ICoME 2020

International Conference for Media in Education 2020

CONFERENCE PROGRAM

AND PROCEEDINGS

Diversity education in

ICT advanced society

International Conference for Media in Education 2020

CONFERENCE PROGRAM
AND
PROCEEDINGS

Theme
Diversity education in ICT advanced society

August, 17th & 18th, 2020

Oline Cnference
(KOBE・ JAPAN)

Zoom In (but Fasten Your Seatbelt)

Tamara Fudge
TFudge@purdueglobal.edu
Professor
Purdue University Global
Indianapolis, USA

Lynne Williams
Lwilliams4@purdueglobal.edu
Professor
Purdue University Global
Indianapolis, USA

The year 2020 has presented many challenges, not the least of which is the COVID-19 pandemic forcing schools to temporarily close for the spring semester. Along with the instant need for students to obtain computers and internet service was the faculty's hasty retooling of content delivery and assessment into an online format. Video tools – especially Zoom – became the method of choice for this unscripted and unexpected online learning due to the relative ease of use, similarity to face-to-face lecturing, and the fact that the basic service is free. Unfortunately, Zoom was not ready for the onslaught, and security issues and other problems were discovered; over the course of many weeks, the owners of Zoom were forced to make changes as each new problem emerged. The result of the research and analysis points to the use of Zoom and other video tools as an adequate stop-gap measure for online learning, but with the caveat that faculty need to be aware of the flaws and understand how to best mitigate them.

Key words: teleconferencing, webinar, online teaching, online security, Zoom

INTRODUCTION

The Covid-19 pandemic has radically changed the K12 - College teaching landscape overnight. Countless classes that were traditionally taught face to face have suddenly had to retool for the online environment with very little guidance from administrators. The most obvious method for providing a simulated face to face experience appeared to be some sort of video teleconferencing application such as Skype, Google Hangouts, or Zoom. However, in the rush to get classes online, there has not been adequate planning surrounding this shift, particularly regarding security.

Zoom has emerged as the teleconferencing tool of choice, but not necessarily predicated on any practical considerations. Teachers who have not taught online previously may have difficulty using the video tool for a variety of reasons such as device incompatibility, slow broadband, and general unfamiliarity with the online environment. Students may also only have access to slow (or no) broadband as well as a variety of technical issues such as audio lag, freezing, or jitter. In addition, Zoom has suffered from a host of security problems including Zoombombing, privacy issues, and a lack of data encryption.

The issues related to rapidly taking a face to face class online need to be revealed, specifically those involving Zoom as an online teaching tool.

RESEARCH DESIGN AND METHODS

Much information has been shared online since the pandemic quarantine precipitated this problem; secondary data analysis and archival study are the primary method for this research, with some historical

background regarding video conferencing. Anecdotal information was gathered from news sites and other sources to illustrate problems and solutions. Lastly, some observations are made by direct experimentation with the video tools in question.

BACKGROUND: THE PANIC OF MARCH 2020

In March of 2020, traditional K-12 and college education in the United States was caught by surprise by the Coronavirus pandemic. Face-to-face contact was determined impossible due to the obvious physical threat of a dreaded and largely unknown disease. Two main problems immediately surfaced: some students did not have the technology necessary to get online, and the teachers lacked time, tools, and training. The focus here is the latter.

While online programs were already set up for content delivery using sophisticated Learning Management Systems and organized curriculum guidelines and methods, the traditional classroom teacher simply was not trained as an online curriculum designer and multimedia developer. Despite premium tools often being unavailable and administrations largely clueless to provide guidance, teachers had to forge ways to continue instruction by "going online."

For many, this lack of direction – and lack of time – meant the format chosen was simply to "replicate their face-to-face courses online" (Lang, 2020, para. 10). The most logical first response, then, was to try to save the live lecture-style format and use a video tool to reach their students.

