Business Law
summer 2020

Legal Matters®

Let's Zoom: The legal challenges of the videoconferencing explosion

Videoconferencing isn't exactly new, and many people have been using Skype or FaceTime for face-to-face conversations for quite some time.

But it's no secret that the pandemic opened many more businesses to regular videoconferencing through a host of readily available tools, including Zoom.

What many business owners might not be thinking about are the possible legal risks associated with the widespread use of these platforms. Generally, the tools companies are using were intended for more casual or smaller-scale use.

Let's start with Zoom, which is now popular from day-to-evening, for everything from a client meeting to a virtual happy hour.

In March, the Office of the New York Attorney General sent a letter to Zoom expressing concerns about the platform's "existing security practices." The letter stated that those practices might not be "sufficient to adapt to the recent and sudden surge in both the volume and sensitivity of data being passed through its network."

Specifically, the letter stated a cybersecurity concern that "malicious third parties" could access users' webcams, an issue that has occurred with platforms like this before.

The same day that the New York Attorney General sent the letter, the FBI's Boston Division issued a statement warning users about the hijacking of videoconferences and online classrooms, something that's come to be known as "Zoom-bombing."

©fizkes

While Zoom has been singled out in the conversation around videoconferencing due to its sharp rise in popularity, the privacy issues are not specific to Zoom. The issue lies in the fact that such platforms are now being used on a much bigger scale and before businesses have considered the legal concerns or trained their employees on those

continued on page 3

ALLRED, BACON, HALFHILL & YOUNG, PC
11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

Protecting trade secrets when your team works from home

©maxkabakov

Any proprietary information that belongs to your business might be a "trade secret" or protected confidential information.

Trade secrets are a type of "intellectual property" owned by your business and they are protected by law. You can require people who work for you to keep trade secrets confidential.

Under federal law, a trade secret is defined as information from which your business gains "independent economic value" and which is not generally known to others. Also, you, as the owner of the information, must have taken "reasonable measures" to keep the information secret. Similar definitions also exist under the laws of most states.

While determining whether "reasonable measures" have been taken requires a fact-specific analysis, it generally includes such things as informing your employees, vendors and others about the proprietary nature of the information, noting that in business documents and employee handbooks, and transmitting the information only in secure ways, both physically and electronically.

When your team comes into the office, it's easier to control their access and how they do and don't share protected data. However, when some or all workers shift to teleworking, it's a different story.

Especially in smaller businesses, many employees use personal computers or laptops at home and their own WiFi connections, which might have less security in place. The next thing you know, your trade secrets are out of your control.

The key to protecting your business is to be sure you're taking reasonable measures to secure your trade secrets.A recent case from Illinois highlights the issue. A federal court there held that a company failed to take reasonable measures to protect its trade secrets when it gave its employees access to a shared drive, gave the same password to multiple employees, failed to encrypt files on the shared drive and didn't restrict employees' use of the material that contained the trade secrets.

Several other court cases have ruled similarly in cases with somewhat related fact patterns. Clearly, the risk can be even greater when employees are working from home, and that means being even more careful with your trade secrets.

Here are some suggestions on how to do it. Your business attorney can advise you on the details for your particular company.

Develop a work-from-home policy for confidential company information. Make sure it's clear what information you're trying to protect and ask your workers to sign the policy before you give them access.

Teach employees about cybersecurity. Give your workers guidance on malware, phishing scams and other ways information can be compromised while working online.

Add confidentiality statements when people log-in. Create a pop-up to make this apparent and consistent.

The key to protecting your business is to be sure you're taking reasonable measures to secure your trade secrets.

Provide company laptops for home use. It's ideal if you can provide secure devices for your team to use at home, and allow them to log-in only through secure servers.

Create procedures for secure remote access. A great way to do this is to require two-step authentication for your team to access your networks.

Password protect all company databases. Provide a unique password for each user.

Make rules for how hard-copy information is managed. One way to do this is to tell employees they cannot print or copy company materials without your permission. They could also be required to keep files in locked file cabinets. And all documents should be shredded when they are no longer needed.

Prepare for when employees leave or are terminated. Be ready to terminate access to all networks, databases and devices if someone leaves the company under any circumstances.

We welcome your referrals.

We value all of our clients. While we are a busy firm, we welcome your referrals. We promise to provide first-class service to anyone that you refer to our firm. If you have already referred clients to our firm, thank you!

The legal challenges of the videoconferencing explosion

continued from page 1

concerns.

Often, videoconferencing platforms run through data centers that are located in other countries, and businesses using them might not even know where. The result is that users' data might be exposed in places that don't have the same privacy protocols as the U.S.

While this could be a risk if you use these tools to chat among family and friends, the risk rises to a higher level when you use videoconferencing for a business negotiation or to obtain sensitive information from a customer.

One seemingly helpful tool offered by these videoconferencing platforms is the option to record the chat. However, the federal government and all states have laws that require at least one party to consent before recording a private conversation. In the following states, all parties must consent: California, Delaware, Florida, Illinois, Maryland, Massachusetts, Montana, New Hampshire, Pennsylvania and Washington.

Failure to get consent can rise to the level of criminal wiretapping.

In the past, recording these conversations wasn't always the easiest thing to do, so most businesses didn't think about training employees on the issue.

However, the current tools make it possible to record a conversation with just one click. That means someone who works for you could easily record a conversation without thinking anything of it.

It's also hard to set any controls on the videoconferences connected to your organization. The sudden rise in working from home means people are quickly setting up their video calls through personal accounts, over which you don't have any control.

It's also important to think about it in the reverse. That is, you or someone who works for you could be recorded in a video chat with another vendor, client or customer.

In fact, even before the recent surge in video calls for business cases where recorded calls were used as evidence in business disputes were already on the rise.

It's important to speak with a lawyer who can give you specific guidance for your business, but here are some ways you can minimize your risk.

Set up company-wide software for videoconferencing. With enterprise software implemented for everyone who works with you, it is easier to put limits on the use of the platform.

If you use other video options such as Zoom, mute the audio. Consider using the video function in tandem with your company-based phone conferencing for audio.

Use the private meeting function. In Zoom, there are two options for making a meeting private: requiring a meeting password or using the waiting room feature to control who can enter.

Provide the meeting link privately. Be sure to email your meeting link only to invited parties, and do not share it on social media.

©fizkes

Confirm that you and your team are using updated versions of all software. Zoom updated its software in January of this year, including a security update, which added passwords as the default for meetings and made it impossible for a user to randomly scan for meetings to join.

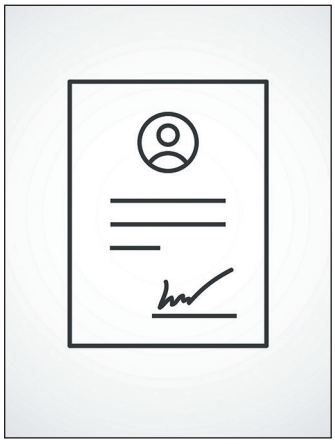
Use the "Host Only" setting for screensharing in Zoom. This minimizes the risk of privacy breaches.

Conduct quick reviews on the possible risks of any platform you use. Be ready to adjust quickly to any security or privacy concerns, both for yourself and your workers.

Train your employees right away. Provide guidelines for employees on best practices, including a ban on recording unless all parties consent, just to be safe. Advise employees that anything they say could be recorded, and update all policies to match with your company's best practices.

ALLRED, BACON,
HALFHILL & YOUNG, PC
11350 Random Hills Road, Suite 700 | Fairfax, VA 22030
(703) 352-1300 | admin@abhylaw.com | www.abhylaw.com

Tips for executing agreements electronically



Electronic execution of agreements is quickly becoming more commonplace in most businesses.

But how can you obtain authorized e-signatures and be sure it is a sound agreement?

Contract formation is generally governed by state law rules, and the requirements are similar for a virtually executed contract:

- The agreement must state that the customer consents to enter into the agreement electronically.
- There has to be a way to identify the individual electronically signing the agreement.
- The process for obtaining the other party's signature must indicate their promise to enter into the agreement. This is called "actual expression."
- The signer must have the authority to execute and deliver the agreement on the customer's behalf.

When you are making an agreement with an individual, it's relatively easy to confirm that the person had the authority to enter into the agreement.

However, when you're making an agreement with another business, it can be a little dicey. In such a situation, when someone on the other side clicks the "I agree" button, it might be unclear who actually did the clicking. Further, it might be unclear whether the e-signer is authorized to make the agreement on the part of the other business in the first place.

To protect yourself and end up with a legally executed agreement, make sure that the agreement is e-signed by someone who is authorized to do so and that the signer is truly agreeing to enter into the terms contained in the contract. Either include procedures to confirm the identity of the person clicking "I agree" or use a third-party service to authenticate that person's identity.

Consult a business attorney to confirm that you are managing your electronic agreements in a way that makes them enforceable.