The University of Washington should transfer from Zoom to Google Meet or Microsoft for online learning

Nisha BK[1]
[1]English 182, University of Washington, Seattle, Washington

Abstract

Zoom has become a prominent online learning tool for college students in and outside of the classroom. Although the application is easy to navigate for multiple purposes, Zoom-bombing, other security issues, and academic censorship has caused controversies around the application. Zoom-bombing, a term that has gained the public's attention, is the result of individuals and groups hacking into Zoom meetings to spread hate speech, pranks, and various other malicious acts. This paper compiles evidence and insight from several research papers preferring the use of Google Meet, or Microsoft Teams over Zoom and how the University of Washington (UW) should reconsider the platform used for remote learning. Google Meet and Microsoft Teams, both have similar functionalities as Zoom like screen sharing, dial-ins and are safer to use than Zoom. Although both Google and Microsoft are large technology companies that have faced security challenges, they are still better to use than Zoom. The technology companies have provided service for longer periods of time, and are catering to larger audiences as a whole through different branches like Gmail, G-Suite, and Office 365.

Keywords: Zoom-bombing, end-to-end encryption, remote learning, video conferencing platforms, COVID-19, Academic Censorship

Introduction

Technology has revolutionized the way students learn by making learning accessible to most through online learning sites, examples include: Canvas, Slack, G-Suites and many more. Online learning platforms have become ever so prominent in the present learning environment due to SARS-CoV-2 which is commonly known to the public as the Coronavirus 2019

(COVID-19). Platforms such as Zoom, Google Meet, Microsoft Teams, WebEx Teams, and GoToMeetings have had a massive flux of usage by customers due to COVID-19 restrictions. These platforms have been implemented and integrated into K-12 education, as well as college education for online learning, and have been the major communication platforms during the pandemic (Singh *et al*, 2020). Zoom, one of the popular video conferencing platforms, is being utilized the most for academic purposes within universities. The University of Washington is one of the universities that has heavily integrated Zoom conferencing within their educational system. Due to Zoom's persistent security issues, and controversial control over academic freedom, institutions should shift towards using Google Meets, or Microsoft Teams instead of Zoom.

Due to Zoom's easy accessibility features like "...screen sharing, screen recording, team chats, and searchable history" (Singh *et al,* 2020), it has become a widely used conferencing application. Prior to COVID-19, Zoom had 10 million users on a daily basis, by March of 2020, its daily users increased to approximately 200 million (Singh *et al*, 2020). The application has the capacity to hold approximately 500 participants at a time and can allow 49 participants to be seen on gallery view (Singh *et al*, 2020). Although Zoom has gained popularity for its ability to provide a way to connect with others while learning remotely, and has provided a platform to remotely learn, the application has faced major security and censorship issues. In regard to the security issues, Zoom has been accused of using clients' personal data in suspicious ways and not having proper security measures (Wagenseil, 2020). Allegedly, the usernames and passwords have been retrieved from the Zoom database and sold on the dark web (Wagenseil, 2020). Although it is not explicitly stated what the usernames and passwords are used for in the dark web, hackers can utilize user login information to access other social media platforms where

Zoom clients might have used similar information. In addition to the security issues, Zoom has been accused of academic censorship. As recent as October 23rd, 2020, a webinar on academic censorship organized by New York University (NYU) was shut down. The webinar was held in response to the cancellation of an earlier event organized by San Francisco State University (SFSU) on September 23rd, 2020, where Leila Khaled, a member of the Popular Front for Liberation of Palestine (PFLP) was scheduled to speak (Lytvynenko, 2020). The American Association of University Professors of New York University (NYU-AAUP) executive committee stated that the censorship and event cancellation is a violation to the mandatory event academic freedom. They also pointed out concerns with the involvement of third-party vendors on deciding what is academically acceptable in online learning platforms like Zoom ("Statement from the NYU-AAUP Executive Committee (10/23/2020)"). According to Zoom, the webinar violated multiple Terms of Service, Acceptable Use Policy, and community standards, but not further information was stated (Lytvynenko, 2020).Whether or not one is a college student, this topic matters to a wider variety of audience such as K-12 institutes, universities/colleges, teachers, students, and parents because data privacy is important for all users. Without data privacy, people could get a hold of viable information like bank account details, and other invasive personal information. It is also a matter of feeling like one had control over what others know about them.

