The view from "Zoom University": surveillance and control in higher ed's pandemic pedagogy pivot

Article (Published Version)


This version is available from Sussex Research Online: http://sro.sussex.ac.uk/id/eprint/107011/

This document is made available in accordance with publisher policies and may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher’s version. Please see the URL above for details on accessing the published version.

Copyright and reuse:
Sussex Research Online is a digital repository of the research output of the University.

Copyright and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable, the material made available in SRO has been checked for eligibility before being made available.

Copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational, or not-for-profit purposes without prior permission or charge, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.
Symptoms of the COVID-19 pandemic include a dry cough, a high fever, and an unprecedented influx in the use of networked technology. Illustrating the latter trend is the increased use of the popular videoconferencing platform Zoom, which grew from 10 million meeting participants in December 2019 to over 200 million in March 2020 when nearly every educational institution in the United States shifted to remote learning (Yuan). This nationwide move reflected a surprising and sudden consensus across spheres of commerce, governance, and public services. Through Zoom or other videoconferencing platforms, communities attempted to repair the normalcy lost in the absence of in-person interactions with computational solutions. Campus-based higher education shifted in-person class discussions, lectures, and even labs online; faculty who had never before taught online were suddenly forced to do so; and teaching and learning centers ramped up technical and pedagogical support to accommodate the shift—all within a two-week span.

Students pushed back. Some checked out and simply didn’t attend class online. Others logged in but engaged minimally, turning off their cameras or otherwise resisting participation in class. On a larger scale, student lawsuits demanded tuition refunds because the ubiquitous “Zoom University” abraded their university experiences. Online education was all the same, they argued: “had I chosen Millersville [a much less expensive and selective school] over Gettysburg, I would now be receiving the same quality of education, since they have moved online as well,” a Gettysburg College student wrote (Blackwell). “Sitting in my own home, and not in a gorgeous classroom paid for by rich donors and students’ tuition -- that’s not what I was promised,” said a University of Chicago student (quoted in Anderson). “If I wanted to go to an online school, I could go to an online school. I paid to go to class and sit in a lecture,” said a University of California-Irvine student (quoted in Anderson). Student satisfaction in their education dipped significantly (Digital Promise).

The sudden shift to online education, coupled with the economic, health, and social stress of the pandemic itself, pitted frustrated students against overworked faculty and mid-level administrators who were mostly uncompensated for this labor in shifting education online.

The students checking out, turning off, or filing lawsuits against their universities resisted the apparent deflation of their educational experiences (Hubler). But we see them as also resisting a more general technologizing trend in their education. Students recognized instruction delivered through networked technology as separate from and inferior to, yet also more sinister than, face-to-face instruction. Bubbling to the surface, this resistance reveals just how far universities have pushed through the implementation of “content management systems” (CMSs) and video software platforms that nakedly evoke Jeremy Bentham’s panopticon. The adoption of popular CMSs such as Blackboard, Canvas, Microsoft Office Suite, Top Hat, Zoom, Panopto, and other ed-tech platforms
has been homogenizing universities for years. Although we could have just as easily named a “Blackboard University” in the 2000s, in this article we use “Zoom University” as a term to identify a cultural crescendo regarding higher ed’s decision to funnel its instruction, along with student and faculty data, through corporate platforms, and we refer to this technological shift generally as the “pandemic pivot.” The slow boil of the corporate-tech trend facilitating student experiences erupted in spring 2020: students let us know that they don’t want to be projected through networks, subjected to digitalization, datafication, surveillance by cameras, computational systems, and the authorities that drive them. We acknowledge the necessity of networked ed-tech during this critical moment and more broadly for diverse accessibility concerns. Given the need for this technology now and moving forward, here we focus on a critique of systems of control that it perpetuates, reading resistance in student pushbacks and those of other surveilled university populations.

Figure 1: Tweet by “Evelyn,” “Lol you thought you were better than me cause you went to Harvard??? We’re all attending Zoom University now.” 13 Mar 2020. https://twitter.com/just_a_dreamer5/status/1238616862189068289?lang=en

We argue that the widespread adoption of Zoom in higher education during the COVID-19 pandemic did not simply perpetuate but instead exacerbated the issues of surveillance and control inherent to the use of educational technology. We begin by tracing the rise of ed-tech, establishing Zoom as both the logical extension of prior technologies and an unprecedented phenomenon. Considering Shoshana Zuboff’s theories of counter-declaration and synthetic declaration, we then outline a framework for resisting (in lieu of “opting out” from) corporate ed-tech platforms and apply it specifically to Zoom. Through the lens of James Brown, Jr.’s writing on hospitality, we discuss surveilling actors that threaten user and institutional privacy. We then identify some populations that are disproportionately affected by this infrastructure of surveillance and control. We conclude by extending a survey of “counter-declarations” that were, are, and could be enacted by
administrators, instructors, and students as methods of resisting the dehumanizing experiences of Zoom University.

