

Resisting Crisis Surveillance Capitalism in Academic Libraries

Callan Bignoli, Sam Buechler, Deborah Caldwell et Kelly McElroy

Volume 7, 2021

Special Focus on Refusing Crisis Narratives

URI : <https://id.erudit.org/iderudit/1084791ar>

DOI : <https://doi.org/10.33137/cjalrcbu.v7.36450>

[Aller au sommaire du numéro](#)

Éditeur(s)

Canadian Association of Professional Academic Librarians / Association
Canadienne des Bibliothécaires en Enseignement Supérieur

ISSN

2369-937X (numérique)

[Découvrir la revue](#)

Citer cet article

Bignoli, C., Buechler, S., Caldwell, D. & McElroy, K. (2021). Resisting Crisis Surveillance Capitalism in Academic Libraries. *Canadian Journal of Academic Librarianship / Revue canadienne de bibliothéconomie universitaire*, 7, 1–25.
<https://doi.org/10.33137/cjalrcbu.v7.36450>

Résumé de l'article

Dans cet article, nous examinons ce que nous identifions comme le capitalisme de surveillance de crise dans l'enseignement supérieur, en nous appuyant sur les travaux de Naomi Klein et Shoshana Zuboff. Nous définissons le capitalisme de surveillance de crise comme l'intersection de la collecte de données non réglementée et omniprésente avec la marginalisation continue des groupes raciaux et sociaux vulnérables. À travers cette grille, nous examinons les récits de crise liés à la réussite étudiante et à l'intégrité académique et examinons comment la pandémie de COVID-19 a permis des soi-disant solutions qui collectent des quantités massives de données sur les étudiant.e.s en toute impunité. Nous suggérons un cadre de refus du capitalisme de surveillance de crise issu des travaux de Keller Easterling et Baharak Yousefi, identifiant des moyens de résister et de construire le pouvoir dans un contexte où la source du mal est partout et intentionnellement cachée.

© Callan Bignoli, Sam Buechler, Deborah Caldwell, Kelly McElroy, 2021



Ce document est protégé par la loi sur le droit d'auteur. L'utilisation des services d'Érudit (y compris la reproduction) est assujettie à sa politique d'utilisation que vous pouvez consulter en ligne.

<https://apropos.erudit.org/fr/usagers/politique-dutilisation/>

érudit

Cet article est diffusé et préservé par Érudit.

Érudit est un consortium interuniversitaire sans but lucratif composé de l'Université de Montréal, l'Université Laval et l'Université du Québec à Montréal. Il a pour mission la promotion et la valorisation de la recherche.

<https://www.erudit.org/fr/>



Resisting Crisis Surveillance Capitalism in Academic Libraries

Callan Bignoli

Olin College of Engineering

Sam Buechler

Washington State University Vancouver

Deborah Yun Caldwell

University of North Carolina at Greensboro

Kelly McElroy

Oregon State University

ABSTRACT

In this paper, we consider what we identify as crisis surveillance capitalism in higher education, drawing on the work of Naomi Klein and Shoshana Zuboff. We define crisis surveillance capitalism as the intersection of unregulated and ubiquitous data collection, the continued marginalization of vulnerable racial and social groups, and a persistent and performative state of emergency in the academy. Through this lens, we examine the twinned crisis narratives of student success and academic integrity and consider how the COVID-19 pandemic further enabled so-called solutions that collect massive amounts of student data with impunity. We suggest a framework of refusal to crisis surveillance capitalism coming from the work of Keller Easterling and Baharak Yousefi, identifying ways to resist and build power in a context where the cause of harm is all around and intentionally hidden.

Keywords: *academic integrity · COVID-19 · privacy · student success · surveillance*

RÉSUMÉ

Dans cet article, nous examinons ce que nous identifions comme le capitalisme de surveillance de crise dans l'enseignement supérieur, en nous appuyant sur les travaux de Naomi Klein et Shoshana Zuboff. Nous définissons le capitalisme de surveillance de crise comme l'intersection de la collecte

de données non réglementée et omniprésente avec la marginalisation continue des groupes raciaux et sociaux vulnérables. À travers cette grille, nous examinons les récits de crise liés à la réussite étudiante et à l'intégrité académique et examinons comment la pandémie de COVID-19 a permis des soi-disant solutions qui collectent des quantités massives de données sur les étudiant.e.s en toute impunité. Nous suggérons un cadre de refus du capitalisme de surveillance de crise issu des travaux de Keller Easterling et Baharak Yousefi, identifiant des moyens de résister et de construire le pouvoir dans un contexte où la source du mal est partout et intentionnellement cachée.