Zoom Security Issues

In April, the New York Times conducted an investigation where they found that people were using numerous sites like Twitter, Instagram, and Reddit to plan Zoom-bombing by sharing Meeting IDs, and passwords (Secara, 2020). Then again on May 12th, 2020, Oklahoma City University's graduation ceremony was interrupted by Zoom-bombers who projected racial slurs and inappropriate behavior during the formal event (Wagenseil, 2020). Additionally, on

November 8th, 2020, Gonzaga University Black Student Union (BSU) experienced Zoom-bombing where the members were attacked with derogatory and racial slurs. The university released a statement on November 11th, 2020 claiming, "…"Zoom-bombing," was shocking, offensive, and hate-motivated act intended to inflict emotional pain and trauma," ("Update On The Hate..." 2020). Due to the severity of Zoom-bombings, the FBI has threatened perpetrators with jail time as punishment for these disruptive campaigns (Secara, 2020). The attackers take advantage of the fact that Zoom clients use weak passwords to make the account, and once they hack into the Zoom account, it is easier to gain access to other applications because most users tend to use the same log-in information. Zoom claimed to be using end-to-end encryption, one of the safest encryption methods because it uses cryptographic keys when processing information (Secara, 2020). End-to-end encryption does not make private messages and information available to people other than the sender and receiver. Instead of using end-to-end encryption, Zoom uses Transport Security Layer (TSL) encryption, which allows the information to go from the user to the Zoom server (Secara, 2020). Figure 1 shows that the information from different Zoom collaborations go through Zoom servers because they use "server-side decryption" (Secara, 2020).

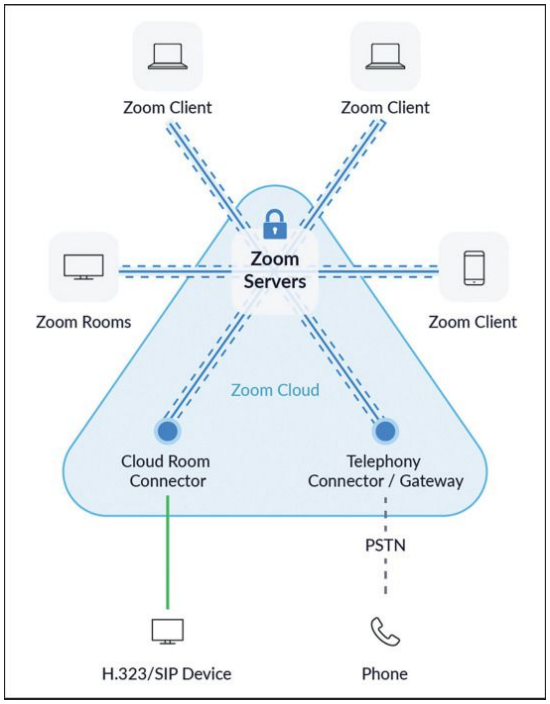

Figure 1. Information communicated through go through the Zoom server. The different branches of Zoom like the Zoom rooms, Zoom clients, and Zoom dial-ins all go through Zoom servers. Reprinted from "Zoombombing – the end-to-end fallacy," by Secara, I.-A. (2020). Network Security.