The use of video for educational purposes is far from being new. Television was employed as an educational medium as early as 1934 at the University of Iowa (Sleator, 2010). Coastline Community College, the first non-traditional school that actually had no campus of its own, used television in 1976 as one of its methods, transmitting courses through their local Public Broadcast Station (Luskin, 1976). Closed-circuit transmissions were used in that decade to connect multiple rooms of students in a traditional university to the one professor's live lecture (Fudge, 2018).

TOOL CHOICES

Not all video tools are useful for the teaching situation. There are some live meeting applications such as Cisco WebEx and Adobe Connect, but these require payment, which would not have been budgeted by school boards or affordable for the teachers themselves. Free tools would be most logical for this quick transition.

Skype is free but limits attendees to 50, which is difficult for large lecture classes; Google Hangouts only allow 25 people; FaceTime requires an Apple device; Microsoft Teams is gaining in popularity but requires downloading of software, which may be prohibitive for some users (Paul, 2020).

Quickly, Zoom became the tool of choice for completing the spring semester (Paul, 2020). Publicity, ease of use, and the fact that it is free likely aided in its popularity.

TO BE EXPECTED

When using a new online tool, there are some issues that can be expected, including an emotional response. Considine (2020) noted that college faculty who had never taught online reported feeling intimidated, and "students need a bit of curiosity and enthusiasm to even enter the online space" (p. 22).

Some technical issues experienced with Zoom in particular could also be expected. Teachers and students alike might have device issues, broadband problems, or lack of technical understanding. Additionally, technical glitches such as freezing, audio delay, and outages occurred.

It was the *unexpected* issues that provided cause for concern.

ZOOM'S UNEXPECTED ISSUES

Notably, Zoom's original purpose was not for online schooling or the widespread deployment of the application. Lorenz (2020) explains "the platform was built as an enterprise technology tool, not a consumer social tool. As such, the company was not prepared to moderate user behavior as other social networks do" (para. 14).

There were many corrections to make over the first few months of the pandemic. Three complications are especially worthy of exploration: Zoombombing, deepfakes, and the use of gathered data.

Zoombombing

Defined: Someone attending a Zoom session who has not been invited, with the potential for overt disruption (Krebs, 2020).

In the first few months of quickly-designed online learning, many Zoom sessions were held without requiring passwords; this caused some meetings to be disrupted by unwanted individuals and "an alert by the FBI on how to secure meetings against eavesdroppers and mischief-makers" (Krebs, 2020, para. 5). Zoombombing trolls were found to occasionally inject hostile attacks with white supremacist language or pornography (Krolik & Singer, 2020), and plans for an anti-Semitic attack on a Philadelphia Jewish school by 8chan was exposed in early April (Hodge, 2020).

With meeting IDs of only 9-11 characters in length, hacking simply was all too possible, and Zoom finally took the initiative to set all new meetings by default to requiring a password (Krebs, 2020). Even after better security measures were constructed, Oklahoma City University's early May graduation ceremony was hacked with racist content (Wagenseil, 2020).

Passwords alone do not provide full security, of course. In early April, hacking tools such as zWarDial successfully infiltrated 100 meetings in an hour (Krebs, 2020). There is also a troubling setting that allows attendees to share their screens without first asking the host for permission (Lorenz, 2020).

Deepfakes

Defined: The imposition of someone else's face on a different person's body in video format using Artificial Intelligence algorithms (Gerstner, 2020). Audio might well be added or altered to accomplish the perpetrator's goals (Greengard, 2020).

Ethical issues arise from this capability. A sophisticated version of this technology, CGI (Computer-Generated Imagery), is sometimes used in Hollywood movies. One well-known example is the inclusion of Peter Cushing "acting" in the 2016 movie Rogue One: A Star Wars Story despite his passing years before in 1994. The ethics of using the likeness of an actor after his or her death is questioned, and licensing for posthumous activity may have to be forthcoming to protect an estate (Hardawar, 2016).

