Association for Asian Studies Statement Regarding Remote Teaching, Online Scholarship, Safety, and Academic Freedom

AAS Board of Directors

July 23, 2020

Executive Summary

Videoconferencing tools such as Zoom present universities with stark technological, pedagogical, and moral considerations, especially with regard to the security of student and faculty data. These issues arise from the censorship and data-monitoring and informing requirements imposed by various foreign jurisdictions, in particular China, and are especially pressing due to the present COVID-19 pandemic, when many students must participate in online courses while located abroad. The expansive laws in China accommodate state censorship and compel online platforms to police and report inappropriate or illegal actions. Such regulations undermine academic freedom and place students and faculty in possible legal jeopardy, not just for the present moment, but for years into the future, making the scrupulous disposition of online material all the more imperative. Faculty and university administration should be cognizant of these challenges when planning and teaching their courses and when considering the acquisition and operation of education-related software systems. Faculty are urged to take seriously potentially conflicting issues of equity, accessibility, and vulnerability when interacting with students online. University administrators are enjoined to educate themselves regarding the legal and political challenges that contemporary regimes pose to free intellectual exchange via online teaching and conferencing and to provide guidance to faculty and students about possible risks. Other recommendations address the collection and aggregation of data, the vetting of vendor data handling and privacy policies, and the importance of consultation with faculty and students regarding the adoption and operation of teaching and conferencing platforms, among other matters.

Full Statement

The global coronavirus pandemic has made videoconferencing tools such as Zoom essential for teaching and other forms of academic communication. Many scholars have discovered that the advantages of videoconferencing transcend their emergency use, and it is likely that even after the threat of COVID-19 is mitigated enough to resume regular in-person interactions, scholars, students, and universities will use online meetings more and for more varied activities than in the past. In-person academic exchange, like print-and-paper publishing, now has a major online complement, and just as we increasingly transmit information and access books and journals digitally, we will conduct more lectures and seminars online.

However, a series of incidents involving Zoom and the People's Republic of China has raised concerns about the potential for China or other governments to compromise the privacy, reliability, accessibility, and security of videoconferencing apps, and to use data gleaned through these apps for state purposes. For example, data originating in the United States during some Zoom sessions was directed through some of the company's China-based servers, making participants potentially subject to state surveillance and/or legal action.[1] Although Zoom has addressed some of the concerns, it seems that for the foreseeable future, Zoom and other online meeting providers will have limited ability to prevent state intrusion by the governments in the countries where they do business. Meanwhile, universities will have to keep using such apps if they wish to use videoconferencing to teach and communicate with students and colleagues in those countries through videoconferencing. In fact, the same concerns apply to all online communication tools, including digital publishing, courseware, and the transmission of course- and research-related documents. Furthermore, the recent passage of Hong Kong's National Security Law, and especially its Article 38, means that the vulnerability of online communications poses a direct threat to the safety of anyone, regardless of where they reside, who teaches or studies topics deemed off-limits by the Chinese Communist Party or Hong Kong government.

The following guidelines are meant as a set of considerations for faculty (particularly in Asian Studies but applicable to all fields) and university administration as they navigate the contradictory demands now imposed upon us by our increased reliance on online academic exchange and the new threats this poses to academic freedom and safety.

---

[1] Chinese laws pose potential civil and criminal liability for a wide range of online content including, but not limited to, a range of political commentary, sexual content, violent content, or coarse language. China's 2019 Provisions on the Governance of the Online Information Content System make illegal the distribution of a wide range of content that is available in US universities. Students seeking to access content, professors sharing content online, and universities that host content could all be found civilly or criminally liable for this activity. This issue exists independent of platform choice.

1. General Considerations

Academic freedom is the central principle governing pedagogy and research in the university ecosystem. It embodies the same valorization of truth-seeking that underlies peer-review and committee-based admissions, hiring, promotion, and granting of research funding, affirming that the betterment of human knowledge requires open intellectual exchange and evaluation of ideas. Yet if extraneous forces have the power to distort the scholarly interpretation of factual evidence or restrain its expression, our research and pedagogy are tainted as well.

Threats to the safety and livelihood of students and scholars, or to their families, that arise from their academic or scholarly activities comprise an acute violation of academic freedom. In today's globalized academic ecosystem, academic freedom is not something that applies solely to people within the physical boundaries of a given education institution. Rather, it is a protection that a university has the obligation to extend over its academic activities wherever they occur, whether on its domestic home campus, on a foreign branch campus, in the pages of a journal, or online. The issue of security and reliability of videoconferencing and other course software, therefore, is not a matter simply for university administrators or IT technical staff to address: it affects the very heart of academic endeavor and should concern every member of the university.