According to a study conducted by The Citizen Lab, a call between two people, one from the United States, and other from Canada, was traced to a server in Beijing, China (Secara, 2020). Even though Zoom's headquarter is located in San Jose, CA, the company's SEC filing reported three China based companies for aiding the development of Zoom (Secara, 2020). Zoom uses a key encrypted in Electronic Code Book (ECB) called ASE-128, which is the simplest form of ASE key which according to the CEO of Zoom, Eric Yuan, AES-128 is below standards. (Secara, 2020). The CIA recommends using ASE-256 encryption key, the advanced version, with end-to-end encryption, and storing the key securely to avoid hackers and for effective data protection (Secara, 2020). In addition to the security threats from TSL encryption and AES-128 key, using Zoom on a desktop can pose dangers because Zoom can accept requests from any source (Secara, 2020). Alongside data privacy issues, Zoom has faced criticism for censorship.

Zoom Academic Censorship Effects

As online classes have become the primary form of learning due to COVID-19, teachers and students have done their best to accommodate the situation by using Zoom applications. As mentioned previously, Zoom faced backlash from many after the censorship of Palestinian event where Leila Khaled was supposed to speak. Then again, an event assembled to speak out against censorship was canceled by Zoom, which created more outrage from people. Academic censorship can mean different things to people, but in a way, it is to set barriers between education and learners. For instance, if students never learned about colonialism in school, then the way we view society would be different and in turn harmful for obvious reasons. Likewise, when remote learning is the only option, it is important that Zoom is held accountable for these actions.

Zoom, Google Meet, and Microsoft Teams

With the primary focus being on data privacy, and the secondary interest in preserving academic freedom, institutions like the University of Washington should use Google Meet, and Microsoft Teams for remote learning rather than relying on Zoom. All three are video conferencing platforms with similar features and minor differences in functionalities and pricing. Depending on the subscription, Google Meet can hold up to 250 participants, and the integration with other Google applications like Google Calendar make it accessible to join meetings. Zoom on the other hand can allow up to 500 people, while Microsoft Teams allows up to 250. To keep information private, Google Meet uses in-transit encryption, which means that messages are encrypted between Google servers and users. Zoom uses TLS, which does allow the company to decrypt messages and other activities. Microsoft Teams also use in-transit encryption and store data using Secure Real Time Transport Protocol (SRTP) for audio, video, and sharing. Both Google Meet and Microsoft Teams do not have meeting time limits but Zoom only allows free

users with 40 minutes meeting limit unless users upgrade to the version that allows up to 24-hours video conference. Recording video meetings is convenient in Google Meet because they are automatically saved in the Google Drive and can be accessed through Google Calendar. Similarly, recordings in Microsoft Teams take place in cloud and are saved to Microsoft Stream. The meetings can also be shared with people if they were not able to attend. Meanwhile, recordings in Zoom are saved only to the local computer. For screen sharing, Google Meet and Microsoft Teams only allow one person to screen share at a time but Zoom allows multiple participants to do so during the meeting. When hosting remote classes, it is important and convenient to be able to see as many people through the grid view as possible. Google Meet allows participants to see everyone and the main speaker is highlighted. Zoom can fit up to 49 participants using the gallery view, while Microsoft Teams does not make it possible to view every person. For deaf individuals and people who prefer captions, Google Meet and Microsoft Teams offer a live caption feature, which automatically generates captions as the presenter is speaking. On the contrary, Zoom offers a manual caption feature that requires someone to type while the speaker is speaking. Ultimately, all three platforms offer additional features, like Google Meet has intelligent muting, can integrate with other Google Workspace applications, and has emojis and GIFs. Zoom has annotation tools, background features (that is a great conversation starter), and hosts can conduct polls. Microsoft Teams also has valuable features like private channels, email Teams channels through Outlook, and polls (Verbrugghe, 2020). Figure 2 summarizes the functionalities available in Google Meet, Zoom, and Microsoft Teams.