Mots-clés : COVID-19 · intégrité académique · réussite étudiante · surveillance · vie privée

A CONSIDERATION of core professional values for library workers in North America may lead you first to the American Library Association (ALA) *Code of Ethics* (2017a), the American Library Association *Library Bill of Rights* (ALA 2006), or the International Federation of Library Associations and Institutions (2012) *Code of Ethics for Librarians and other Information Workers*. All of these documents underscore the importance of patron privacy in library services, and indeed many academic library workers would identify privacy as foundational to a library's mission (ALA 2017b). The ALA *Code of Ethics* states, "We protect each library user's right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted" (ALA 2017a). Article VII of the *Bill of Rights* reads, "Libraries should advocate for, educate about, and protect people's privacy, safeguarding all library use data, including personally identifiable information" (ALA 2006). A legal dimension to this focus on privacy extends beyond professional ethics as well. In Canada, education is under provincial jurisdiction; acts including British Columbia's Freedom of Information and Protection of Privacy Act (FIPPA) require protection of certain types of information about students. In the United States, several laws exist at the state level to protect the privacy or intellectual pursuits of library patrons; additionally, the Family Educational Rights and Privacy Act (FERPA) and Protection of Pupil Rights Amendment (PPRA) protect student information.

The ALA *Code of Ethics* and *Library Bill of Rights* have both been amended a number of times since their original ratification by the organization's council in 1939. Many things have changed in libraries over the last eighty years, including our definitions of library use data. What is important to acknowledge, however, is just how hard it has become to understand what use data *is*—how it is used, where it is kept and by whom, what is already being done with it, and where it might end up. The academic library's place is usually cast as support for protagonists: faculty, students, and the institution as a whole. When forces outside the library request aid, the library, ever service-oriented, often complies, eager to prove its value and demonstrate it through use data, particularly given ever-shrinking funding for higher education. As a result,

while we may see ourselves as champions of privacy, academic library workers are often complicit—knowingly or not—in compromising user privacy, either directly through the tools and collections we provide access to, or tacitly through participating in broader collection and use of data by our institutions.

As we have seen again and again in the last few decades, during moments of crisis and social unrest, civil rights such as privacy are often curtailed while the profit margins of big businesses skyrocket. A key example of this phenomenon is described in Naomi Klein's *The Shock Doctrine* (2007), where she details the George W. Bush administration's use of political and environmental crises to push forward corporate interests. The crisis narratives around 9/11 led to impacts including amplification of government surveillance. The USA PATRIOT Act, passed less than two months after the 9/11 attacks, dramatically tightened U.S. national security with an emphasis on the surveillance of electronic information. Section 215 of the act required that library workers cooperate directly with law enforcement, spurring a now oft-cited moment of resistance to surveillance among library workers. In response to Section 215, the ALA issued statements and attempted to influence legislation, and some library workers publicly refused to cooperate (Estabrook 2003), seeking to ensure that circulation records were expunged (Drabinski 2006). Though Section 215 technically expired in March 2020, in the years since 9/11, the rise of surveillance capitalism and unmitigated user data collection has created a host of new privacy protection challenges for library workers.

Since 9/11, academia in general and libraries specifically have gone from objecting to the very obvious dangers of government surveillance to embracing a more insidious version of the same tactics under the guise of using data collection to demonstrate value, efficacy, and the justification of dollars spent. This reflects the broader societal acceptance of surveillance capitalism as defined by Zuboff (2019): the commodification of personal data for profit-making or achieving other institutional goals. Megan Oakleaf's widely read and respected 2010 ACRL publication, *Value of Academic Libraries: A Comprehensive Research Review and Report (VAL)*, encouraged a framing of value in libraries centered around quantifiable data obtained through student surveillance and removed from "external perceptions of quality and satisfaction with library services" (Oakleaf 2010, 4). Since its publication, our professional development landscape has been littered with workshops, trainings, how-tos, and vendor products aimed at helping libraries prove their value to penny-pinching administrators and skeptical naysayers. But today, assessment and surveillance technologies have expanded far beyond what existed when this framework was developed. And now, eleven years later, academic libraries have the capacity to *prove* more than ever before. As designated gateways to knowledge that

manage access to vendor databases and provide computers and other educational technology by which to access these online materials and others required for study, and as physical locations that may require credentialed access to buildings through means such as card-swiping, libraries are, knowingly or not, collecting unprecedented amounts of data on the populations they serve. In a study intended to assess the library's impact on graduation rates, Soria *et al.* (2017) reported on student usage data including

loaning books (including interlibrary loans and electronic books), using electronic resources (including academic journals accessed, website used, and databases searched), logging into library computer workstations, enrolling in library instruction courses (introduction courses, workshops, or instruction integrated into courses), and reference resources used (such as meeting with a peer research consultant or chatting with a reference librarian). (Soria *et al.* 2017, 815).

This interest in quantifying as much as possible about the experience of using a library, combined with the growth of software platforms and data collection tools to quantify it, has become prevalent but our existing policies, procedures, and professional standards have not adapted to address these practices. Before the era of Big Data, any surveillance mechanisms applied to our patrons such as manual door counts, usage statistics, and so forth could be expunged, and their tangible nature limited the scope of potential harms. Now, libraries can harvest patron data to a degree far beyond what was manageable in the era of tangible recordkeeping, and these data are far more easily shared and kept in perpetuity. University systems and other parent institutions may now require libraries to collect and share data with other campus departments, such as in the case of card-swipe data, and control of the preservation and security of those data then lie outside the jurisdiction of the library.