While not on a Hollywood production level, Zoom has the potential to cause harm. Applications such as Avatarify allow a Zoom participant to exchange someone else's face – such as that of a famous person – for the user's own (Cole, 2020). While it takes some technical knowhow to accomplish this task, the code is freely available and the result is a "neat trick" that would be distracting at best (Cole, 2020, para. 6).

More importantly, Zoom offers video that can be used to attack any other person also in attendance, whether it is the teacher, a guest speaker, or another student. Someone who wishes to create a deepfake in a program such as FakeApp just needs a video of the person who is to be impersonated (Gerstner, 2020); Zoom offers this opportunity, and there are many video capture tools available. A Zoom

session's captured video could be used in pornographic scenes, false news reports, and other videos with the purpose to assassinate the victim's character (Greengard, 2020)

Whether a video is real or a fake is not always easy to determine, but there are some new detection systems that can often analyze facial movements, lighting, and other elements (Toews, 2020).

Gerstner (2020) explains that not only can a deepfake steal intellectual property and "personality rights," it also can invite legal charges of public defamation of character or emotional distress, the latter which can be served through a tort called IIED: Intentional Infliction of Emotional Distress. However, by the time a fake video has been disseminated, detection tools and lawsuits will not erase the damage done to the victim.

Data Tracking

Defined: The collection and analysis of data collected by an application, sometimes through indirect means and typically meant to assist a company in improving products and services for the customer (Freedman, 2020).

Data tracking is common and allows companies to serve their customers better. However, sometimes the data collected is sold or shared with other companies (Freedman, 2020). There are regulations on data capture, storage, and sharing, but it is possible that companies may violate such compliance before they adapt to ever-changing laws (Freedman, 2020).

A privacy policy is a document shared with customers that explains how data is collected, for what purpose the data is intended, and if the data will be shared. Zoom's privacy policy can be reviewed at https://zoom.us/privacy. It was updated in late March and then again in July 2020.

According to Wagenseil (2020), Skype, Webex, Microsoft Teams, Google Hangouts, and other such applications have "questionable privacy policies," as does Zoom ("Friday, May 1"). Even with a written policy, there have been many concerns during the time in question, some of which are shared here.

In late March, it was noticed that Zoom attendees who subscribed to the LinkedIn Sales Navigator tool had been granted access to other people's LinkedIn profile data upon entering a Zoom session (Krolik & Singer, 2020).

Yet another feature affecting those who logged in on their iPhones was found to send user data to Facebook (Krolik & Singer, 2020). Zoom, whose home offices are in California, was summoned with a class-action lawsuit for violations of the state's Data Protection laws for this infraction; other lawsuits were also filed in the weeks following for other problems (Hodge, 2020).

Zoom also had an attendee attention tracking feature. While this may at first seem like it would be helpful to ensure that students pay attention (the teacher is notified if the student clicks outside of the Zoom window and remains there for more than 30 seconds), it should be noted that not all learning is visual; the audio surely would be of value and would not necessitate full pictorial attention (Koch, 2020).

By mid-April, information about a half million accounts had been sold by hackers (Hodge, 2020). By the end of the month, more security issues flowed. One bug allowed hackers access to webcams and microphones, another routed calls through China, a cloud exploit was found, the Federal Trade Commission was asked to investigate, foreign surveillance was discovered to be possible, a particular hack could record a meeting without participants' knowledge, and "bug bounty hunters" started looking for problems they could sell to others (Hodge, 2020).

As late as July 10th there were still problems, such as a bug that would let a hacker commandeer a computer using Windows 7 or earlier versions (Wagenseil, 2020).

Some school districts responded by banning the use of Zoom, Germany warned their citizenry about the dangers, Singapore banned it, Singapore warned their citizens, the U.S. Senate was told to avoid it, and the Pentagon restricted its use; New York City originally banned Zoom but rescinded the ban in early May (Hodge, 2020).

To be fair, Zoom worked to correct issues as they were brought to them. They started offering end-to-end encryption for all users in mid-June, for example, and are working with the New York Attorney General to clean up other security matters (Wagenseil, 2020). They also added a "Report User" button that can be used in a live session (Hodge, 2020). However, these are reactive rather than proactive, so there are still fears that other problems may arise.

OTHER OBSERVATIONS

As previously noted, Zoom was not originally designed as an educational seminar tool, so many of the settings and administrative tools are heavily geared toward business users rather than teachers or instructors. This does not necessarily mean that Zoom cannot be used effectively in a classroom setting, simply that the hosts need to familiarize themselves with the application and be aware of the various settings, particularly in the free version which does not include most of the more powerful administrative tools. For those users who are not particularly technically savvy, this can present a fairly steep learning curve.

The free version gives the host a limited set of tools, including the ability to host meetings. Meetings are geared toward collaborative online gatherings where the participants share information of various types. A Zoom meeting allows the host to mute participants but all participants can be given the ability to unmute their audio, although this may not be desirable in a classroom setting. Participants in meetings can also share video without permission from the host. As of March 26th, 2020, the free version of Zoom meetings will default automatically to screen sharing for "Only Host," which is the safest option to avoid disruption. Free version meetings allow up to 100 participants. In-meeting chat is available in free meetings as are "meeting reactions" and "nonverbal feedback" which are similar to emojis. Closed captioning and recordings are also available in the free version.

When starting a meeting, hosts should check the Security settings (bottom of Zoom Meeting screen) to ensure that they have selected the participant behaviors that they wish to allow; otherwise participants will be able to share their screens and unmute their microphones at will. The Share Screen settings should also be checked and generally set to "Host Only."

Zoom also offers Webinars which differ from Meetings in that Webinars are designed for a lecture style presentation rather than collaboration. Webinars are likely to be the more comfortable option for educators as they give the host much more control over participant behavior. However, webinars are only available with the paid option.

CONCLUSION

It needs to be said that starting in March 2020, Zoom and other video tools served as a stop-gap measure for online learning, and that the unpreparedness of both faculty and their administrations to deal with the quick transition to "teaching online" has had some consequences. Wagenseil (2020) insists that despite the problems, the corrections made by Zoom in the last few months mean it should be safe for use except for discussing trade secrets or personal information such as a health history.

Two sources in particular provided detailed chronologies of Zoom use in early- to mid-2020 and provided some excellent recommendations, as did security expert Brian Krebs:

- Wagenseil (2020) strongly recommends that Zoom be used within a web browser rather than the downloaded software, as the web browser will include the most up-to-date improvements. He also suggested that Zoom session hosts change the default file name for recorded sessions and to remember that anything in a video meeting may be recorded.

- Koch (2020) recommends that attendees avoid logging in with Google mail or Facebook so that the data therein is not shared.
- Krebs (2020) recommends disabling the feature that allows participants to enter the Zoom room before the teacher/host arrives.

In addition, a K-12 or college teacher using Zoom may consider the following:

- To avoid Zoombombers: Ensure that you require a password to enter a Zoom meeting. Insist that students use their real names to enter, not a nickname, so you know who is in the room with you. Know what settings you have chosen when setting up a meeting.
- To avoid being the victim of a deepfake: Consider using a PowerPoint or screenshare instead of showing yourself.
- To minimize undue data sharing: Log in using your web browser, not the application on your desktop or on your phone. Read and understand the privacy policy.

Video is not the only way to teach online, but offers a personalization that is not felt from viewing a website, working from instructions provided in a PDF, or going to YouTube videos. Lederman (2020) points out that the teaching skills needed to teach online are different than in person; while the technology is important, it is the pedagogy designed for online learning that must be addressed as well as the cultural implications of change. This means that the tools are not the only component to consider – although surely the use of any tool must be careful and knowledgeable.

REFERENCES

Cole, S. (2020, April 16). This open-source program deepfakes you during Zoom meetings, in real time. *Vice.* https://www.vice.com/en_us/article/g5xagy/this-open-source-program-deepfakes-you-during-zoom-meetings-in-real-time

Considine, A. (2020, May/June). The Zoom where it happens: Academic theatre programs quickly adjust to remote learning in the age of COVID-19. *American Theatre, 37*(4), 20-23.

Freedman, M. (2020, June 17). How businesses are collecting data (and what they are doing with it). *Business News Daily.* https://www.businessnewsdaily.com/10625-businesses-collecting-data.html

Fudge, T. (2018, Fall). Online learning today: An extension of your grandmother's correspondence course. *Colleague 2 Colleague (C2C) Digital Magazine, 1*(10), 11. http://scalar.usc.edu/works/c2c-digital-magazine-fall-2018--winter-2019/online-learning-today-extension-grandmothers-correspondence-course

Gerstner, E. (2020, January). Face/off: "DeepFake" face swaps and privacy laws. *Defense Counsel Journal, 87*(1), 1-14.

Greengard, S. (2020, January 1). Will deepfakes do deep damage? *Communications of the ACM, 3*(1), 17-19. https://doi.org/10.1145/3371409

Hardawar, D. (2016, December 20). '*Rogue One' is a milestone (and warning sign) for CG resurrection*. Engadget. https://www.engadget.com/2016-12-20-star-wars-rogue-one-cgi-actor.html

Hodge, R. (2020, May 8). Zoom security issues: Zoom buys security company, aims for end-to-end encryption. *CNet.* https://www.cnet.com/news/zoom-security-issues-zoom-buys-security-company-aims-for-end-to-end-encryption

Koch, R. (2020, March 20). *Using Zoom? Here are the privacy issues you need to be aware of.* Security Boulevard. https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/

Krebs, B. (2020, April 2) 'War Dialing' tool exposes Zoom's password problems. *Krebs on Security.* https://krebsonsecurity.com/2020/04/war-dialing-tool-exposes-zooms-password-problems

Krolik, A. & Singer, N. (2020, April 2). A feature on Zoom secretly displayed data from people's LinkedIn profiles. *New York Times.* https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html

Lang, J. M. (2020, May 18). On not drawing conclusion about online teaching now – or next fall. *The Chronicle of Higher Education.* https://www.chronicle.com/article/On-Not-Drawing-Conclusions/248797

Lederman, D. (2020, April 1). Preparing for a fall without in-person classes. *Inside Higher Ed.* https://www.insidehighered.com/digital-learning/article/2020/04/01/preparing-quietly-fall-semester-without-person-instruction

Lorenz, T. (2020, April 7). 'Zoombombing': When video conferences go wrong. New York Times. https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html

Luskin, B. J. (1976). *Coastline Community College: A dream with a reality*. Fountain Valley, CA: Coastline Community College.

Morrison, S. (2020 May 7). Zoom tries to buy its way out of its security problems. https://www.vox.com/recode/2020/5/7/21250560/zoom-keybase-facebook-google-encryption-video-chat

Paul, K. (2020, April 9). Worries about Zoom's privacy problems? A guide to your video conferencing options. https://www.theguardian.com/technology/2020/apr/08/zoom-privacy-video-chat-alternatives

Sleator, R. D. (2010, August 1). The evolution of eLearning background, blends and blackboard. *Science Progress, 93*(3), 319-334. https://doi.org/10.3184/003685010X12710124862922

Toews, R. (2020, May 25). *Deepfakes are going to wreak havoc on society. We are not prepared.* Forbes. https://www.forbes.com/sites/robtoews/2020/05/25/deepfakes-are-going-to-wreak-havoc-on-society-we-are-not-prepared

Wagenseil, P. (2020, July 11). Zoom security issues: Here's everything that's gone wrong (so far). *Tom's Guide.* https://www.tomsguide.com/news/zoom-security-privacy-woes