SFU FACULTY OF COMMUNICATION, ART AND TECHNOLOGY | SCHOOL OF COMMUNICATION

TEL +1 778 782 3687
FAX +1 778 782 4024
sfu.ca/communication

Simon Fraser University
Shrum Science Centre K9671
8888 University Drive
Burnaby BC
Canada V5A 1S6

April 21, 2020

Mark Roman
SFU Chief Information Officer

Dear Mark Roman, IT steering committees, and SFU community,

We, the faculty at the School of Communication, are writing to express a number of concerns regarding the popular online platform Zoom. We are aware that SFU has already licensed a pilot - an understandable move, given the urgency of bringing large groups online together in the current situation. However, **we urge the SFU administration to carefully consider any lasting investment in Zoom**, given its questionable business practices and its poor record in cybersecurity and privacy protections that we outline below.

As a large client, we need to be mindful of ethical and economic issues implicit in the technology platforms we choose. As a university, we need to be even more careful in our choice of technologies as our adoptions constitute tacit endorsements. School districts around the world, including New York and Singapore, are already beginning to ban Zoom over these concerns (as outlined below). SFU is not forced to turn to Zoom to deliver remote education. Services like jitsi provide a free, open-source alternative that is easy to use and is built from the ground up to better support privacy, while SFU already has a reliable alternative in Bluejeans for smaller meetings. While the present situation does require urgent responses, we believe that part of SFU's responsibility during times of crisis is also to consider the wider implications that decisions made now will have for years to come.

Zoom does not offer a secure platform. Zoom's cybersecurity flaws are well documented. For example, for Mac users, Zoom gives itself the power to turn on your webcam and put you into a call without your permission. (Apple has now issued a system update to prohibit this 'function'.) Similarly, a former NSA hacker revealed that Zoom can be used to take over your Mac – including your webcam and microphone.

Further, Zoom frequently overstates its performance in this regard. For instance, Zoom often promises 'end to end encryption', but independent reporting by the University of Toronto's Citizen Lab shows that this is *not* the case.

In times of pandemic, these vulnerabilities are now manifesting in a new genre of hate speech aimed at students and educators. "Zoom bombing" is rife: the FBI reports two cases where Zoom classes were gatecrashed by trolls, who screamed out a teacher's home address and showed off swastika tattoos. While passwords and other steps can help reduce the threat, Zoom's popularity and poor security means that it remains especially vulnerable to new forms of hacking and trolling.

Zoom does not protect the privacy of our students and instructors. Most notoriously, Zoom's attention tracking feature lets the host/admin know if the user has clicked away to a different window. If students chat privately to each other in a Zoom call for example, the teacher can also access those records without their knowledge.

In Zoom's privacy policy, its answer to "Do you sell our data?" is a casual "Depends on what you mean by sell". The more accurate answer is "Yes, extensively": Zoom extracts user data even if they do not have an active Zoom account, as long as they participate in a call. Zoom also sells users' data to Facebook – even if they have never had a Facebook account.

Zoom has now moved to correct some of these issues, but these represent hasty quick fixes on the heels of resounding global criticism. *The New York Times* reports that Zoom has "never felt the need until now to rigorously examine the platform's privacy and security implications for consumers." Eric S. Yuan, Zoom CEO, says: "the risks, the misuse, we never thought about that." That is not good enough for our students and instructors.

Experts worldwide are advising against Zoom adoption. In addition to school districts dropping the service, Zoom is currently being investigated by the New York Attorney General, and the Electronic Frontier Foundation warns us about using it. There is now a class action lawsuit in California for Zoom's invasive data extraction practices.

Zoom's actions conform exactly to what communication scholarship has called *infrastructural imperialism* (e.g. Siva Vaidhyanathan, University of Virginia) or *platform imperialism* (e.g. Dal Yong Jin, SFU): a recurring pattern when technology companies knowingly violate laws and social norms around privacy and other ethical issues as a quick path to dominance, and then belatedly walk back only the most controversial practices to maintain a veneer of ethical behaviour. We have no reason to believe that Zoom will be a leader in either cybersecurity or privacy issues. More importantly, the SFU community should be wary about financially supporting this type of corporate model beyond our current short-term adoption.

With this letter, **we urge SFU to explore every alternative to Zoom for larger-scale video conferencing,** especially open-source options. **We further urge SFU to ensure that any long-term arrangement is vetted** to consider the platform's 1) privacy and security features; 2) use of surveillance models and backdoor data collection; 3) funding model and reliance on exploitative corporate practices.

Collectively signed by the faculty at the School of Communication

21 April, 2020