Between the trend toward more unified control of student and user surveillance data by university campuses and general awareness of the pervasiveness of data collection by technology companies, there is a widespread sense of futility when it comes to privacy, including in libraries. If the vendors and data aggregators are going to get the data anyway, the argument goes, then why shouldn't libraries have as much opportunity to use those data to our advantage? And if the vendors can help us organize and interpret our own data for purposes of assessment and value-proving, then so much the better. Many libraries have accepted invasive assessment practices and tools with little pushback, failing to acknowledge how the collection and reporting of metrics other than circulation undermines patron privacy. The potential for quantifying and creating value is too great a temptation for undervalued and cash-strapped libraries to refuse. We have accepted vendor proposals and practices as they are written, and we imagine a walled garden between library data and the massive corpus of data collected about all people where there likely is none. Thus, libraries'

role as explicit or implicit collaborators in the wider academic surveillance problem must be acknowledged and addressed.

Writing this in 2021, we are alarmed at how existing concerns about academic integrity and student success have ballooned during the COVID-19 pandemic. These existing concerns—that without monitoring and preemptive measures, students will inevitably cheat and damage the value of the institution; that without intrusive data collection, students (particularly from marginalized communities) will not complete their education—already rest on questionable premises, and the technological solutionism of the neoliberal university is an unsurprising response to these moral panics (Morozov 2013; Seeber 2016). Oakleaf’s (2010) framework provides renowned and pervasive articulation of this mindset in academic libraries. It has been central to the field’s embrace of learning analytics, or LA—described succinctly as “educational data mining” by Jones and Salo (2018) and first conceived in the aftermath of another crisis, the Great Recession—leading to libraries tracking student use of their buildings and resources in an attempt to quantify their importance on campus, as in the case of Soria *et al.* (2017). The COVID-19 pandemic has only exacerbated these concerns, magnifying both the potential, presumed threats to academic integrity and student success and the resultant inflated measures to anticipate and prevent them. The tangible aspect of LA has an especial appeal at times like these, offering what looks like quantifiable answers to the burning questions of how student success and academic integrity are affected by the ongoing crisis. While data-driven measures may be described as innovative, they often instead encourage a narrow-minded view of how academic performance can be assessed. Instead of exploring new ways of evaluating student success in order to better accommodate remote learning during a deadly global pandemic, academic institutions judge how things are going through the lens forged by LA frameworks in wholly different circumstances, continuing to focus on what can be measured through abundant user data.

Naomi Klein identified new articulations of disaster capitalism just a few months into the COVID-19 pandemic in her essay “Screen New Deal” (2020). She describes how the pandemic has provided another opportunity for big technology companies to turn big profits, creating “a living laboratory for a permanent—and highly profitable—no-touch future.” Unwittingly or not, academic libraries and their parent institutions are contributing to the “pandemic disaster capitalism” that Klein identifies. With the onset of the COVID-19 pandemic, colleges and universities transitioned to remote instruction models and spent extensively on academic surveillance technologies, often with little or no pushback or even informed processes at all. In December 2020, amidst severe layoffs of teaching faculty, the City University of New York signed a two million dollar contract with Turnitin, a plagiarism-

detection product (Waltzer 2020). Education technology companies have capitalized on this moment, creating vicious cycles of profitability for themselves at the expense of both institutions and students. Citing the unavailability of academic resources during lockdown periods, students turned to Chegg, a website that provides a massive database of digitized textbooks (including answer keys) in exchange for \$14.95 USD a month (Adams 2021). “Publishers, after selling expensive textbooks to students, sold the answers to the homework questions in those expensive books to Chegg,” explains educational technology (edtech) writer Michael Feldstein (2021). “Chegg sells the answers to the questions to the students, who often use them to cheat. To combat this problem, universities pay for proctoring software.” As libraries traditionally serve as a hub for access to course materials, including textbooks, they are caught up in broader waves of surveillance technologies; indeed, “the very services libraries depend upon to fill their collections endanger patron privacy” (Lamdan 2019).

Channeling the resistance of some of our colleagues in the aftermath of 9/11, we call on library workers to resist academic surveillance and, in so doing, refuse crisis narratives around student success and academic integrity that have been amplified by the COVID-19 pandemic. We also have learned from our history: we recognize that celebrating the incremental success of resistance can obscure the wider failures. Despite how we might remember the period immediately after 9/11 twenty years later, not all library workers joined in refusing law enforcement requests for voluntary cooperation in providing information about patrons' reading habits and Internet preferences (Estabrook 2003). The one-time resistance of some library workers to state surveillance of circulation records did not prevent the much larger-scale surveillance apparatus from growing. “There are . . . fundamental limits to a strategy of resistance that is essentially reactive and narrow in focus,” Emily Drabinski warned in 2006 (14). “While librarians respond quickly and effectively to challenges posed [in the wake of 9/11], we have little in the way of sustained resistance to systemic forces that undermine information equity and access in less visible but more fundamental ways” (Drabinski, 14). Library workers can also struggle to convert our codes of ethics into meaningful action. As Sarah Lamdan writes, “library ethics are points upon which we should hold our vendors accountable, not obligations to internalize and carry on our backs” (2019). To that end, we will focus on ways that library workers can seek coalition with others—students, other academic workers, and beyond—and to be vigilant about how libraries fit into the broader culture of growing academic surveillance.