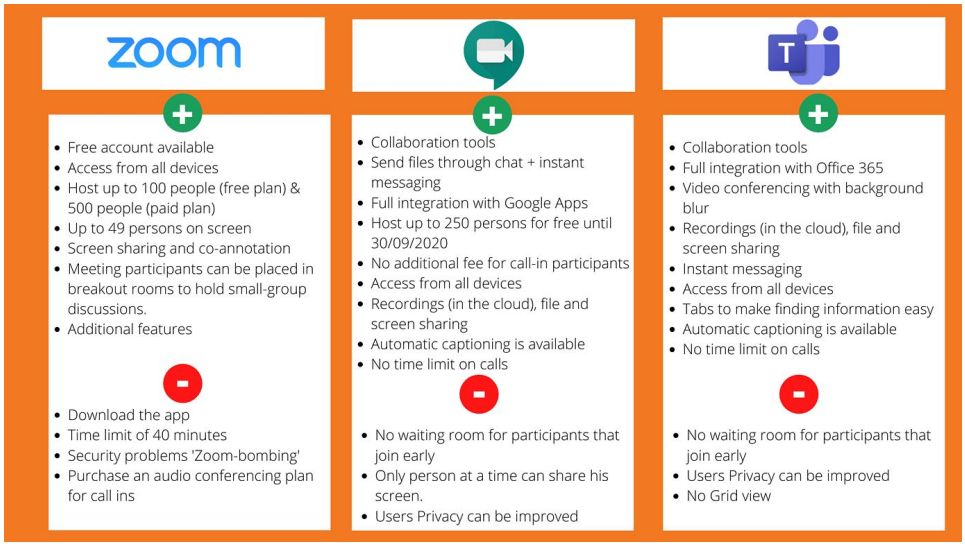

Figure 2. Summary of the different video conferencing platforms. The table summarizes the pros and cons of using the different platforms.Reprinted from "Comparing Zoom, Microsoft Teams and Google Meet," by Verbrugghe, C. (2020, April 10). *Europe Fourcast.*

Pricing

Institutions like the University of Washington need an Enterprise Subscription offered by Google Meet for $25 per user per month. This plan also allows up to 250 participants and live streams as well. Figures 3, and 4 give a summary of different plans and their price points offered by Zoom and Microsoft Teams (Verbrugghe, 2020).

Figure 3. Zoom plans and corresponding price points. There are four different plans users can choose from, and one of them includes a free plan. The University of Washington is most likely to have the Business plan or the Enterprise plan for remote learning. Reprinted from "Comparing Zoom, Microsoft Teams and Google Meet," by Verbrugghe, C. (2020, April 10). *Europe Fourcast.*

