infrastructure Security Agency has encouraged those working remotely “to adopt a heightened state of cybersecurity” as there is a significantly elevated risk of malware, phishing attacks and ransomware demands in the midst of the coronavirus pandemic. This document begins with a brief summary of the relevant ABA Model Rules of Professional Conduct. Next, it provides a number of considerations or practice pointers that should be observed to safeguard the lawyer-client relationship and client data. It concludes with a list of resources for additional information on this topic. Of special note in this time of crisis is The ABA Standing Committee on Law and National Security and the Health Law Section webinar, Remote Working in a Time of COVID-10: Cybersecurity Issues You Need to Know, which is available on-demand free for ABA members at: https://www.americanbar.org/events-cle/ecd/ondemand/398558739/.

Summary of Some Relevant Ethics Rules

Several of the ABA Model Rules of Professional Conduct have particular relevance to the risk posed by remote or telework. These include:

Model Rule 1.1- Competence
Under Rule 1.1, “a lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”

Comment [8] of Rule 1.1 provides that an attorney’s duty of competence in relation to technology includes “keep[ing] abreast of the changes in the law and its practice, including the benefits and risks associated with relevant technology.”

Model Rule 1.4- Communication
Attorneys have an ongoing responsibility to evaluate the level of security required in their communications with clients and to know the methods and means to best protect the
confidentiality of that information.

**Model Rule 1.6- Confidentiality**
Rule 1.6 addresses a lawyer’s obligation to keep client information confidential. Confidentiality is critical to any attorney-client communication. The Rule states: “A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent…”

Comment 18 to Rule 1.6 recommends that attorneys assess the sensitivity of the information. The greater the sensitivity, the less risk the lawyer should take.

**Rule 1.15-Safekeeping Property**
Rule 1.15 provides “A lawyer shall hold property of clients or third persons that is in a lawyer’s possession in connection with a…” An ABA ethics opinion has extended this rule to electronic data held by attorneys.

**Rule 5.3- Responsibilities Regarding Nonlawyer Assistants**
Rule 5.3 provides: “With respect to a non-lawyer employed or retained by or associated with a lawyer…[,] a lawyer having direct supervisory authority over the non-lawyer shall make reasonable efforts to insure that the person’s conduct is compatible with the professional obligations of the lawyer.”

**Practice Pointers**

1. Determine whether your law firm or organization has rules or policies for remote or telework, and if so, read them and make every effort to comply. Contact your organization’s IT staff or external IT Vendor if you have questions or concerns.

2. If you are using your personal device(s) for remote work, be sure to enable basic security features including a PIN, fingerprint, or facial ID feature and an automatic “log-out” after 5 minutes on a mobile device and 20 minutes or a bit longer on a tablet/iPad/laptop/PC. Confirm that your passwords are unique for your home routers and other access points, i.e., never use the default password that comes with the equipment. Phrases make the best passwords! The ethics rules require attorneys to take reasonable data security precautions. The greater the sensitivity of the information you handle, the greater the inherent risks; thus additional security precautions may be required. It’s best to discuss with clients and your IT department or vendor.

3. Protect your computer communications from eavesdropping. If you use WI-FI at home, make sure your network is set up securely. Specifically, look to see if it is using WPA2 or WPA3 security. Make sure your password on your network is also strong. Pass “phrases” are now viewed as more secure than pass “words.”

---

1 WPA means WiFi Protected Access. WPA became a standard in 2003. WPA2 followed with additional security in 2004, and WPA3 was rolled out in 2018. If you are not sure of the type of WiFi security you have, the age of your router may provide a clue.
4. If your organization has a VPN (virtual private network), use that to connect to your work environment with your remote device(s). If not, consider using your own VPN. You can find numerous providers online for computers. These VPN providers also enable you to use the VPN with your phone, tablet, iPad, and other devices.

5. Keep your computers and mobile devices patched and updated. Most operating systems provide an option to check and install updates automatically. Enabling the automatic update option is a good idea if you do not want to check for updates periodically. This also mitigates the threat of “zero-day” attacks that can sometimes occur on the same day an update is released.

6. Be on the lookout for phishing emails related to remote work. Do not click on anything that looks suspicious. Hackers and scammers will try to take advantage of the COVID-19 situation. Lawyers and law firm personnel are attractive targets for ransomware and malware because they sometimes have client data, confidential information on client business strategies, and other confidential information. Law firms may also have information that can serve as the gateway to their client’s systems.

7. Implement encryption options to ensure that confidential information requires a password or “private” key for access. Encryption can also be used on laptops, smartphones, and tablets. There are a number of companies that offer third-party encryption services including ShareFile or Citrix Mimecast. When in doubt- ENCRYPT!

8. When using the share screen feature of ZOOM\(^2\), BlueJeans, WebEx, or other video conferencing technologies, be mindful that your desktop can be viewed by all participants. This creates confidentiality concerns. For example, using a virtual background can prevent viewers from seeing notes or other information in your work area.

9. Be mindful of confidentiality issues if using an Amazon Echo or similar device in the same room as your remote office. These devices collect and store data. The accumulated voice recordings (your “history”) should be deleted after any confidential audio communication.

10. Be mindful of specific laws relating to data privacy. If dealing with the clients in the EU, the General Data Protection Regulation is applicable. Also, there are new data privacy laws in several states including California and New York that need to be considered.

11. Take measures to safeguard any client information if using web-based cloud storage.

---

\(^2\) Check out Craig Ball's blog on how to prevent Zoom "bombers" by implementing available security tools in Zoom: [https://craigball.net/2020/03/23/protect-your-meetings-from-zoom-bombers/](https://craigball.net/2020/03/23/protect-your-meetings-from-zoom-bombers/). Also see the helpful tips in the following article about "ZoomBombing": [https://techcrunch.com/2020/03/17/zoombombing/](https://techcrunch.com/2020/03/17/zoombombing/).
Confirm that the cloud provider provides encryption both “in transit” (uploading and downloading) and “at rest.” Confirm that: (i) the provider offers other robust security measures, (ii) the data is readily available, and (iii) the provider will not retain the data beyond your request for storage.

**Resources**

ABA Model Rules of Professional Conduct

The ABA Legal Technology Resource Center Website
[www.americanbar.org]>groups>departments_offices>legal_technology

The ABA Cybersecurity Legal Task Force Website
[www.americanbar.org]>groups>cybersecurity


ABA Formal Opinion 477R –provides guidance to assess the security necessary to protect client information.


David G. Ries, *2018 Cybersecurity*, TECHREPORT, January 18, 2018
[www.americanbar.org]>groups>techreport>ABATECHREPORT2018

The ABA Standing Committee on Law and National Security and the Health Law Section webinar, Remote Working in a Time of COVID-19: Cybersecurity Issues You Need to Know, is available on demand and free for ABA members at:
[https://www.americanbar.org/events-cle/ecd/ondemand/398558739](https://www.americanbar.org/events-cle/ecd/ondemand/398558739)

“The ABA is offering a free webinar Wednesday, April 8 from 2:00 PM - 2:30 PM ET, which will feature David Hepburn, the Global President of Actionstep, a cloud-based practice management software company. The webinar will focus on impacts of COVID-19, innovative tools and practices for remote practice management and client communications and a Q&A session. A registration link is available at:
[https://umsystem.zoom.us/webinar/register/5215846451807/WN_9hQxoWJRTTqGXOWopMNsvG](https://umsystem.zoom.us/webinar/register/5215846451807/WN_9hQxoWJRTTqGXOWopMNsvG) .