Background

As we consider these surveillance technologies and practices, two particular concerns guide our discussion. First, we recognize that the companies behind these tools tend to hold onto data indefinitely, giving users little transparency about how it is shared, let alone any control over the retention schedule. Second, we recognize that surveillance technologies and practices replicate and deepen existing social biases. Together these concerns create conditions that can implicate academic libraries, even unintentionally, in broader nets of surveillance.

Lack of Transparency and User Control

While institutions of higher education may face some compliance requirements (such as FERPA in the United States), colleges and universities may themselves collect certain types of data without clear or enforceable limits. At the very least, we have seen that universities are reluctant to interfere in the data collection activities of their vendors, as reflected in the relative silence of the University of British Columbia regarding Proctorio's lawsuit against its employee Ian Linkletter, who posted on Twitter about the invasive data collected by the proctoring software (Alden and Ha 2020).

When information about someone becomes digitally instantiated, or taken from “the real world” and captured in the form of something that can be processed and communicated by machines, it becomes a liability for the person in question because of the lack of legal protection and the opacity of what that data looks like and where it winds up (Public Books 2020). The very process of digital instantiation of certain data may directly contradict long-standing library commitments to patron privacy. As an illustrative example of this, many colleges and universities employ keycard access systems that require students and employees to tap or swipe an identity card to enter buildings and spaces on campus, including libraries. While most library workers would balk at the idea of requiring patrons to sign a visitor log that may be shared with non-library entities, in the case of keycard access data, library employees may not be aware that these data exist, let alone know who has access to them, where they are stored, or who may request them.

Unfortunately, this data opacity doesn't begin and end at keycard access. Because of the nature of the internet in 2021—driven as it is by targeted advertising and marketing analytics—it has become extremely difficult for users to explore the web without being tracked in some form. This includes electronic resources, with their reliance on third-party tracking applications such as Google Analytics and Adobe Audience Manager. After studying the source code of fifteen publisher platform sites, Cody Hanson wrote that it is not “possible for libraries to provide meaningful

assurance of privacy or anonymity to users of licensed resources” (2019). It is not yet a common practice for libraries to make tracking detectors and ad blockers available on public-use computers, which, while not a complete solution, could provide a small degree of transparency,

User tracking is a logical offshoot of surveillance capitalism. It requires that as much information as possible be converted into a digital form to make predictions about, and therefore make money from, users of technology platforms. Zuboff (2019) writes that part of what makes this economic system possible is the “shadow text,” the information hoarded about users that is freely available for companies to access and monetize but never exposed to the people it is extracted from. The shadow text is embodied in the “data double,” a “digital duplicate of our lives captured in data and spread across assemblages of information systems” (Jones 2018). The data double becomes especially troublesome in reidentification—that is, when there is sufficient information in one or more databases to be able to identify a person who should have been, or believed themselves to be, anonymous. If that sounds like finding a needle in a haystack, consider an article recently published in *College & Research Libraries* about a study that used card-swiping data, demographic information, major, and other metrics to assess student success relative to library use. According to Briney (2021), combining the anonymized data in the study with publicly accessible reports from the U.S.’s Integrated Postsecondary Education Data System (IPEDS), LinkedIn profiles, and online graduation announcements would make identification of specific library users possible. The current era of ubiquitous data collection and minimal regulation extends well beyond academia, moreover; a 2019 study determined that a combination of fifteen demographic attributes (such as date of birth, zip code, marital status, and race) from various data sources would render 99.98% of the population of Massachusetts uniquely identifiable (Rocher *et al.* 2019). Our data doubles and shadow texts are more intimately linked to us than we realize.

Big tech companies such as Facebook, Google, and Amazon are the dominant players in surveillance capitalism, but their lucrative business models have captured the interest of smaller players in other industries, including education. As Hanson’s (2019) research, the SPARC Community-Owned Infrastructure project, and the Library Freedom Project’s Vendor Privacy Scorecard (2021) show, library vendors do not have a track record of sharing library workers’ values about patron privacy, and they build their platforms accordingly. Beyond user tracking, libraries’ commitment to patron privacy and equal access may also be directly incompatible with the broader practices and policies of vendors. In addition to selling library subscriptions for popular legal database Westlaw, Thomson Reuters built the CLEAR Investigation software used by U.S. Immigration and Customs Enforcement (ICE), “use[d] to collect

thousands of data points on people in order to assist with their investigations and identify community threats” (DiVittorio and Gianelli 2021). Beyond the research databases it sells to universities and colleges throughout the world, LexisNexis’ lucrative Risk Solutions arm of its business appears to be supplanting CLEAR for the ICE contract (Biddle 2021). To stay afloat at a time when print publishing is an endangered business model, “publishers are becoming predictive data analytics corporations” (Lamdan 2019). In a world where shadow texts and data doubles mean profitability, and an increased emphasis on quantifiable metrics drives administrative decisions and assessment in higher education, libraries are challenged to uphold privacy in an environment that actively undermines it.