2. Considerations for Faculty

When teaching or interacting with colleagues and students in online situations, faculty should consider the vulnerabilities and dangers to which each participant may be exposed as a result of their place of residence, nationality, or the topic under discussion. Furthermore, the responsibility of scholars (and institutional review boards) to protect sources and collaborators when conducting fieldwork should govern our daily classroom teaching.

An instructor teaching remotely must simultaneously consider issues of equity, accessibility, and vulnerability, which can pose contradictory imperatives:

- Physical safety of students in remote locations
- Accessibility of class sessions and course materials to students in remote locations
- The instructor's own safety and on-going access to the country of their academic interest
- Avoiding censorship[2]

---

[2] Given that academics compromise their writing or speech due to a threat or perception of a threat in combination with a lack of faith in universities and other institutions to protect them, it is not really "self" censorship at all, but simply censorship. A hostage with a gun to his head is never accused of "self-censorship" when he tailors his video remarks to desires of his captors.

- Communicating with university administrators and objecting to top-down policies that hamper an instructor's ability to respond dynamically to conflicting imperatives
- Criminal and civil liability for students, faculty, and staff

While some of these are concerns in online teaching generally, the mass reliance on videoconferencing and learning systems software during a global pandemic in an era of rising authoritarianism creates particular challenges. For example, will a software vendor live up to promises to encrypt videoconferencing? Will the vendor provide student data to foreign governments, as it may be required to do by law in various jurisdictions? Will the vendor or a foreign government block students abroad from participating in online classes? Does a student abroad have safe and adequate internet access to the class and class materials? Is there a reliable and safe way to transmit course files, including writing that may be controversial or recordings of lectures or discussion classes which may contain viewpoints to which a state will object, as well as the identity and speech of individual students? Will students, faculty, or universities be held criminally or civilly liable for content they distribute/consume in other countries?

Only the instructor, in consultation with students, can make these assessments, since they require knowledge both of the country and of the student's individual situation. However, it is incumbent upon universities to offer guidance. While we are writing this statement as scholars of Asian Studies, the issues we raise affect faculty in a wide range of disciplines who discuss controversial topics. Furthermore, individual faculty cannot be expected to have a full understanding of all the unique internet regulations of the different jurisdictions where their online students may be located. As a result, caution, individual attention, flexibility and redundancy of systems may be the best approaches to reconciling the need for online interactions and the potential perils they pose. Below are some suggestions regarding main points of vulnerability.

- Be extremely cautious about recording, storing, and transmitting recordings of discussion classes, especially where student identity and students' opinions are evident. While videoconferencing software promises end-to-end encryption, that becomes irrelevant when the class is reduced to a file transmitted over the internet or stored. Such files can be duplicated and could potentially pose a risk to class participants years after the class has finished.
- Instructors may be asked or feel a need to censor course content in order to protect students abroad. When restrictions on course content are absolutely necessary for reasons of safety, the restrictions should not affect students who are not in jeopardy. Where possible, missing content should be provided to international students at a later date when it is safe to do so. Finding ways to provide uncompromised course content to

remote students safely should be an urgent goal in development of technology and teaching systems.[3]

- To help with safety, accessibility, time-zone issues, and so on, instructors should consider individual or small group tutorials for students who are located abroad.
- Instructors should think creatively to alleviate these new threats to academic freedom that result from online teaching on a global scale. What features of the online teaching environment might allow one to circumvent governmental attempts at surveillance or intrusion? Some may wish to employ alternative or multiple video-conference systems; run an audio link in parallel to a Zoom-style conference; make an audio recording to send later (a much smaller file than video, with participants anonymized); encourage students to participate in controversial classes from accounts and under aliases which do not reveal their identity, and with video off or obscured. Creative approaches, as well as technical solutions, are needed.
- Faculty, particularly those with tenure, should provide frequent feedback to IT officers and university administration about what works and what doesn't. Where safety and academic freedom are at stake, more than ever the needs of pedagogy should shape the technology, not vice-versa.
- Universities, in conjunction with the American Association of University Professors or other related organizations, should provide faculty with a policy overview of internet regulations in countries that could pose a potential risk in order to help faculty protect themselves and their students.

3. Considerations for University Administrators

In the past, university decisions on the adoption and use of course software have generally been made with little faculty consultation, let alone consideration of implications for international students. Notably, the initial adoption of Zoom by nearly the entire academy occurred before Zoom had even a minimally adequate domestic privacy policy in place (it was still harvesting student data for commercial purposes) and with no forethought about how Zoom would interact with governments abroad. Such top-down decision-making regarding online pedagogical systems cannot continue unreflectively in the age of COVID-19 and Hong Kong NSL Article 38. For example, in ignorance of possible threats to the safety of students in and from China, at least one

---

[3] By contrast, actively working with foreign partners to assist in censorship, as Cambridge University Press did, or as some UK universities are now apparently doing to filter course content for delivery to China, is deplorable. The system employed by King's College London, Queen Mary University of London, York and Southampton allows an Alibaba affiliate to manage a "security allow list" that can approve or block Chinese students' access to course materials assigned by these British campuses.

