Schulte Roth&Zabel

Alert

Videoconferencing: Tips for Schools to Navigate Security and Privacy Risks

April 14, 2020

The COVID-19 pandemic has resulted in a dramatic increase in the use of web-based video and audio conferencing ("WC") services by schools, as most, if not all, schools have been closed and students are attending virtual classes from home. While the availability of this technology is not new, and in fact has been widespread in some industries for several years, many schools are adopting WC for the first time or relying on it in new ways. With its expanded adoption and use, the security and privacy issues associated with the use of WC technology have come into the spotlight. For example, Zoom has become subject to attorney general inquiries in New York, Connecticut and Florida and several lawsuits citing security and privacy concerns.[1]

On March 30, 2020, the FBI's Boston field office issued a warning after numerous accounts of WC hijacking, colloquially referred to as "Zoombombing" or "Zoom raiding," with an emphasis on two incidents involving schools in Massachusetts, namely:

- In late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialed into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction.
- A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.[2]

As a result of these concerns, on April 4, 2020, the New York City Department of Education ordered its teachers to stop using the videoconferencing platform Zoom, at least until the data privacy and security issues are resolved.[3] In addition to schools, instances of hijacking reported in the media have focused on the use of WC by religious groups and public service organizations such as AA, where intruders have

[1] *See*, e.g., https://www.cnbc.com/2020/04/03/zoom-probed-by-three-states-for-potential-privacy-violations.html; htpps://www.cnet.com/news/zoom-every-security-issue-uncovered-in-the-video-chat-app/.

[2] *See* https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic.

[3] *See* http://www.nydailynews.com/new-york/education/ny-education-officials-stop-zoom-remote-learning-20200404-vzicdsvzmvd2llmnu3gevszeeu-story.html; https://www.cnet.com/news/school-districts-reportedly-ban-zoom-over-security-issues/.

posted hateful, pornographic or otherwise offensive and disruptive content, often by exploiting a publicly-posted meeting link.[4]

These alarming developments highlight the serious concerns presented by the use of WC services for distance learning, where unauthorized access could disrupt and disturb classes and lessons. Unauthorized access also has implications for the privacy of students and faculty, whose personal information may be discussed or displayed during a lesson or one-on-one meeting between a student and a teacher.

Finally, schools should be aware that use of third-party WC service providers for distance learning may raise compliance issues under the Children's Online Privacy Protection Act ("COPPA"). COPPA only applies to operators of commercial websites and online service providers, so it generally does not impose obligations on schools. However, the Federal Trade Commission ("FTC") issued guidance on April 9, 2020, indicating that, in the educational context, schools can consent on behalf of parents to the collection by WC service providers of student personal information under certain circumstances.[5] Accordingly, with WC service providers likely to look to schools to obtain consent under COPPA, school administrators should be aware of best practices in this area as well.

As discussed in this *Alert*, there are a variety of measures schools can take to mitigate the security, privacy and indirect compliance risks associated with conducting distance learning through the use of WC services.

WC Services Technology

Generally speaking, WC services use software and hardware to permit remote users to connect and exchange live video, audio and written content, through laptops, desktops, smart phones and similar computerized devices. WC vendors provide users with the software and hardware that enables such communications. WC software offers users various features, which vary across service providers, but typically include access controls (used by a host to manage participant access to a meeting), meeting recording, screen sharing and live chat among the users.

Best Practices for WC Platforms

Many schools are using Zoom, Microsoft Teams or Google Meet for their WC solutions. Irrespective of the platform utilized, however, school administrators should evaluate their use of WC services and adopt reasonable measures to protect the security and privacy of WC communications. Below is a list of best practices, compiled based on guidance from the FBI and IT experts, that can serve as points of reference:

1. *Run the Latest Version of WC Software.* WC service providers periodically release new versions of, and updates to, WC software that are intended to address security vulnerabilities, fix known bugs or provide new features or functions (some of which may be useful in improving the security of the WC services). Updating to the latest version of software is critical to keeping in step with bad actors as they find new ways to hack or disrupt WC services.