Social Bias in Surveillance Technologies

Despite the rhetoric of neutral and sleek innovation that pervades Silicon Valley, computers and software replicate and can easily multiply the biases of the humans that built them. For example, facial recognition, which is used in proctoring software, shows bias against non-white users. In their *Gender Shades* project, Buolamwini and Gebre (2018) studied three commercial gender identification systems and consistently found that facial classification algorithms performed best with lighter-skinned males and most poorly with darker-skinned females. Students of color find themselves needing to trick proctoring systems into recognizing their faces. In the fall of 2020, one Afro-Latina user spent at least four hours contending with her face not being recognized by the program ExamSoft; she tried sitting under fluorescent light, natural light, and repositioning herself multiple times before the software accepted her image (Patil and Bromwich 2020). Writing in the *MIT Technology Review*, librarian Shea Swauger offers more examples of who is acknowledged and recognized as human by these programs and who is not:

A Black woman at my university once told me that whenever she used Proctorio's test proctoring software, it always prompted her to shine more light on her face. The software couldn't validate her identity and she was denied access to tests so often that she had to go to her professor to make other arrangements. Her white peers never had this problem.

Similar kinds of discrimination can happen if a student is trans or non-binary. But if you're a white cis man (like most of the developers who make facial recognition software), you'll probably be fine. (Swauger 2020)

Bias in technology both reflects and exacerbates historical patterns of disproportionate surveillance of Black, Indigenous, and other racialized communities, poor people, non-citizens, and other marginalized groups. Ruha Benjamin calls this “the New Jim Code”: new technologies that reflect and reproduce existing inequities but that are promoted and perceived as more objective or progressive than the

discriminatory systems of a previous era” (2019, 5-6). Or, as Safiya Noble writes, “technology consists of a set of social practices, situated within the dynamics of race, gender, class, and politics” (2012, ii). As prison abolitionist Mariame Kaba writes, whether it takes the form of technology or cops on the street, “surveillance is never neutral and it is situationally recognized. . . . Young Black people in particular are on some sort of inevitable march down the path of criminality [that] gives license to surveil, to watch, to strike them down before they grow” (2021, 89). Some test proctoring software flags inappropriate locations, which could be the parking lot of a local restaurant or public library where a student without home internet access can use the WiFi. This reflects historical patterns of racialized unequal opportunity. In Canada, only 45.6 percent of rural households (CRTC 2021) and just 30 percent of First Nations communities have access to 50/10 Mbps broadband connections (Stewart 2020). Similarly, in the U.S., roughly a third of American Indian/Alaska Native, Black, and Latino families lack access to high-speed home internet compared to only 21 percent of White families (Future Ready 2020).

Institutional policy that requires students to have their cameras on during Zoom sessions assumes they have a safe, quiet place to be “in class” at home, favoring the success of students with particular advantages their classmates may not share. In higher education, these technologies and pedagogical norms create an environment where students are set up to expect and accept surveillance, rather than recognize their own agency and opportunities to choose what data is collected and how it is used. Monitoring tests with proctoring software, rigidly enforcing norms for digital classrooms, and making conclusions based on library learning and usage statistics are all examples of what Ruha Benjamin has called “narrow solutionism,” or focusing on individual behavior rather than the larger systemic forces that impact student performance (2019). Citing Reeves (2015), Zoe Fisher (2018) writes, “[the] architecture of privilege permeates [student success] . . . [which is] systemic and structural, still more often defined by your zip code, income, race, and inheritance than almost anything else you do.” Instead of addressing or even considering the underlying disparities that might lead to a student’s perceived inattentiveness or inability to pass an exam without assistance—such as unreliable access or no access to the internet, uncomfortable or unsafe working conditions, or, for first-generation students, adaptation to the expectations of higher education—technologies are deployed as another means of enforcing conformity that exacerbates these disparities.

A response to crisis events built with technology that watches and tracks people with the intent of punishing them—such as Proctorio, Turnitin, and myriad LA software—creates a new matrix of oppression we identify as *crisis surveillance capitalism*, in which poorly regulated and ubiquitous data collection by highly

profitable analytics and technology companies intersects with the continued marginalization of vulnerable racial and social groups. Despite libraries' stated values and commitment to patron privacy, and whether or not it is their intention, they are often complicit in crisis surveillance capitalism.

Redefining Crisis Narratives

Libraries are sites of specific acts of academic and vendor surveillance and are complicit in campus-wide or even broader corporate regimes of data collection (Salo 2021). While libraries are rarely the primary driver behind these initiatives, like any campus unit keen to prove its value, they often succumb to the demand with little or no effective resistance. We will explore narratives of student success and academic integrity in higher education that implicate libraries in increased and un(der)checked surveillance, and which have only intensified during the COVID-19 pandemic.