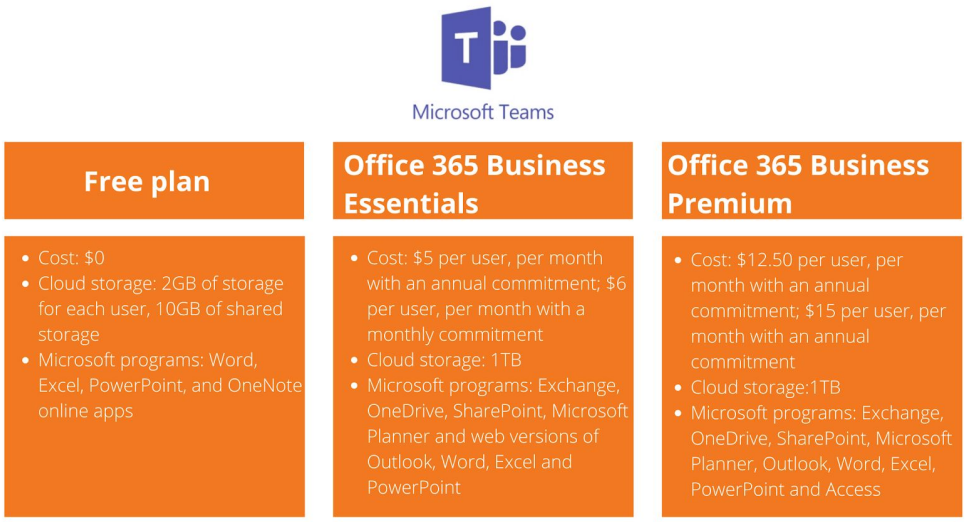

Figure 4. Microsoft Teams plans and corresponding price points. There are three different plans and out of the three, two of them require payment. The University of Washington is most likely to use the Office 365 Business Essentials or Office 365 Business Premium. Reprinted from "Comparing Zoom, Microsoft Teams and Google Meet," by Verbrugghe, C. (2020, April 10). *Europe Fourcast.*

Based on the similarity in functionalities and the fact that the UW already has Office 365 and G-Suite, the switch from Zoom to Microsoft Office or Google Meet would not be financially burdensome.

Microsoft Teams Security

According to the Microsoft Teams security and compliances document, Teams does not use user data for anything besides providing service for the clients. For instance, emails, documents or other information communicated via Teams are not scanned for advertisement purposes (MicrosoftHeidi). Microsoft Teams utilizes Advanced Threat Protection (ATP), which gives clients the option to decide if the content is malicious and inappropriate, so the users can block it (MicrosoftHeidi). ATP also gives users the power to determine what happens to the content after blockage (MicrosoftHeidi). Another safety feature is called SafeLink, which

examines URLs, and uses "time-of-click" protection to shield users from encountering harmful links once they click on it. Along the same idea, the Safe Attachments feature checks for and protects against malicious attachments. Lastly, the Data Loss Prevention (DLP) makes sure that sensitive information is not shared with the wrong people. Figures 5, and 6 provide a summary of the different Office 356 protective tools that are put in place for data privacy. Figure 7 shows the list of places where data is stored.

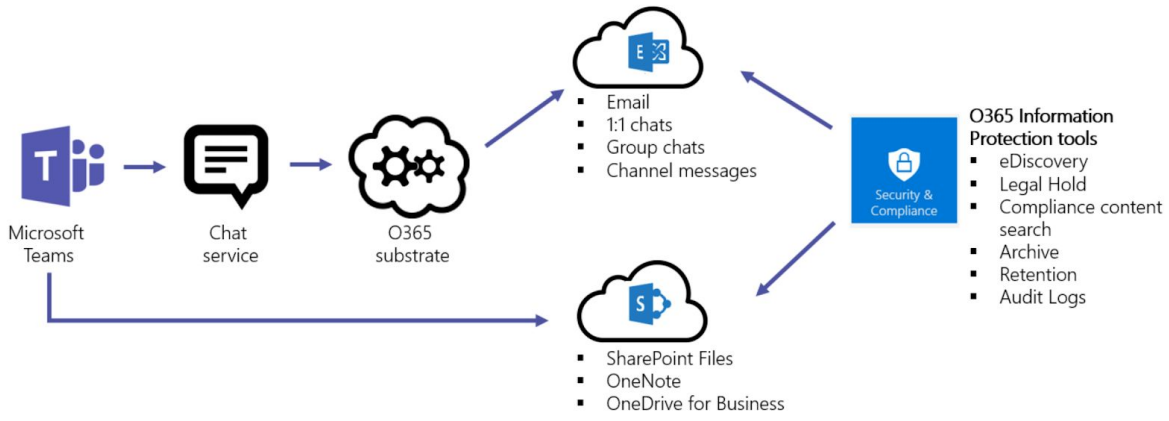

Figure 5. Displays the "Information Protection Architecture." Shows how the data from Teams travels through the different Microsoft Applications. The information is protected by the different Office 365 protection tools. Reprinted from "Overview of security and compliance," by MicrosoftHeidi. *Microsoft Teams.*

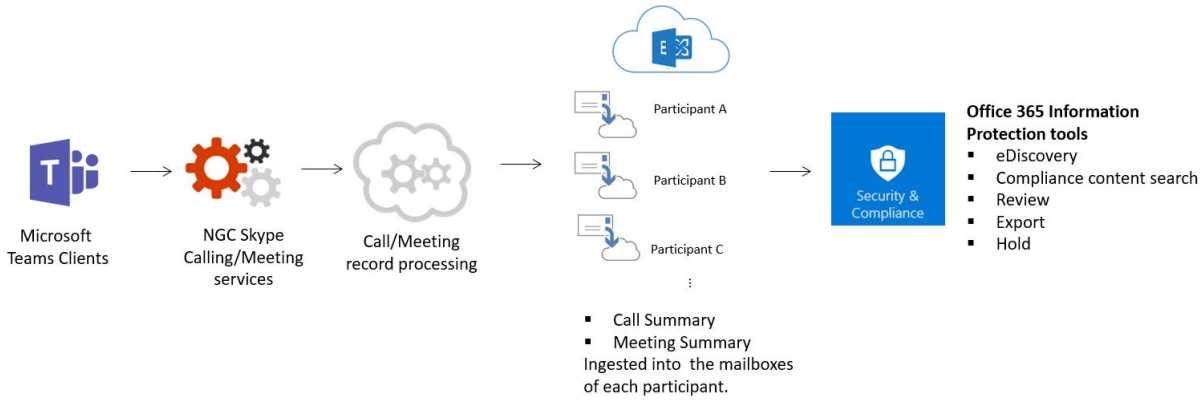

Figure 6. Displays the "Information Protection Architecture." Shows how call and meeting data is processed in different Microsoft applications. The data is secured by Office 365 protection tools. Reprinted from "Overview of security and compliance," by MicrosoftHeidi. *Microsoft Teams.*

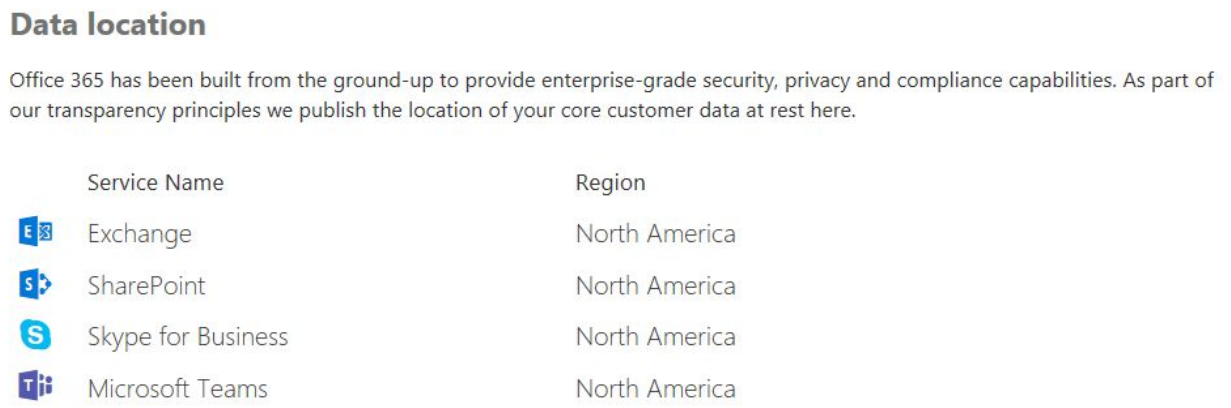

Figure 7. Displays the "Location of data in Teams." Microsoft is transparent with where the data from Microsoft Teams is stored. Reprinted from "Overview of security and compliance," by MicrosoftHeidi. *Microsoft Teams.*

Discussion

Zoom does not use the most protective encryption tools for Zoom client data privacy, but is used by millions including the students, professors, and other academic professionals at the University of Washington for online learning. The rise in numbers can be due to Zoom's ability to host up to 500 participants and easy to use features. Despite the gained popularity for its convenience, Zoom has faced criticism for not practicing safe encryption methods like end-to-end encryption like the company claimed. The University of Washington can start using Google Meet and/or Microsoft Teams because the video conferencing platforms have protective tools for data privacy. As a form of compromise, Zoom can be used for low stake activities like virtual meetings, family "gatherings," et cetera, but using it to learn online should be taken more seriously. This change will not happen overnight as instructors and students have just begun to get comfortable with Zoom, so the idea of switching to Google Meet and/or Microsoft Teams

will not be immediately favored. With the right communication about the importance of data privacy and benefits of switching to Google Meet and/or Microsoft Teams, people will be willing to adapt to other video conferencing platforms. Even though Google Meet and Microsoft Teams use more secure encryption for data privacy, there is a claim that these video conferencing platforms collect data in order to build "consumer profiles, and potentially tap into the video for purposes like training facial recognition systems" (John, 2020). A flaw that Google Meet had before was the absence of a meeting password, so anyone would enter the meeting, which can cause problems similar to Zoom-bombing (John, 2020). With online learning being the norm due to COVID-19, it is important to be mindful of data privacy and online security. With every online medium there come flaws, but despite the flaws Google Meet and Microsoft Teams have, they serve as better video conferencing platforms because other factors such as better encryption contribute to overall data security.

Acknowledgement

I want to acknowledge the different sources I have used to write this paper, and my classmates from English 182 for editing this paper. I acknowledge Professor Caitlin Postal's versatility in allowing me to explore a topic of my interest. I would also like to thank my mentor, Mickey V. Ruiz, for making edits on this paper.

References

John, A. (2020, April 30). It's Not Just Zoom. Google Meet, Microsoft Teams, and Webex Have Privacy Issues, Too. Retrieved December 04, 2020, from https://www.consumerreports.org/video-conferencing-services/videoconferencing-privacy-issues-google-microsoft-webex/

Lytvynenko, J. (2020, October 27). *Zoom Deleted Events Discussing Zoom "Censorship"*. BuzzFeed News. https://www.buzzfeednews.com/article/janelytvynenko/zoom-deleted-events-censorship.

MicrosoftHeidi. *Overview of security and compliance - Microsoft Teams*. https://www.buzzfeednews.com/article/janelytvynenko/zoom-deleted-events-censorship.

MSFTTracyP. *Safe Links - Office 365*. Safe Links - Office 365 | Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/atp-safe-links?view=o365-worldwide.

Robmazz. *Communication compliance - Microsoft 365 Compliance*. Communication compliance- Microsoft 365 Compliance | Microsoft Docs. https://docs.microsoft.com/en-us/microsoft-365/compliance/communication-compliance?view-o365-worldwide.

Secara, I.-A. (2020, August 19). *Zoombombing – the end-to-end fallacy*. Network Security. https://www.sciencedirect.com/science/article/pii/S1353485820300945

Singh, R., & Awasthi, S. (2020). *Updated Comparative Analysis on Video Conferencing Platforms-Zoom, Google Meet, Microsoft Teams, WebEx Teams and GoToMeetings*(No. 4026). EasyChair.

Update On The Hate Incident Perpetrated Against Our BSU Students This Past Sunday. Gonzaga University. (2020). https://www.gonzaga.edu/about/president-leadership/messages-media/2020/update-on-the-hate-incident-perpetrated-against-our-bsu-students-this-past-sunday.

Verbrugghe, C. (2020, April 10). *Comparing Zoom, Microsoft Teams and Google Meet*. Your Premier Google Cloud Partner in Europe Fourcast. https://www.fourcast.io/blog/comparing-zoom-microsoft-teams-and-google-meet.

Wagenseil, P. (2020). Zoom security issues: here's everything that's gone wrong (so far). *Tom's Guide*, 11