**Ed-Tech has always been watching us**

It is tempting to claim that higher ed’s adoption of Zoom marks a predictable advancement in the progression of ed-tech. After all, surveillance has always already been present in these technologies. Shoshana Zuboff warns scholars of history and technology against falling victim to this type of fallacious rationalization: “When we encounter something unprecedented, we automatically interpret it through the lens of familiar categories, thereby rendering invisible precisely that which is unprecedented” (12). It is necessary to call “new” that which is unprecedented to lay bare its exigency, mechanics, and implications. Pandemics are not unprecedented. And surveillance technology has long reified the unidirectional and uneven power distributions within educational hierarchies. In necessitating the networked technology, however, the pandemic operates as a kairotic crisis. Because it was sudden and widespread, the pandemic enabled an unprecedented development in educational surveillance technology.

Surveillance has long been a central and pernicious component of ed-tech. The objective of surveillance is control, as even a cursory read of Foucault would tell us, and for ed tech, surveillance is used to access and control students’ thought processes. The eraser debate among 19th century educators, for instance, was essentially one about surveillance: if students could erase their work, then the teacher wouldn’t have access to evidence of student thought processes (Baron). These conversations about the need to surveil students were then repeated with the advent of spellcheck. Similarly, in the 1950s, B.F. Skinner used his operant conditioning work with pigeons to design technology that would positively shape student behavior. Termed “teaching machines,” this technology would control every moment of the learning process (Watters, “Education Technology”). When technology mediates thought, the actors who control technology—in this case educators—assume a position of power.

Since the early days of computing, ed-tech has become the white noise of the contemporary university. Martin Weller charts the dominant course through computer-mediated communication (CMC), blogs, and open education resources until arriving at what he terms the “dystopian turn.” He cautions educators to be skeptical of technologies such as AI, learning analytics, and massive open online courses (MOOC) because of the issues they incite “relating to privacy, ethics, surveillance, and de-professionalization” (Weller 177). These issues, however, have already been upon us.

Echoing Weller and other educators concerned with the increasing dominance of ed-tech, Audrey Watters argues that we are in a dystopian moment with education, escalated if not incited by the pandemic. Surveillance tech brought us to the precipice, to this “moment where everything is falling apart and the solution [. . . ] is software that sounds like ‘panopticon,’” such as the video program Panopto (Watters, “All Watched Over”). Ed-tech’s panoptic pivot pits students against instructors and institutions in what Elizabeth Losh calls a “war on learning” (8) that uses weapons such as plagiarism monitoring, test proctoring, and other surveillance technologies to control student behavior, and, ostensibly, their learning—but as Losh points out, these technologies were deployed well before spring 2020 (“Introduction”). However, when the pandemic hit, dorms, cafeterias, classrooms, and physical presence were barred, and ed-tech became the university itself. As the technologies we relied on suddenly moved from background noise to foreground siren, the ways that these technologies frame, present, and interpellate users became more acutely apparent. As the entire university experience was funneled through ed-tech, Zoom in particular emphasized and intensified the unidirectional power dynamics that are shot through ed-tech’s history.
Initial problems related to overzealous surveillance, poor implementation, and network security that occurred with the turn to Zoom in March 2020 can be traced to the corporate contexts from which it, and many other education technologies, were developed. On April 1, 2020, Zoom founder and CEO Eric Yuan acknowledged these challenges and their origin:

First, some background: our platform was built primarily for enterprise customers – large institutions with full IT support. These range from the world’s largest financial services companies to leading telecommunications providers, government agencies, universities, healthcare organizations, and telemedicine practices. Thousands of enterprises around the world have done exhaustive security reviews of our user, network, and data center layers and confidently selected Zoom for complete deployment.

However, we did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home. We now have a much broader set of users who are utilizing our product in a myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived. (Yuan)

To respond to this new context, Zoom removed an “attendee attention tracker feature,” which alerted hosts when meeting participants switched away from the Zoom screen for too long, and which educators balked at (although test-proctoring software such as Proctortrack uses similar features). They also added privacy features and released videos meant to substitute for the IT support the software platform could no longer assume (Yuan).

These specific challenges to this piece of corporate software were unprecedented; however, the top-down power dynamics associated with ed-tech have long been scaffolded by higher ed’s ongoing corporatization. Our courses are run through CMSs for which our universities pay a hefty sum; students flow through registration systems like PeopleSoft; we organize departments on Microsoft Teams, Box, and local email servers; our students compose through Microsoft Word, Adobe Creative Suite, and within the notepads of their smartphones. Teaching support centers have collapsed into IT centers. Academic reliance on corporate technology has been reflected by an explosion in the market. In 2019, investment in ed-tech companies experienced a 16% increase from the previous year, “[reaching] at least $1.66 billion across 105 deals” in the United States (Wan and Wade). Already infrastructural, this ed-tech network was rendered indispensable by the onset of the pandemic.

**Opting out is no longer an option**

As the university itself became ed-tech, and as most synchronous contact was filtered through Zoom in particular, faculty and students and administration were compelled to participate in the platform. The already illusive model of “opting in” or “opting out” of a platform simply disappeared. Within higher ed, the urgency of remote instruction translated into university mandates or strong encouragement for platforms for remote instruction. Many of these platforms were already in use and had been critiqued for the ways they surveilled students and instructors or swept them up into corporate models of education. We can view the compulsory funneling of instruction through digital platforms via Shoshanna Zuboff’s description of “surveillance capitalism” and her models that address the problem of opting out.