To be in a state of crisis implies a norm against which the crisis is measured: there is a normal state of things and there is the crisis state, which is an event with a beginning and, conceivably, a definitive end, at which point we will return to that default state of normality. Seeger and Sellnow state that “[c]risis denotes some abnormal event or events that threaten values, goals, and resources. As a consequence, describing an event as a crisis is a rhetorical act that calls for some immediate action to alleviate the potential threat” (2016, 10). Our task during a crisis is to address the things broken by or made visible by the crisis, and to do so with urgency and extreme solutions, all justified under the presumption that the state of crisis is bound to a limited timeframe and will, at some unknown date in the future, be resolved. Things will go back to the deliberately vague normal state, which remains largely nostalgic and nebulously undefined. The factors which contributed to the crisis are examined, but only to the extent that they contribute to the crisis (Roitman 2014).

Within an alleged crisis of academic integrity and student success, the idealized normality may be a time when students didn't struggle to complete their degree, or when cheating and plagiarism were less frequent, or at least more easily identified. For library workers, as articulated within Oakleaf's VAL report it may be a time when libraries were valued by the rest of the academy, when budgets were flush, and we were central to conversations around technology and information on campus (2010). This normality may never have really existed, or may be in reference to a set of conditions, defined through a white cisheteropatriarchal lens that can be seen either as so far from our current reality as to be meaningless, or in desperate need of an overhaul. We see this in higher education, and in academic librarianship, where there are regimes of austerity due to funding crises (Almeida 2020). As public

funding for higher education has shrunk, ballooning student tuition fees have become crucial to most higher education budgets, and expanding the student body to include historically underrepresented communities has increased overall enrollment. Publications and conferences about resilience have become a cottage industry within the field due to the ongoing need and widespread distress caused by the constant pressures presented by these narratives.

If these normal circumstances have never existed, or have never been meaningfully defined, let us consider then that the urgency to solve these crises may be just as fabricated. Crisis, then, might be considered not an event bound in time but a tool, a structure that is a persistent part of the patterns described by Naomi Klein and embodied in the metrics of the VAL report. Because there is presently a tendency to operate within a crisis framework that only envisions what we do not want, our solutions prioritize surveillance and carceral mindsets, or deficit logic (Heinbach et al. 2019), by focusing on the need to identify behaviors that are undesirable. Such logic states that we must identify these behaviors to punish or prevent them, and this identification cannot be accomplished without surveillance. Below, we will further examine how student success and academic integrity exemplify this kind of crisis narrative in higher education as a whole and libraries in particular.

Student Success and Academic Integrity

As we discuss student success here, we understand it as a culmination of measurable and assessable actions, offerings, and resources that provide students with what they need to stay and graduate at a particular institution and enter the next phase of their lives (Magnus *et al.* 2018). Student success becomes an institutional crisis when student needs are not met, causing them to leave the academy. This threatens retention rates and, in turn, funding. Because tuition dollars are fundamental to the existence of colleges and universities, these crises and any actions made in response to them—regardless of how deeply they may appear to be rooted in the interests of individual students and narrowing societal gaps in educational attainment—will always ultimately center the financial interests of an institution or department.

Academic integrity crisis narratives explicitly cast students as potential wrongdoers. This mindset assumes that plagiarism and cheating are widespread and that students must be prevented from engaging in these negative behaviors at all costs. It positions technology as both an enabler to the problem and its potential solution. This crisis narrative is not new—Seeber (2016) notes the calls in the 1980s for the development of “new methods of detecting and preventing academic dishonesty” in response to the “epidemic” caused by the “information explosion,” in this case the invention of the photocopier (Hardy 1981). In the forty years since,

technological capabilities for cheaters and plagiarists and those seeking to catch them have increased exponentially, and has only accelerated during the remote work and education of the COVID-19 lockdowns. Use of third-party software and technology to perform test proctoring, plagiarism detection, writing assessment, and other tasks has expanded (Harwell 2020, Swauger 2020). These student-focused services involve both covert and overt surveillance practices (e.g., biometric recognition and recording students in their home environments) and disproportionately impact students from marginalized and underrepresented communities.

Who Are the Victims of These Purported Crises?

The initial framing of these crises centers on addressing and correcting student experiences—particularly marginalized student experiences—around systemic and institutional failures in order to help them make it through college. However, these surface-level sentiments are quickly bogged down by the financial risks institutions find themselves in if they don't act. This creates a sense of urgency in understanding student needs, leading to initiatives that, following the logic of frameworks like those outlined in the VAL report, leverage a paternalistic view of learning formulated through excessive and intrusive LA data collection that devalues student privacy (Jones et al. 2020; Jones et al. 2019; Ko 2019). The continued collection and access of these data is then used towards understanding and defining the adjustments needed to learning processes and environments (Jones *et al.* 2019). Academic libraries' participation in this cycle has been increasing rapidly in response to “decades' worth of pressure to justify budget expenditures and prove their value” (Jones *et al.* 2019, 263).

By conflating the use of analytics to address and measure student success with the perceived, or desired, value of institutional access and offerings, a dangerous precedent is being set. It is one where we—actors both in and outside of the academic library—begin to misalign “success” with capitalist notions of use and consumption (Farkas 2013; Grande 2018; Magnus *et al.* 2018; Jones *et al.* 2019; Jones *et al.* 2020;). If counting is a way to show success, success becomes defined by what can be counted. It is also one where we participate in the digital instantiation and, thus, commodification of human experience. With crisis surveillance capitalism controlling the means in which we interact with and understand students, our potential to enact further harm is expounded, especially through student success initiatives that target marginalized communities (Magnus *et al.* 2018, SPARC 2021). Specifically, instead of addressing the important needs and concerns of our students, we add more content to their data doubles. Exaggerated further through students' compulsory use of these technologies, students become subjected to systems of

harm and “social control” (Benjamin 2019, 167-168) and their behavior is crystallized, without their knowledge or understanding, in Zuboff’s “shadow text” (2019).