U.S. university decreed that “all classes” would be recorded and stored by the university in Fall 2020 for the purposes of “asynchronous instruction,” without implementing procedures for protecting the privacy of student participants in the class meeting or considering whether students in China could safely stream or download such recordings in non-encrypted form.

Administrators now must strive to follow new principles for guaranteeing academic freedom above the transactional matters of contracting with software companies and accommodating authorities in autocratic counties.

- Universities should recognize that the defense of academic freedom is a university responsibility, not something to be borne alone by individual faculty or students, who are relatively powerless in such situations. Moreover, universities should acknowledge that the principle of academic freedom extends wherever in the world the university community operates, and requirements to “comply with local laws,” when those laws violate academic freedom, should be met with more than a shrug and meek acquiescence. Software companies should ask governments, and universities demand that software companies stipulate specifically, which statues are being complied with. We urge universities to work together, creating collective bodies that can remonstrate with clout against state actors who impinge on academic freedom and threaten scholars. Universities need to provide robust advocacy, employing all possible legal, diplomatic and financial resources to defend their students and faculty when they are threatened, and, again, do so collectively when necessary to increase impact.
- University administration should actively solicit the input of knowledgeable faculty in courseware choices and, most important, leave critical decisions about online pedagogy to the instructor, in consultation with their students. Universities should recognize that some of the best ways of alleviating problems associated with remote instruction rely on interpersonal rather than technological interventions and recognize that faculty are devoting extra time to provide individual attention to remote students.
- A fundamental principle guiding university adoption of technological solutions is the minimizing of data collection of all kinds. Every technology contract should be explicitly negotiated with this end in mind. It is not ethical to allow corporations to use students for data-harvesting for marketing or for the development of their own businesses, e.g. predictive analytics. Such data-harvesting is actively dangerous to students and faculty in the context of widespread corporate cooperation with authoritarian governments.
- A second fundamental principle is to guard against technology policies that aggregate or centralize data, especially when they are creating linked databases. Going beyond HIPAA guidelines, in an age of insecure information, universities should try as far as possible to develop decentralized and identity-preserving data systems in which the breach of one system does not have a cascading effect on others.

- Universities should negotiate strong contracts with software companies that 1) respect the privacy of students and faculty and minimize data collection, particularly with identifying features; 2) safeguard intellectual property created, stored, recorded, or conveyed on or via technology platforms, including from commercial exploitation by the vendor or third parties; 3) specify the vendor's policies with regard to potential state interference; and 4) address similar matters. The university should make clear up front that actions such as dropping students from classes, providing their data to third parties, eavesdropping or allowing eavesdropping on classes, and similar behavior comprise a violation of academic freedom and a violation of contract and are incompatible with the academic mission the vendor's software hopes to serve. Contracts should stipulate financial and legal remedies should vendors threaten academic freedom and endanger scholars in this manner. The terms of contracts in regard to these matters should be public and widely shared among universities as best practices.

- Where possible, universities should provide multiple and redundant software systems to accommodate diverse faculty needs and, most importantly, to avoid two potential dangers: 1) the all-our-eggs-in-one-basket situation, in which a university becomes entirely dependent on a particular company's products and thus has no recourse if its chosen software vendor decides it is not in their commercial interest to uphold measures protecting academic freedom; and 2) the one-stop-shopping situation which facilitates outside interference: If the university's entire course catalog or conferencing is on one software platform, it is easier for malign actors to hack it or convince companies to open a back-door or turn over data.

- Universities should also carefully consider their legal liability for sharing content in different jurisdictions and clearly outline what, if any, support they will offer faculty and students who may face legal liability in other jurisdictions so that individuals can carefully calculate their personal risk as they engage in teaching and learning.

- Explicit consent must be sought from faculty and students about use of data generated through any technology platforms they are required to use in university settings. For example, if student data on platforms like Canvas are being used to monitor attendance and participation by deans, this requires prior consent from the student in question to allow the use of data for this purpose. Similarly, use of platform-generated data to evaluate faculty performance requires explicit and prior consent. If the university is considering adopting features on technology platforms that depend on data-mining such as predictive analytics, this should be discussed and approved by both the faculty and the student body. In general, such technologies, which violate the fundamental principle of minimizing data collection, should be avoided.