The adoption of corporate tech positions surveillance as the default state and privacy as a commodified feature. “Surveillance capitalism,” explains Zuboff, describing what she identifies as an unprecedented phenomenon, “unilaterally claims human experience as free raw material for translation into behavioral data” (8). In its forced funneling of communications through digital
networks, the pandemic translated specific human experiences into resources for the telecommunications industry.

Zoom operates in accordance with this definition of “surveillance capitalism” both by profiting from user data in the traditional sense and by capitalizing on the institution-cum-user’s initiative to both protect and surveil its subjects. Zoom is relatively transparent regarding its privacy policy: it collects material ranging from email, username, and password, etc. for free accounts as well as billing name, address, phone number, payment method, company name, etc. for paid subscriptions. It then shares this data with partners, for corporate transactions, for business reasons, and for legal reasons (through just about any outlet that will generate profit and excuse liability), essentially participating in the data brokering market developed by actors such as Google, Apple, Facebook, and so on (Zoom, “Zoom Privacy Statement”). Moreover, as a videoconferencing platform, it profits from surveillance in that it markets a tool for employers to monitor their workers (e.g., administrators monitor faculty/staff, who in turn oversee students), charging premiums for the ability to surveil more people for longer, and, ultimately, to maintain a record of these transactions through cloud recordings. These features can be a convenience for both users and administrators; their functionality shapes users and compels them to add to Zoom’s data stores. Zoom is produced by, adheres to, and perpetuates a culture of surveillance capitalism.

Zuboff articulates two forms of challenging surveillance capitalism: “counter-declaration” and “synthetic declaration.” Counter-declaration relies on the individual user’s knowledge about abstract privacy principles (e.g., “data ownership”) and their ability to apply cyber security practices (e.g., encryption). Counter-declaration, and opting out more broadly, is a responsibility of the user rather than system administrators. Synthetic declaration involves the mass application of an alternative framework. She describes the interplay between the two strategies: “[w]e bide our time with counter-declarations and make life more tolerable, but only a synthetic alternative vision will transform raw surveillance capitalism in favor of a digital future that we can call home” (344).

Counter-declaration merely becomes a form of harm reduction. And it is often limited by the fact that users are coerced into opting in to get basic functionality of software (e.g., clicking on end user license agreements, or EULAs) and then must navigate technologically challenging methods of partially opting out. Counter-declaration of education technologies in the pandemic teaching situation entails operating privacy settings and tools offered within the systems that are required for them to do their jobs and manage their lives. Counter-declaration strategies of strong encryption and data ownership are important, especially now, but they miss the big picture according to Zuboff and Renata Ávila in a recent broadcast conversation aptly titled “COVID-1984.” Synthetic declaration—a much greater lift involving collaboration with institutions—would mean more widespread adoption of flexible education technologies designed with learning at the core, rather than business models that prioritize data collection and communication.

Zoom’s implementation of end-to-end encryption (E2EE), a privacy measure that prevents outside parties from accessing communications, is illustrative of the fluctuating process of privacy-seeking. Zoom initially restricted enhanced privacy protections such as E2EE to users with paid subscriptions, ostensibly to cooperate with government authorities, but implicitly correlating privacy with economic status. Yuan commented, “‘Free users—for sure we don’t want to give [them] that, because we also want to work together with the FBI, with local law enforcement, in case some people use Zoom for a bad purpose’” (quoted in Hunter). To use Zoom, free users were only required to input a pseudonym and email address, rendering them practically anonymous but not technically secure, as law enforcement could still track messages. Bowing to pressure from organizations like the Electronic Frontier Foundation (EFF) (Hunter), Zoom enabled E2EE for all users
in June 2020; however, the feature is optional and not turned on by default. Users have the option to gain an additional layer of privacy, but to do so, they must have the technical knowledge to enable the option and input a phone number, sacrificing a degree of anonymity. Put into Zuboff’s framework, they must counter-declare.

Zoom’s investment in privacy as a premium feature reveals that privacy has always been a good with restricted access. The ability to control networked technologies is more available to those who either have the knowledge to implement security measures or the finances to afford premium features. As digital spaces are vulnerable to privacy threats, counter-declarations become conscious, rhetorical acts.

Hospitality and vulnerability in ed-tech networks

The radical hospitality of networks that James Brown, Jr. identifies, with its attendant global and local vulnerabilities, is activated in our physical classrooms but it has been accentuated in our pandemic teaching contexts. Networked systems are susceptible to external disruption, and the phenomenon of “Zoombombing,” the disruptive intrusion of uninvited meeting attendees, exposed this vulnerability. Drawing on Derrida’s Law of Hospitality and Wendy Hui Kyong Chun’s concept of machinic “dialogue” online, Brown points out that when we move into online spaces, the properties of information and network protocols mean that we open ourselves up to guests, both wanted and unwanted. Though he was writing years earlier, Brown seems to capture the network security issues of the pandemic pivot in March 2020:

Networked life forces us to interact with others, even when we haven’t extended an invitation and even when we haven’t been invited. Life in a network society – one in which information and bodies constantly move and collide – means never getting to be alone and never getting to be offline. It means never getting to decide in any thoroughgoing way who or what enters your “home.” [. . . ] This situation is one defined by hospitality, but not a hospitality that involves a clearly defined host or guest. [. . . ] The other arrives, over and beyond our choices to filter or turn away. (1)

The challenges of hospitality in open networks are not specific to digital contexts, Brown points out through a dramatic example of a suicide bomber in a public square (20-21). Not incidentally, some of the public health challenges of the pandemic—specifically, how to regulate our interactions with each other in shared physical spaces—are also fraught with hospitality challenges. Safely sharing screens is perhaps not much different than safely wearing masks in mixed groups.