What Is at Risk from the Solutions to These Crises?

Within crisis surveillance capitalism, what is at risk is student privacy. Universities and colleges in Canada and the United States value privacy insofar as their privacy practices meet a minimum requirement determined by governmental decrees (e.g., FERPA and FIPPA). However, following the letter of the law still leaves room for institutions to implement data-focused initiatives such as VAL and Proctorio that endanger student privacy in the name of addressing student success and academic integrity crises.

As institutions posit success through a lens of use and consumption, these data initiatives can include tracking how students interact with campuses and their resources and then assigning that use to traditional markers of success (Robertshaw and Asher 2019). The spread of the COVID-19 pandemic, and the subsequent frantic scramble to convert all instruction to remote study, caused a marked increase in surveillance technology usage to oversee remote students. Throughout 2020 and into 2021, many students have revealed in social media posts how this rushed rollout, and the use of proctoring software specifically, has impacted them in disastrous ways—from darker skinned students not being recognized as being on camera to students having to throw up under the watchful eye of a stranger due to prohibited bathroom breaks (Harwell 2020; Swauger 2020a, 2020b).

The access and use of student information, especially information that has historically been used to perpetuate bias, can be used to further marginalize students. A common example of this, mentioned in the introduction, is collecting and assessing student ID card data from compulsory use to access buildings, attend events, or use institutional materials and property. Kristin Briney (2021) uses this example to narrate how libraries participate in the mishandling of data particularly through re-identification of individuals. This becomes even more nefarious when the data are sourced from predominantly white institutions (PWI) and include non-white participants. Briney notes, “a person’s minority status makes them easier to identify here, especially if they have a non-[w]hite name or do not pass for [w]hite in departmental photos” (Briney 2021).

While academic library workers have a hand in directly establishing practices that contribute to the risks of crisis surveillance capitalism, we also serve as bystanders to the harm being inflicted on students by our campuses and our vendors. This is apparent in our approach to vendors and publishers who knowingly cause harm to users, particularly against Black, Indigenous, and other racialized people, poor people, and people without immigration status. This can present in

three prominent ways, the first being continued subscription to publishers who are known to abuse user data, such as the previously mentioned Thomson Reuters and LexisNexis who provide user data to ICE as part of their surveillance efforts (DiVittorio and Gianelli 2021; Lamdan 2019). The second way is ignoring concerns about and relinquishing control to enhanced surveillance that targets marginalized groups, such as the social database systems discussed in Virginia Eubanks' (2018) *Automating Inequality* and Ruha Benjamin's (2019) *Race After Technology*. The third way is participation in vendor-prescribed security initiatives that center surveillance and user data collection-- for example, the publisher-based conglomerate Scholarly Network Security Initiative (SNSI). Specifically, in a 2020 online seminar, SNSI made reference to utilizing additional "plugins" for proxies to protect publishers' intellectual property—the justification for which uses xenophobic rhetoric (e.g., claiming that SciHub and the like are "foreign actors") as well as targets non-United States countries specifically (DeMarco 2020).

Who Actually Benefits from The Solutions to These Crises?

When library workers act as bystanders, businesses and institutions can employ student success narratives to keep from having to change their practices. For example, they can find new ways to leverage the surveillance and data collection services provided by edtech while remaining within the structures they are legally bound to. Even if institutions recognize issues with invasive surveillance practices, edtech vendors are still able to depend on these narratives by holding that the benefits derived from their use far outweighs the concerns. The Proctorio Team (self-named) explicitly used this justification within an editorial piece for *Inside Higher Ed*:

It may be important to note that there is a potential threat to society when students are not expected to meet integrity standards set forth by their institution. The healthcare setting is a prime example of this. When a healthcare provider is not held to the highest standards of academic integrity, people's lives are at risk. By protecting academic integrity, institutions can rest assured that the value of their degrees, and future patients, are protected (Proctorio Team 2020).

Libraries have experienced and documented this kind of reasoning within their own work as well. Library workers at Auraria Library in Denver, Colorado recently conducted an investigation of vendors' business practices, the results of which hold a candle to the grim realities of crisis surveillance capitalism and who benefits from the narratives of student success and academic integrity crises:

If our library cancelled our Westlaw subscription, this would put our students at a disadvantage and they may not be able to secure employment in the legal field. Our librarians talked with legal and paralegal professors on campus and trialed other products,

but Westlaw is what law firms use. As Lamdan (2019) points out Westlaw and Lexis are the dominant resources used within the legal profession.

It put us in a position of having to support one student group over another. While cancelling Westlaw would be a strong statement of our library's values, it would not change Thomson Reuters' work. (Divittorio and Gianelli 2021)

In the post-9/11 era, many library workers understood that compliance with law enforcement was a direct threat to the precepts of intellectual freedom and right to privacy; extending this to include private vendors of databases and data collection software, and even our own umbrella institutions, has been slower and more challenging. Resisting law enforcement was, perhaps, easier to resist because libraries were not beneficiaries (e.g., the PATRIOT Act in the American context). But in the face of budget cuts and increasing subscription costs and campus partners asking why they must pay for library workers when Google exists, academic libraries stand to gain from these invasions of privacy. As a result, calls for similar resistance have been tempered with more accommodating approaches.

The entire edtech surveillance imagination is taken up with what students could be doing wrong and creating ways to penalize them for it, but there is no vision of what the ideal is. By the time we finish cutting away all of the things that academic integrity is not, and all of the measures used to preemptively preclude behaviors that might possibly lead to violations, students are left to contort themselves into a void that leaves no space to be human. As Zuboff warns, “if you have nothing to hide, you are nothing” (2019, 479). The implications of crisis surveillance capitalism in higher education are very real and affect students in ways we will be coming to terms with long after they leave our institutions; whether they graduate or don't, whether we mean to or not, we are adding to their data doubles. As Virginia Eubanks notes, “[Data freezes] its targets in time, portraying them as aggregates of their most difficult choices” (2018, 195).

Refusing Crisis Surveillance Capitalism and Claiming our Agency

Given the ever-increasing pervasiveness of data collection as described above, resisting surveillance can feel impossible. Eva Galperin (2018) uses the term “privacy nihilist” to describe the sense that privacy is hopeless, given the many compromises to date—since my photo is already online, and facial recognition software is already being used, why bother resisting? In this section, we take a harm reduction approach to crisis surveillance capitalism, rooted in the understanding that it can be difficult to make massive change quickly and that small actions can lessen negative impacts. Even incremental gains in privacy can protect people, and active refusal of crisis narratives helps draw attention to the falsity of those narratives. At the same time, as

we noted in our opening, we recognize that resistance must be sustained over time and is best approached from a broad base rather than atomized to niche issues. While library workers may have effectively resisted library-specific elements of post-9/11 surveillance in the United States, they failed to place this work within a broader struggle to resist the larger, more complex waves of surveillance capitalism; on the contrary, libraries often welcomed these products as part of regimes of assessment and convenience. While the explanations for this failure are beyond the scope of this paper, we seek to explore and encourage resistance at both granular and broad levels.

In considering modes of resistance, we use a framework outlined by Keller Easterling, that we came to know via Baharak Yousefi (2017). Easterling proposes that infrastructure provides the unseen rules that govern what individual actors and organizations do, noting that “what the medium is saying sometimes prevents us from seeing what the medium is doing” (2014, 13). As we have examined in this piece, crisis narratives around student success and academic integrity purport to support students, while also quietly collecting massive amounts of data that can be monetized, in line with surveillance capitalism. More specifically, libraries may operate with stated professional values that support privacy while simultaneously undermining those values through active participation or as bystanders. In an environment where tools increasingly suck up personal data for unknown uses, standing aside is an act of acceptance. In this section, we explore how individual library workers can apply these tactics: on their own, or as part of broader coalition groups, including students, faculty, or other academic workers. Easterling outlines a number of activist practices more adaptive and ambiguous than traditional modes of protest, suited specifically to the ambivalent, ever-shifting extrastate global capitalism she describes, including gossip/rumour and exaggerated compliance. While Yousefi applies these ideas to diversity, equity, and inclusion in libraries, we find them equally suited to crisis surveillance capitalism as we have described it in academic environments. These chaotic, subversive strategies may feed into more traditional modes of resistance, such as boycotts, protests, and legislative responses. We hope library workers see actions they can do right here, right now, and also how to connect into broader networks.

Gossip/Rumour

Gossip and rumour are forms of unofficial, unsanctioned communication, spread through informal networks. As Yousefi notes, “Talking has always been dangerous for those in power” (2017, 98). Gossip, rumour, storytelling, and other ways of creating multiple narratives can destabilize singular corporate narratives supporting surveillance capitalism. Library workers often already depend on word of mouth

for outreach, whether about sharing student resources or building instructional partners.

The lawsuit that Proctorio has filed against UBC instructional designer Ian Linkletter seeks to crack down on exactly this form of resistance. Linkletter, who is trained as a librarian, posted his concerns about the data collected by Proctorio to Twitter, a social media site that serves as a space for gossip, rumor, and other informal information circulation. He included images from Proctorio training documentation. Proctorio then filed a lawsuit, which Linkletter is battling as a Strategic Lawsuit Against Public Participation (SLAPP), an attempt to close off public discourse and free speech.¹ A UBC student who complained about Proctorio on Reddit faced the wrath of the company's CEO, who posted chat logs with the student from the user help desk (Lee 2020). This may have, understandably, created a chilling effect for other students or professionals who might have shared their stories, but far from tamping down critique, it further inflamed public sentiment. The company's attempts to shut down discourse aren't limited to UBC: it has also filed public records requests at public universities, requesting names of people who have filed public records requests related to Proctorio (Johnson 2021). