PRACTICAL GUIDE TO WORKING FROM HOME

FOR FELLOWS WITH SOLO AND SMALL FIRMS DURING COVID-19

ZOOM SECURITY

We are using video conferencing applications more than ever while working from home during the Covid-19 emergency. We use them to stay in touch with other professionals and with our clients. *Technology may change but our ethical obligations do not.* Unlike our big-firm colleagues who have IT departments to handle the technology, solos and small firm lawyers must manage both the technology and the ethical issues. This article looks at both types of issues arising from the Zoom video conference tool.

Applicable Ethical Rules

We must always be mindful of Model Rule of Professional Conduct 1.6(c): "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." To determine what is reasonable, we look to MRPC 1.1, which requires us to be competent. Comment 8 extends that duty of competence to technology: "[A] lawyer should keep abreast of … the benefits and risks associated with relevant technology …." Some states now even require annual technology training as part of the lawyer's CLE obligation. *See, e.g.,* 27 NCAC 1D.1518(a)(2) (available at this link) (last accessed April 12, 2020).

Our ethical duty is not situational. This state of emergency doesn't absolve lawyers of our duties. It may influence what is reasonable, but the underlying duty to protect our clients' confidential information persists. It is therefore relevant that soon after many solos and small firms began using Zoom, concerns about that specific application's security and privacy practices came to light.

The goal of this discussion is not to single out Zoom as good or bad. This discussion reflects only that it is already widely used and having to learn a new program now would add stress during an already stressful time. But we can't bury our heads in the sand and refuse to change if we need to. Lawyers have an ethical duty to evaluate the security and privacy issues.

One reason Zoom is so prevalent is the ease of downloading the app and immediately using it with hardly any learning curve. That is part of the

problem we face. *It is too easy to use Zoom without taking the time to learn to use it properly.* One can start using it without ever looking under the hood, so to speak, at the settings needed to enhance security and privacy. (Your author sheepishly admits to doing this himself.) Fortunately, the developer has reacted quickly to take these concerns seriously. Note that the enhanced security is for the paid versions. As with other software, you must pay for it to get the full benefit.

Improved Security

The company is offering training for its users to enhance their security:

> **STAY SECURE**
>
> **Privacy and Security Resources**
>
> **Resources by CrowdStrike:** Cybersecurity in the time of COVID-19
>
> **Blog:** How to Keep Uninvited Guests Out of Your Zoom Event
>
> **Blog:** Best Practices for Protecting Your Zoom Meetings
>
> **Blog:** Secure Your Zoom Meetings with Waiting Rooms

https://zoom.us/docs/en-us/covid19.html (last accessed April 12, 2020). Moreover, on April 1, 2020, the company announced a 90-day plan to address security concerns that you can access through the link embedded in this sentence (last accessed April 12, 2020). The CEO and Founder, Eric S. Yuan, promptly began a series of weekly "Ask Eric Anything" video conferences on April 8, 2020 (last accessed April 12, 2020). Articles about Zoom security have become a cottage industry. With a hat tip to Tom Overbey, Former Chair of the Technology in the Practice Committee, see, e.g., this zdnet article: make-sure-your-zoom-meetings-are-safe-by-doing-these-10-things (last accessed April 16, 2020). This article will take a more in-depth look at the security issues after addressing privacy and recommending how to use Zoom.

Privacy Concerns

In addition to the security issues, Zoom has had some questionable privacy practices. Some of these involve the ability of hosts to keep track of who is using other programs on their computer instead of focusing on the meeting. There have also been reports that hosts could view presumably private

chats. These are problems with the hosts' privacy practices and not with Zoom as a company. The lessons here extend beyond any one software platform:

- Give your attention to the matter at hand. You're not as good at multi-tasking as you think.
- Don't put something in writing that you don't want others to see.

There have also been questions about Zoom's privacy practices as a company. *See* this blog post dated April 3, 2020 by renowned security guru Bruce Schneier (last accessed April 12, 2020). Mr. Schneier claims that Zoom has been cagey about how it has used its customers' personally identifiable information. At the risk of disputing an expert, this author thinks Mr. Schneier's blog post was argumentative and pre-emptively cast doubt on what seems to be Zoom's subsequent sincere commitment to protect its customers. For example, Mr. Yuan states that while Zoom uses a third-party billing engine, "we never share any user data from meetings" because "selling data has never been part of our business model." Summary of "Ask Eric Anything" April 8, 2020 video conference (last accessed April 12, 2020).

The watchdog group Citizen Lab reported on Zoom's use of Chinese servers to handle overflow traffic. The company acknowledged that using the Chinese servers was a mistake that won't be repeated. Beginning April 18, 2020, users will be able to select the data centers through which their data is allowed to travel. Zoom Blog dated April 13, 2020: coming-april-18-control-your-zoom-data-routing (last accessed April 16, 2020). It's easy to understand that the company has made a few missteps while being overwhelmed by new customers looking for an easy way to work from home.

The question then becomes whether Zoom is safe to use while the company endures its growing pains and engages in its self-imposed 90-day timeframe to improve security. **This article concludes that Zoom can be made safe to use for most matters by taking the following steps, but cautions that we must monitor the validity of that conclusion during its 90-day plan:**

- Use a paid version to get the full security benefits.
- Encourage other participants to download and use the Zoom app instead of their browser.

- Spend time with Zoom's security settings to understand them and tailor them to your needs.
- Use a randomly generated meeting ID instead of a permanent Personal Meeting ID.
- Use password-protection for all Zoom meetings, especially ones discussing confidential information.
- Use the Waiting Room to screen meeting participants. You can customize it with your own branding and a message to participants.
- Don't let people join the meeting before the host.
- Lock the meeting attendees once everyone is present.
- Don't allow screen sharing unless the host invites it.
- Don't use Zoom conferences to obtain account numbers, social security numbers, and the like. In addition to the security concerns, it's tedious and error-prone to write down those numbers.
- Consider alternatives for extra-sensitive information or clients asking for heightened security.
- Subscribe to and read Zoom's blog and weekly "Ask Eric Anything" presentations.
- Participate in Zoom's security training.
- Stay informed about Zoom's commitment not to share your or your clients' personally identifiable information with others.
- Search for updates about Zoom's security from respected sources several times a week. (The world is changing quickly so constant due diligence is called for.)

- Follow Zoom's progress implementing its 90-day plan.
- If you do not need a video conference, use your phone.

This article will now focus on two of the common security concerns about this popular app.

Zoom Bombing

One concern is *Zoom bombing*, where someone (hereinafter a "jerk") interrupts a meeting and may even use the screen sharing function to publish pornography or something else inappropriate. This is more likely to happen in a meeting that has been announced in an open forum, such as a social media post. It can, however, happen if the jerk guesses the 9- or 11-digit meeting identification number. Of course, there are programs to help jerks guess those numbers. *See* this recent article about how hackers do this (last accessed April 12, 2020).

Zoom bombing, however, should not be a problem in password-protected private meetings involving only a few participants who have received a personal invitation. The meeting invite should include the password embedded in the link so the invited participants don't have to type it in. Even if the jerk guesses the meeting identification number, he won't be able to guess the password. **The biggest lesson here is to adjust your Zoom settings to always require a password**.

There are some other helpful tips. Use the Waiting Room feature to control who enters the meeting. Change your settings so that persons have to ask to share their screen. Finally, lock the meeting once all the participants have joined.

Status of Encryption

A more serious concern is the lack of true *end-to-end encryption*. True end-to-end encryption means that only the participants in the video conference can decode the transmission and see the video. Jim Lamm, the Chair of the Technology in the Practice Committee, points out that this issue involves the concept of keys. Encryption requires the use of keys. Just as a hotel manager has a master key and could possibly spy on guests, Zoom has a key and *could possibly* decrypt the users' video call. *See* this article dated March 31, 2020 on The Intercept (last accessed April 12, 2020). Zoom has responded to this concern in two positive ways.

First, it is working to allow the customer to generate the key. In his first weekly address, the CEO stated that the company was focusing on rolling out improved encryption "over the next 45 days." Summary of "Ask Eric Anything" April 8, 2020 video conference (last accessed April 12, 2020).

Second, Zoom forcefully denies ever having spied on its users: "**Zoom has never built a mechanism to decrypt live meetings for lawful intercept purposes, nor do we have means to insert our employees or others into meetings without being reflected in the participant list.**" Zoom blog article dated April 1, 2020 (bold emphasis in original) (last accessed April 12, 2020). This sounds like the way that companies like Apple don't design a way to unlock cell phones so they won't have to do it for government investigators. Consumers demand privacy and punish companies that ignore it. Zoom seems to recognize this and to be responding appropriately.

Zoom's published statements go a level deeper and distinguish between encryption of video conferences when all the participants have downloaded and are using the Zoom app and ones where participants are taking part by means like conference room equipment. If one of the participants is using a phone or a conference room setup, Zoom acknowledges that it decrypts the incoming transmission at its server before sending it to the other device. "When users join Zoom meetings using devices that do not inherently use Zoom's communication protocol, such as a phone (connected via traditional telephone line, rather than the app) or SIP/H.323 room-based systems, Zoom's encryption cannot be applied directly by that phone or device." Zoom blog article dated April 1, 2020 (last accessed April 12, 2020). Indeed, this may be necessary to work with the wide variety of users' hardware. **The lesson here is to use the app — assuming you are comfortable with Zoom's use of your and your clients' personally identifiable information**.

The Ethics of Zoom Use

Despite the positive statements Zoom is making, concern remains because of the reports of Zoom's questionable practices prior to its recent response. The question then becomes the interaction of that concern, the company's past actions, judgment about its stated commitment to security and privacy, and a lawyer's duty under MRPC 1.6(c) to make "reasonable efforts" to prevent disclosure of confidential information.

Can we trust the company's promise to do better? Zoom's definitive statements accompanied by its proactive 90-day plan sound convincing that

Zoom is and will be safe to use for private meetings. What process should we follow to ethically make that judgment?

ABA Formal Opinion 477R (published as revised on May 22, 2017) (last accessed April 12, 2020) guides our discussion. That opinion stated that is not *per se* unethical to use unencrypted email, but there will be circumstances where the lawyer must use encrypted email. Moreover, some clients will insist on it. *While our ethical duty is not situational, how we comply with it is*. The need for security varies with the circumstances. The opinion discusses the factors to be considered when deciding whether to use heightened security. Each of us must apply those factors and make our own judgment call. Zoom may not always be appropriate, and it makes sense to be careful about the information discussed on a Zoom video conference.