Beyond overt security breaches, the hospitality of Zoom University is threatened by sanctioned actors. Our class videostreams do not travel directly from our houses to others but pass instead through cables and servers and are subject to a tangle of global and local jurisdictions. Compelled to work from home, students and instructors are subjected to additional elements of surveillance within our own networks. Because the network’s built-in hospitality opens it up in all those contexts, there may be new forms of radical ruptures of classroom privacy moving forward through this pandemic teaching moment. These ruptures act as unique forms of control or surveillance, ones that are not inherently institutional or corporate but enabled through the technology employed by these systems. We might have seen these ruptures coming if we had paid closer attention to the properties of hospitality in open networks that Brown describes.

Issues with network security and unwanted guests or antisocial behaviors in the use of Zoom for classes highlights some of the vulnerability problems in higher ed’s embrace of corporate technologies. Although Zoom’s ability to drop users into a meeting through the click of a link was appealing for education and a key ease-of-use feature for students and faculty during the pandemic
pivot, this accessibility forced questions of user privacy and security. Protections like passwords, waiting rooms, and blocking screen sharing were already available features in Zoom. But assuming a business context with a professional IT staff and paid employees with a stake in a company, Zoom initially turned off most privacy settings by default and provided few security prescriptions regarding their use (Pierce). In doing so, Zoom shifted the responsibility of securing the network against outside surveillance and disruption—of counter-declaring—to the user or administrator.

These defaults resulted in a rash of Zoombombings, where students or outside trolls would enter a lecture and share offensive images on their screens. Inside Higher Education describes a class’s first online meeting, which “was disrupted by a participant sharing a pornographic video, participants choosing offensive display names, and a chat filled with racist and vulgar comments” (Redden). The professor lamented that he had to end the class and then subsequently figured out “tech fixes that would allow [him] to maintain tight control over what happens in a Zoom classroom” (Redden). In retrospect, considering the shift from local to global networks, perhaps it should have been obvious that our classroom networks were vulnerable to trolls and shenanigans. Anyone who has spent significant time in online communities is aware that trolling by pornographic image-sharing or violations of language decency are hazards of open fora. Whitney Phillips observes that these acts of trolling reflect problematic aspects of culture generally; they are “agents of cultural digestion” (135).

It is not by accident that Zoombombings often rely on the same racist and sexist tropes Phillips observes in earlier networks such as 4Chan. Trolls reflect existing orders of dominance by exploiting the technological platforms and networks available. Trolling is an art of disruption, for which the already disrupted and vulnerable context of remote learning presented a fine target. These incidents thus reflect a continuum between online and mainstream culture and educational and corporate contexts.

University administrators and instructors alike had to work in accordance with institutional, governmental, and corporate provisions to counter-declare against external threats to security and hospitality. By the end of March, many educational institutions had realized that unrestricted screen sharing was a likely vector for Zoombombing and had changed the default policy to restrict screen sharing to hosts of Zoom meetings. In early April, the FBI retroactively released security guidelines on videoconferencing that recommended password protection, waiting rooms, and other restrictions on guest access (Department of Homeland Security). They noted that the speed and lack of knowledge was a major cybersecurity vulnerability during the pandemic pivot online (Department of Homeland Security). Lamenting “I really didn’t understand why hackers would want to hack into a classroom,” Yuan and Zoom released a series of security updates and instructional safety blog posts (quoted in Konrad). These tactics by no means constituted a synthetic declaration—the problem of Zoombombers and trolls more broadly is still very much intact, but they increased the options for users to counter-declare against the attackers. Although Zoombombing acts as perhaps the most aggressive, external exploitation of vulnerability, many other breaches in hospitality occur within the system itself.

Apart from individual trolls, governmental actors posed an issue to hospitality in the Zoom University environment. One of the initial concerns about Zoom’s use in the U.S. in March and April 2020 was the fact some of the development of the platform happened in China and that they routed data through servers in China (Margolin). Its encryption methods made it particularly vulnerable to espionage from the Chinese government (Peters; Marczak and Scott-Railton). In response, Zoom publicly announced that “users outside of China won’t have their data routed through China” and further noted that users with paid subscriptions could select the regional centers through which their data would be routed (Jayarajan; Peters). Zoom’s data-routing measure implicitly admits the
potential for data breaches through unintentional contact with international channels. And that paid users may mitigate this unintentional contact again reveals that privacy, security, and ultimately the ability to effectively counter-declare are premium goods. International politics and differentiated access, present even before the pandemic, play out even more in our mediated classrooms.

Hospitality on Zoom networks has been tested in local, familial ways as well. For example, the collision between home and work has been happening for decades (Hochschild, *The Time Bind*, xxi) but is accelerated by pandemic teaching contexts. We no longer meet in the institutional space of the classroom, which, although not a neutral space because of participants’ different affiliations with it, is still a space removed from the intimacy of home. Universities provide access to our Zoom rooms, but we use our own home networks to host it. Our students have entered our home; we have entered theirs. In March 2020, we scrambled to convert spare rooms and apartment corners into home offices (sometimes shielded behind a virtual Zoom background) and find places for the kids to be neither seen nor heard.

![Figure 2: New Yorker; tweet featuring cartoon by Teresa Burns Parkhurst, “We’re all pretending,” 6 May 2020.](https://twitter.com/NewYorker/status/1258111051033448452)

At Zoom University, we are constantly being surveilled by colleagues and students. Our gestures or mics are often muted, but we learn anyway about each other’s children, pets, parents, roommates, and living situation. We experience “Zoom exhaustion” from repairing the missing gestures and social cues, listening carefully through audio glitching, and filtering out the irrelevant visuals in other people’s backgrounds (Jiang). Although the “bring your whole self to work” movement has made space for personal lives (e.g., sexual orientation, family status, or other expressions of identity) within work lives, this movement has been sudden, and for some quite jarring. For faculty, who are
disallowed either professionally or socially from turning off their cameras and muting, the dual intrusions of work and home are unavoidable.

Due to the nature of globally networked technology, this local and more benign or incidental surveillance translates to breaches in vulnerability beyond meetings and classrooms. In-person teaching contexts have already manifest these collisions through the intrusion of social media in classrooms. Videos of professors violating particular political values are circulated to stoke accusations of problems endemic to universities. These videos, taken in closed-classroom settings by students, take extemporaneous moments in the context of a semester-long course, isolate them, and reposition them in new political contexts (Losh 77-90). As Zoom classes are frequently intentionally or inadvertently recorded, the possibility of this circulation multiplies exponentially. Discord can result, demonstrating some challenging outcomes of hospitality that our courses have already been subject to in a globally networked world.

Our classrooms have been global for some time, but they are open to the network more than ever. Because this networked community is by no means homogenous, the experiences of those operating within it vary in accordance with pre-existing power differentials.

**Zoom University accentuates existing inequalities of race, class, and gender**

In the process of technologizing and corporatizing the university, the erosion of possibilities to opt out, and the new challenges of hospitality over our networks in pandemic teaching, bodies remain. And bodies experience these forces in different ways. The stratification of social class and other pressures plays out in Zoom University, just as it does in traditional universities, although the configurations of challenges may be heightened for women, transgender students, more vulnerable students, and Black, Indigenous, and People of Color (BIPOC) students and faculty. In gesturing towards some of the ways that surveillance affects marginalized communities and compounds stress, we extend the claim that higher ed’s pandemic turn to networked technology accentuates pre-existing power differentials both by denying access to necessary tools to certain groups and placing heightened labor expectations and elements of surveillance and control on others. In this analysis, we draw on theories of surveillance that attend to racialized and gendered bodies such as Ruha Benjamin’s and Chris Gilliard’s work on commercial surveillance technologies and racialized bodies, arguing that the same technologies affect bodies in different ways (see, for instance, Benjamin’s *Race after Technology* and Gilliard’s “Caught in the Spotlight”).

Increased use of surveillance technology pointed at a group is a signature of marginalization; however, lack of access to these tools can be just as problematic (Gilliard). Students have had difficulty fitting themselves into the pandemic paradigm of education for a variety of reasons related to differences in resources and responsibilities. Most students (54%) reported home/family responsibilities such as child and elder care as a challenge during the pivot (Digital Promise). A survey released by Digital Promise, a nonprofit organization committed to closing the digital learning gap, reports that responsibilities were felt most among Hispanic students: 27% reported home/family challenges as opposed to 18% of Black students and 12% of non-Hispanic white students (“Suddenly Online”). Low-income students also experienced greater challenges in online learning because of lower access to the technologies needed to facilitate it (20% experienced online connectivity issues versus 12% in higher income households; “Suddenly Online”). Job loss and decreased access to university resources such as computer labs, libraries, and mental health services also hit more vulnerable students harder (Berg).
Other vulnerable students in prison-education programs could not legally attend classes through networked technologies, and so a growing and essential area of university outreach and equity was conducted through awkward, old-school correspondence models or were simply terminated (Erzen). HBCUs had to manage the crisis with fewer financial resources because “the same history of oppression and institutional racism that ignited protests against police violence across the U.S.A. has left most black schools underfunded, often operating on shoestring budgets and unprepared to absorb sudden shock” (Charles and Dobson). And the crisis has been more acute for HBCUs and their students, many of whom bear a disproportionate impact of the health crisis, family responsibilities, lack of housing, and fewer personal financial resources to withstand job loss (Clark).

