Remote Education by Video Conference: Are You Ensuring Privacy and Security?

By Cameron G. Shilling

Video conferencing is critical for remote education. Schools are using the technology in record numbers to conduct classes, support school events and meetings, provide advising and counseling, and permit students and faculty to connect with friends and colleagues. Like any technology, if not properly managed, video conferencing poses risks to the privacy of students and employees and the security of our personal information. Schools using this technology need to be aware of those risks, and implement safeguards to mitigate or prevent them.

Access and Security Controls

'Zoombombing' is the newest neologism to enter our lexicons, and the most common insecurity. The term derives from a prominent video conferencing application called Zoom, which exploded from about 10 million to 200 million users practically overnight. To participate in a Zoom or other video conference (like Google Hangouts/Meet, Microsoft Teams, Skype, GoToMeeting, Slack, Cisco WebEx, etc.), the event organizer typically emails a link to intended attendees. Without proper security controls, the link can be used by anyone (whether a member of the school community or not) to access the event, and sometimes links are publicized on the school's intranet, website and social media, particularly if the meetings are more broadly open to parents, alumni, and others inside or outside the school community.

Hackers invade video conferences to steal the personal information of the participants, such as names, emails, contact information, photographs, and video images. They also disrupt meetings by overwhelming attendees with offensive content (typically pornography or hateful images and speech), causing the event to need to be terminated. Predators and thieves also covertly penetrate video conferences to gather information about children engaging in classes and school events or connecting with friends, and to acquire details about the home environments of students and school employees. These dangers are exacerbated if hackers have previously installed (or can use the video conference application to install) malware on the computers and mobile devices of those individuals, permitting hackers to control the cameras, microphones, and other applications and information on the computers and devices.

Most video conferencing applications have controls that can be configured to mitigate such dangers. For starters, all conference transmissions should be encrypted. In addition, school event organizers can require students and other participants to enter passwords to access conferences, and can restrict or eliminate the ability of attendees to share content. Schools that operate portals also may be able to deploy the video conference application from the portal, utilizing existing security like multi-factor authentication, password controls, firewalls, and threat detection software. School video conferences also can be established with virtual waiting rooms, permitting school employees to admit only identified and intended students and other participants, or these events can be established as webinars rather than meetings, restricting the ability of the attendees to distribute content or interact with each other.

Notice and Consent, and Secure Retention

Video conference applications commonly either automatically record or permit recording of the content. Given the sensitivity of the information exchanged using this technology, such recording raises significant privacy and security issues. For example, state and federal privacy and wiretap laws require schools to notify and obtain consent from adult students, parents of minor students, employees, and other participants about collection, use, and disclosure of personal information and oral, electronic, and other content recorded during video conferences. As a result, schools should integrate appropriate notice into their video conference applications, and obtain express consent from parents/students, employees, and other video conference participants.

Recorded video conferences also should be securely stored, and the applications permit a variety of retention methods, such as on a cloud, computer or mobile device, or server. Schools should ensure that the retention method selected is secure, including encryption of the recordings and the computer and device hard drives, and use of strong passwords and multi-factor authentication to access such clouds and networks. Additionally, schools should technologically prevent students and unauthorized employees from making their own recordings.

Due Diligence and Agreements

Most video conference providers disclose on their websites the privacy and security controls inherent in their applications, and provide instructions about how to configure those controls. Before using these applications, schools should do due diligence to ensure that the controls are sufficient for their particular uses of the technology, and enable them to comply with the privacy and security laws that apply to the schools as well as the students who participate in video conferences, including HIPAA, COPPA, the California Consumer Protection Act, and the European Union General Data Privacy Regulation. Some video conference providers also will sign agreements that are designed to comply with these privacy and security regulations.

The public health crisis presents a multiplicity of challenges and risks. As schools increasingly adopt technologies like video conference to facilitate remote education, they must implement appropriate measures to ensure that their use of these technologies does not endanger the privacy or security of students, families, faculty, and school employees.

Cam Shilling chairs McLane Middleton’s Information Privacy and Security Practice Group. Founded in 2009, the firm’s team of three attorneys and a technology paralegal assist businesses and private clients to improve upon their information privacy and security compliance, and address any security breach or incident that may arise.