UCI University of California, Irvine

Office of Information Technology

MEMORANDUM

TO: Faculty via Academic Senate

CC: James Steintrager, Academic Senate Chair

Kian Colestock, Interim Associate Vice Chancellor and Chief Information Officer, OIT

July 30, 2020

Executive Summary

Recent revelations of gaps in Zoom's privacy and security, as well as its cooperation with the Chinese government to censor meetings and suspend user accounts, have negative implications for academic freedom and cast a shadow on its fitness for use as a distance learning platform. In light of consumer pressure, Zoom has announced a 90-day plan to implement security and privacy features that equal or exceed its competitors. However, the risks to academic freedom associated with use of Zoom or any other distance education platform cannot be completely eliminated. All major distance learning vendors will comply with foreign government requests for data. Student accessibility to platforms blocked by China's Internet border controls may result in performance and usability issues.

Situation

Recent admissions by Zoom that it censored conference calls and suspended user accounts at the request of the Chinese government as well as routed unencrypted data through mainland China and Hong Kong servers have created concerns in the academic community. The concerns include that Chinese students living and learning in China may be surveilled and put at risk if exposed to content deemed sensitive or unapproved by the Chinese government and/or that content may be censored by the Chinese government. This provokes two questions: 1) What features of distance learning services protect academic freedom and the safety of students learning outside of the U.S. and 2) Are any of them better than Zoom?

Background

The swift move to distance learning tools in the U.S. resulted in the adoption of streaming conferencing technologies that had not been intended for the purpose of teaching and learning. Their ubiquity, ease of use and relatively low cost made them appealing for educational institutions that needed a quick answer. However, privacy and security concerns have arisen as their use has proliferated.

Faculty around the U.S. have expressed concerns with distance education platforms, specifically Zoom, compromising academic freedom and potentially the safety of foreign students, particularly those currently living and learning in China. Most notable was an open letter written by Jim Millward, a Georgetown University professor of Chinese history. This was published in the wake of Zoom's recent admissions of cooperation with the Chinese government.

In response to these concerns, Zoom published a 90-day plan to address trust, safety and privacy issues. Per their update on July 1st, these increased security measures included upgraded data encryption, default security configurations and the ability to turn off data routing through China and Hong Kong (something UCI configured when it was first announced). End-to-end encryption (E2EE) is expected to be delivered before the end of July for beta testing and released for general use soon thereafter. This feature is a method of secure communication that prevents third parties from accessing data as it is transferred between two ends of the data connection. For Zoom that means the data is encrypted between the Zoom software client or web browser and the Zoom cloud server. This is similar to how other distance education platforms implement E2EE.

With these changes, Zoom will have security and privacy features comparable to other distance education platforms such as Microsoft Teams and Google Meet. However, to what extent do any of these platforms enable or preserve academic freedom?

Assessment

Preventing, or at least minimizing, the infringement of academic freedom at a technical level means that a digital education platform should address several key security features. OIT has developed a comparison of major distance education platforms that can be used for synchronous and asynchronous lectures using publicly available information. This comparison is posted on the UCI TechPrep Site under Distance Learning Tools Assessment. The use of E2EE, meeting passwords, waiting rooms, and restricting participation to attendees who have a UCInetID reduce the risk of real-time eavesdropping or censorship. However, all of these vendors have policies to turn over data upon an appropriate foreign government request - so the risk is not eliminated.

Of the platforms surveyed, only two are ready for faculty use today: Zoom and Yuja. Between the two, Zoom is a more feature-rich platform.

Recommendation

Technology vendors are in a constant race to develop and enhance features in order to capture market share. Distance learning platforms are no different. While many of them either have or are improving their security and privacy features that in turn help to enable academic freedom, they all have shortcomings. All of them will turn over data if a foreign government requests it and the request complies with their own local laws. Several of them require VPN access to use, limiting the actual usability of the service. Zoom’s ubiquity and shortcomings have forced it to be more transparent with its privacy and security, and it will very soon add end-to-end encryption. While Zoom remains an imperfect distance learning tool, it is also the most practical and accessible for students living in China. As an alternative for synchronous lectures with smaller classes (< 200 participants), Yuja Video Conferencing is also available upon request.