[4] *See*, e.g., https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html.

[5] *See* https://www.ftc.gov/news-events/blogs/business-blog/2020/04/coppa-guidance-ed-tech-companies-schools-during-coronavirus.

2. *Configure the WC Software with Robust Security Controls.* Although specific features vary by service provider, WC software generally contains controls that give a meeting host substantial control over an invited participant's access to and use of the WC services. When setting up an account, consider establishing defaults that enhance the security of meetings and don't allow the default settings to be changed, such as:

    a. *Use Unique Meeting IDs*. A meeting ID is one piece of information that is used to gain access to a particular meeting. In some WC configurations, meeting IDs are associated with specific users rather than with specific meetings (so all meetings initiated by a user have the same meeting ID). To prevent unauthorized access by persons who received the meeting ID for a prior meeting held by the same host, configure the WC software to generate a unique meeting ID every time a new meeting is created.

    b. *Require Passwords.* Some WC services may permit participant access to a meeting without a password. Require strong passwords for meeting access and do not allow passwords to be disabled by individual users.

    c. *Use Multifactor Authentication*. If available, use multifactor authentication for the meeting host.

    d. *Use Meeting Access Controls.* WC services allow the host to control participants' access to a WC meeting. Wherever feasible, hosts should leverage these controls to enhance meeting security as follows:

        i. *Waiting Rooms.* Waiting rooms allow a host to virtually assemble participants before starting a meeting. Using this feature allows the host the opportunity to validate that only invited participants have joined the meeting before any information is shared.

        ii. *Meeting Locks.* Meeting locks allow the host to restrict a participant's access to a meeting until the host has started the meeting and to prevent any new participants from joining a meeting after it has started.

        iii. *Other Tools.* Some WC services allow a host to mute specific participants or remove them altogether from a meeting. Hosts should be prepared to use those tools as necessary to protect the integrity of a lesson or other meeting.

    e. *Turn off Screen Sharing.* WC services allow teachers and other participants to share their screens. Consider disabling the screen sharing function for all participants except for the host and any other presenters, unless it is required.

    f. *Turn off Recording.* If a WC service allows a meeting to be recorded for playback, disable this feature. If a meeting needs to be recorded, to retain for purposes such as asynchronous learning, consider disabling the recording feature for all participants except for the host and, after the meeting ends, ensure the host downloads a copy.[6]

    g. *Turn off Chat.* Many WC services permit participants to chat by live text. Disable this feature unless it is necessary for the lesson. If chat is enabled, it should be configured so

[6] Schools should provide guidance to personnel about whether/when to record video conferences, as well as how copies of videoconferences are stored, for how long and who can access them based on the nature of the lesson or meeting.

that only messaging among the host and all participants (vs. private messaging between participants) is permitted.

h. *File Sharing Settings.* If a WC service allows file sharing, disable this feature unless it is necessary for a lesson and an alternate school-approved resource, such as Google Docs, is not available.

3. *Use an Enterprise Solution with Sufficient Security Features.* WC vendors provide both personal (or "consumer") and enterprise versions of their software, and many vendors offer versions specifically for schools. Schools should purchase an enterprise solution that supports a sufficient number of participants and provides the necessary functionality, including features designed to enhance security and privacy. Free or lower-cost consumer versions often lack a full set of security controls and embed advertising that increases the risk of a security breach and unauthorized collection of personal information from students or other participants.

4. *Claim and Manage Your Domain*. If a WC service allows, claim your organization's email address domain (such as @srz.com) when adding users to your WC services account. Users with the specified domain (e.g., teachers and administrators) will be prompted to join your WC services account and, therefore, be held to the security and privacy configurations set at an enterprise level.

5. *Educate Faculty, Students and Parents.* Send a communication to faculty, students and parents about the potential risks associated with WC services and best practices, including direction on how to use the controls discussed above. Send updates and reminders to recipients, particularly if the risk may be elevated (e.g., reports of a pervasive hacking scheme).

6. *Conduct Diligence on and Monitor WC Vendors*. Schools should remember to conduct and document the findings of cyber diligence on WC vendors, as for any other information technology vendors.[7] Diligence should be conducted not only when the vendor is engaged but also on a periodic basis thereafter. Schools should also stay up to date on threat communications and responses from WC vendors. WC-related security and privacy issues tend to arise with relative frequency and, similarly, are addressed by vendors on an ongoing basis. Since the COVID-19 pandemic hit, many WC vendors have changed or clarified their privacy practices and issued tips for enhanced security.

COPPA Issues

According to the FTC, schools can consent on behalf of parents to the collection of student personal information — but only if such information is used for a school-authorized educational purpose and for no other commercial purpose.[8] In order for a WC service provider to get consent from a school instead

[7] For example, schools should review the service provider's terms of use and privacy policies to confirm they contain limited use rights that state the service provider has access to the content only to the extent needed to provide the WC service to the organization. Most WC service providers, including Zoom, Microsoft Teams and Google Meet, have user policies that make clear that, as between the vendor and the customer, the customer owns and controls (and is responsible for) the content of the meetings. Additionally, schools that plan to store recordings with the service provider should review the service provider's terms of use to understand how long the service provider will maintain a copy of the recordings (typically 30 days) and the user's rights, if any, to obtain copies of those recordings.

[8] *See* footnote 5.

of from the parent, the service must provide the school the necessary COPPA-required notice of its data collection and use practices.[9]

In addition, the FTC has provided guidance with respect to best practices, summarized as follows:

1. *Disclosure to Parents*. Identify the WC service provider(s) and services whose collection of children's information the school has consented to, make available to parents in plain, easily understood language, the WC service provider's notice about its data collection and use policies and, where feasible, let parents review the personal information collected.
2. *Do Not Let Individual Teachers Select the WC Service Provider*. Schools should decide whether a particular site's or service's privacy and information practices are appropriate, rather than delegating that decision to individual instructors.
3. *Perform Diligence on WC Service Providers*. In deciding which online technologies to use with students, a school should be careful to understand how an operator will collect, use and disclose personal information from its students. Among the questions that a school should ask potential operators are:
    - What types of personal information will you collect from students?
    - How do you use this personal information?
    - Do you use or share the information for commercial purposes not related to the provision of the online services requested by the school? For instance, do you use students' personal information in connection with generating targeted advertising or building user profiles for commercial purposes not related to the provision of the online service? If so, the school cannot consent on behalf of the parent.
    - Do you let the school review and have deleted the personal information collected from their students? If not, the school cannot consent on behalf of the parent.
    - What measures do you take to protect the security, confidentiality and integrity of the personal information that you collect?
    - What are your data retention and deletion policies for children's personal information?

With the use of WC services by schools to conduct distance learning likely to continue for most, if not all, of the spring semester, schools are advised to take a close look at how they implement this technology to address appropriately security and privacy risks.

[9] The online notice must state the following three categories of information (1) the name, address, telephone number and email address of all operators collecting or maintaining personal information through the site or service (or, after listing all such operators, provide the contact information for one that will handle all inquiries from parents); (2) a description of what information the operator collects from children, including whether the operator enables children to make their personal information publicly available, how the operator uses such information and the operator's disclosure practices for such information; and (3) that the parent can review or have deleted the child's personal information and refuse to permit its further collection or use, and state the procedures for doing so. *See* Section C of the FTC's COPPA FAQs, available here.

Authored by Mark E. Brossman, Edward H. Sadtler, John C. Garces, Scott M. Kareff, Kelly Koscuiszka and Donna K. Lazarus.

If you have any questions concerning this *Alert*, please contact your attorney at Schulte Roth & Zabel or one of the authors.

Schulte Roth & Zabel
New York | Washington DC | London
www.srz.com