Those who do have access to the tools to conduct education in the pandemic must contend with a shift in labor expectations. For academics who are parents with children at home, or for women in particular who must always “contend with the site of the home” when they pursue work outside of it (Enoch 5), the collapse of home and work that the pandemic has brought may be particularly fraught. Women, especially those trying to climb the academic career ladder with young children, are being knocked back. We have long known that despite the cosmetic improvements in the representation of women in academe, the pay gap persists, along with higher burden of student debt among women, slower career trajectories, and fewer opportunities for leadership roles—all challenges that are exacerbated for women of color (“The Simple Truth”). Balancing home and career for women was challenging even before the pandemic because women carry more of the cultural and time burden of domestic activities (Enoch; Hochschild, The Second Shift). As Betsey Stevenson, a professor of economics at University of Michigan, told the New York Times, “This pandemic has exposed some weaknesses in American society that were always there, [. . . ] and one of them is the incomplete transition of women into truly equal roles in the labor market” (Cohen and Hsu). This existing inequality led to an unprecedented exodus of women from the labor force in September 2020; four-times more women than men left work at a time when many school-aged children went back to school virtually and required home support to do so. The unemployment rate for Black and Latina women was far higher than that for women overall (Ewing-Nelson). The pandemic’s exacerbated collapse of work and home merely accentuates the challenges and disparities previously felt by women, particularly women of color.

As our bodies and faces are projected onto each other’s screens, and as our data is collected by fiat, the legacy of interconnections between educational technology, surveillance, and race are activated. Ruha Benjamin argues that although “technology is imagined as impacting racial divisions—magnifying or obliterating them [. . . ] racial ideologies [also . . . ] shape the design of technologies” (43), for instance in AI facial recognition (Buolamwini), online search (Noble), and home security cameras (Gilliard, “Caught in the Spotlight”). Gilliard points out that in their digestion of data and deployment, these purportedly “neutral” technologies can amplify racial disparities. For example, technologies that track students have a dangerous legacy that is revived in this time characterized by pandemic and protest, when privacy is a premium good (Gilliard, Infoecosystems podcast). The forms of quantification that our course management systems employ (e.g., tracking student views and visits and word counts) connect to that legacy. Recalling Fanon, Simone Browne calls this a type of “control by quantification” and points to slavery’s legacy and surveillance as operative in contemporary technologies (Browne, Dark Matters, 6). Similarly, Jacqueline Wernimont traces the Anglo-American tradition of this impulse toward quantification, unraveling threads of religious, imperial, and patriarchal paradigms. Especially in the collection of statistics about life and death—which overshadow education in the COVID moment—the corporate and state organizations that control data loom larger. User data is controlled not by those who produced it but by the
corporations who collect it and share it among partners as Zoom’s and most major corporations’ privacy policy allows.

To the racialized legacy of quantification in surveillance, Simone Browne adds racialized visibility as shaping the ways these technologies are received (“Surveillance”). Videoconferencing in particular indexes the histories of visibility and performance in both theater and art, as our bodies are flattened into images on the screen. Dull lighting and muted colors on screen mean that our faces are projected differently. We can “hide self view” on Zoom as a way of curtailing this self-surveillance or counter-declaring, but the experience of performance on screen remains nerve wracking, especially for those with histories of being looked at or performing for others. YouTube makeup and lighting tutorials for the Zoom era are primarily aimed at women, who may feel hyper visible on the screen because of a long history of being objects under a gaze. Connected to a history of Black performance and minstrelsy, Ebony O. McGee and Lasana Kazembe argue that Black professors have higher expectations for performance in academic settings. The legacy of Black performance in theater and screen may influence the videoconferencing experience as well.

Transgender, non-binary, and other gender non-conforming students encounter a unique tension between performance and identification in virtual classrooms. Students’ name concerns including deadnaming (referring to a transgender individual by their birth name), misgendering, and vulnerability. Speaking to Boston University’s paper, The Daily Free Press, a student notes that “manually changing names can become complicated for those who still have their deadname listed in Blackboard” (Lederman). Another student “said they have been misgendered when their camera is turned off due to professors not looking at their name and instead going off of the sound of their voice.” To address transgender visibility issues, many universities (e.g., UC San Francisco, Wooster, Dickenson, etc.) have released guidelines regarding the inclusion of pronouns in Zoom. Explicit declaration of pronouns in Zoom titles, along with the increased practice of including them in email signatures can enable students and faculty both to learn names and pronouns (Pran). However, compulsory pronoun disclosure also runs the risk of causing discomfort to students who are in the process of transitioning or exploring their gender identity. Writing for Fordham Lincoln Center’s student paper, The Observer, Vicky Carmenate points out that “It is not easy to state your pronouns when your physical appearance does not match the societal standard of who people are.” Moreover, any policy or personal choice regarding pronouns is explicit in Zoom, simultaneously and constantly displayed in the visual field, rendering it an overt, political choice for all students.

As John Berger theorized with camera and film, the machine mediating our images changes the way we see ourselves and others—and these changes redound differently on different types of bodies. Updating Berger in the age of computer vision, Azar, Cox, and Impett argue that our images become data artefacts once they are projected into the computer, where their apparent visuality then hides complex computational and social processes. In this section, we’ve outlined how gendered and racial orders of surveillance, visibility, and quantification undergird the apparent visuality of our projected images in Zoom. Educational technology assimilates technology’s histories, especially when it derives from corporate contexts, as Zoom does. These histories accumulate in the pandemic educational context as they are channeled through new platforms of visual projection. Berger’s project—and ours—is to uncover those processes and build toward a literacy in the face of these imagistic technologies.

**Bodies upon the gears: Resisting Zoom University**

Audrey Watters draws our attention to Mario Salvio’s “bodies upon the gears” speech on the steps of Sproul Hall at Berkeley in 1964, a particularly evocative articulation of this resistance against the
mechanisms of corporatization, when students were protesting Berkeley’s ban on political activity (Watters, “All Watched Over”). Pointing to the way that the Berkeley administration likened the Board of Regents to a Board of Directors of a corporation, Salvio proclaimed that students should resist being turned into “raw materials” to be “made into any product” or “bought by some clients of the University.”

We’re human beings! [. . .] There’s a time when the operation of the machine becomes so odious, makes you so sick at heart, that you can’t take part! You can’t even passively take part! And you’ve got to put your bodies upon the gears and upon the wheels [. . .] upon the levers, upon all the apparatus, and you’ve got to make it stop! (quoted in Watters, “All Watched Over”) 

The conflation here between the corporatizing and technologizing of the university—and the negative result on education—uses earlier metaphors of mechanical technology, but it still resonates. In this polemical example, we see students as resistant subjects of an educational machine, instructors occupying a shifting moral ground between persisting as gears or becoming liberators, and corporatized institutions as the controllers of the machine through the vehicle of technology.

Administrators, instructors, and students are all surveilled subjects. However, as we analyze the power differentials, we see that the mechanisms of surveillance and control mediate different subjects disparately while implemented largely unidirectionally through the hierarchy of higher education. Resistance, then, is not a uniform act but a series of counter declarations that are contextually dependent on the subject positions of the surveilled. Here, we examine real and imagined modes of opposition that are or could be carried out by the administrators, instructors, and students. While we may be emerging from the pandemic and thus the totalizing space of all-Zoom classrooms, these counter-declarations will remain relevant in the inevitably networked and mediated classrooms we will teach in from here on out.

Administrators

As both authors come from English composition backgrounds, we specifically discuss the counter-declarations enacted by Writing Program Administrators (WPAs). We hope that these counter-declarations can be applied beyond English departments and encompass policies surrounding teaching and learning in a surveilled academy more broadly. WPAs resist through training initiatives and policy.

HyFlex scenarios recommend, or promise to students who wish to participate asynchronously, that instructors record classes. Recordings can make classes more accessible to students and they can also enable asynchronous teacher observations. But in so doing, recordings introduce additional elements of surveillance and vulnerability. Personal writing catalyzes disclosure, and composition instructors contend with students sharing personal details ranging from the mundane to the traumatic within the scope of narrative assignments and class discussions (Larson 48-49; Spear 53). If classes are recorded, these moments are preserved and in greater danger of circulating beyond the class and rupturing hospitality. As danah boyd observes in her analysis of the affordances of digital publics, data produced within digitally networked publics is persistent, replicable, scalable, and searchable (45). If a conversation about a sensitive topic is recorded in a hybrid classroom, it too will be subjected to these properties. When adopting the HyFlex model (e.g., Beatty), it is crucial for WPAs to alert faculty to the dangers alongside the affordances of recording composition classes.

Facing the HyFlex model at her university, the WPA co-author of this article (Vee) wrote a policy about classroom recording that describes some of its affordances as well as its vulnerabilities, while
leaving room for instructor discretion (https://annettevee.com/documents/FlexPittRecordingPolicy.html). In writing such policies, WPAs must consider student rights to access as well as privacy, the legalities of recording, available technological platforms, and instructor autonomy. Informed consent of students is a legal requisite to recording in most states. Enabling informed decisions about recording should be the WPA’s job. Although WPAs can offer guidance and structure regarding the use of surveillance technology as a form of counter-declaration, it is the responsibility of faculty and staff to interpret these policies and ethically use the technology.

Instructors

Those of us in pedagogical roles can counter-declare by making conscious choices to use technology in a way that is appropriate for the culture of our classrooms and by informing students about the consequences of the technology being used.

Although the pandemic hardwired surveillance technology into our educational infrastructure, we still have a degree of control over the degree to which we opt in. We can choose not to use technology that is not mandated by our institutions. Stating, “We do not do our best, most interesting work when we know we are being watched,” John Warner cautions teachers about automatically using tracking programs such as plagiarism checkers. Tyler Sonnemaker further argues against software like Proctorio, which exacerbates power differentials, especially along the lines of race, class, neurodiversity, gender, etc., by mimicking policing tactics. We can counter-declare by mitigating the authority of infrastructural software, by developing alternative expectations surrounding the participation and engagement of our students, such as the use of synchronous chat or asynchronous blogs, and by supporting students who may not be able to speak as readily on screen because of issues ranging from anxiety to technical problems. And, of course, we can choose not to record our classes, or at least the portions where students are actively participating. Our pedagogy can further reflect these practical decisions.

Although we were and are compelled to teach through Zoom, we can also teach about Zoom. Doing so lends us the opportunity to form a lesson about privacy and data literacy that is transferable to other aspects of our students lives. Estee Beck argues that in networked environments, writing instructors in particular have a responsibility for starting conversations with students about privacy and surveillance. Like most tech companies, Zoom practices maximalist data collection, and by using it as an already present rhetorical artifact, we can help students reflect on their own, often coerced, participation in surveillance capitalism. Alexandria Lockett shows us a way to encourage students to embrace their own authority in technologies. Using the example of Wikipedia, a free and openly editable resource, she notes that ostensibly free technologies do not feel freely available to students who have not been conditioned to see themselves in positions of power regarding technology (Lockett). Teachers can help them embrace that authority and then take advantage of their available resources. Although opting out of screen projection is technically possible, requirements for students to be visible on screen and knowledge of options such as “hide self view” render the possibilities for opting out different among users. In situations where opting-out is still possible, and where privacy settings are available, more tech-savvy users must have and embrace their own authority to counter-declare surveillance.

Students

As they are perhaps the group most vulnerable to surveillance, students also enact the most obvious forms of resistance. We see them making technological counter-declarations within our classrooms
and resisting institutions more broadly through lawsuits. However, these acts are not necessarily cut and dry, and in many cases, when students resist, they risk losing the connection that this technology forges.

When teaching at Zoom University, many instructors have lamented the fact that students refuse to turn their cameras on. Some instructors mandated camera use. Although frustrating to instructors, a student’s choice to turn their camera off can be read as a counter-declaration against surveillance, one to which we should be sympathetic, and one which we can discuss openly and strategically with students. Explaining “Zoom fatigue” as “a pan-descriptor for the symptoms people experience after prolonged technology use—typically CMC [computer-mediated communication] platforms with AVT [audio-video technology],” Robby Nadler notes, “While many report varying issues, the general cost is exhaustion (both physical and mental)” (2). He further clarifies, “That is, interactions that normally do not tire people when conducted in FtF [face-to-face] contexts now deplete people when these same interactions occur virtually” (2). In turning off their cameras, students attempt to combat the exhaustion of being surveilled, but doing so compromises their ability to engage and learn through the available medium. We can first invite students to share their reasons for turning off their cameras to see if we might approach the classroom differently. Taking their exhaustion into account, we can also schedule breaks and agree on times in class when everyone can turn off cameras. We can encourage students to play with how they represent themselves in their backgrounds, camera-off screens, or names.

Student lawsuits constitute another form of resistance. Many of these lawsuits demanded tuition refunds, arguing that online education is intrinsically worth less than its in-person counterpart (Anderson). The lawsuits against universities for the dehumanizing yet still expensive Zoom University are easy to critique for the ways they highlight students’ consumer orientation to campus-based universities and the ways they discount the difficult choices universities were compelled to make during the pandemic. But taking their arguments on the merits, we can hear students protesting ed-tech’s unprecedented visibility at Zoom University. Students and faculty are newly and increasingly aware of what ed-tech has been doing to them all along: turning them into products; depersonalizing the experience of education; subjecting them to surveillance; and exacerbating differences in intersectional identity performance.

**Conclusion**

Given these histories and contexts, we should resist the increased surveillance involved in test proctoring and digital participation in pandemic education. If education is going to bend toward justice, questions of privacy, visibility, and authority must be considered of a piece. We must acknowledge the context of the technology that we have so readily and necessarily adopted by identifying its history, its vulnerabilities, and the ways in which it exacerbates the power differentials that are already present within our institutions. And as we learn how the social and medical disparities between populations do not flatten when coronavirus infects bodies, we need to be aware of the different levels of visibilities in the Zoomification of education. We can see that the hierarchies of higher ed are spiking along with our COVID-19 case counts: well-funded, elite institutions are better equipped to weather the storm; tenured faculty are less likely than adjunct faculty or staff to lose their jobs or have significant exposure to the virus; students without good access to technology to facilitate videoconferencing will have diminished educational experiences. Funneling higher ed through Zoom since March 2020 has resulted in amplifying rather than flattening disparities.
We must question the infrastructural role of corporate technology in higher education, writing modes of resistance within the system through our policy, flexibility, and digital literacy. We must counter-declare against surveillance and corporate control, not by forgoing technology, but by choosing and developing technology that enables us to teach and our students to learn. Zoom has changed the landscape of ed tech. What began as an accessibility tool for universities to continue providing their instruction and services will have a lasting impact on higher education in a post-pandemic world. Universities are now equipped with the digital infrastructure, policies, and trained staff to provide virtual alternatives to in-person learning. Although this updated system undoubtedly introduces new opportunities for accessibility, including flexible labor and learning, it also risks exacerbating existing power differentials and threatening university subjects’ privacy. Future research in this area should examine concerns about privacy and surveillance alongside accessibility affordances for students and faculty for whom the physical classroom has always been challenging. Going forward, we can continue to explore modes of synthetic declaration—alternative systems that center on vulnerable groups and empower them to access education while they control their data and self-presentations within their institutions and their networks.

Works Cited


enculturation is published under an Attribution-NonCommercial-ShareAlike Creative Commons License.
Please see our copyright page for details.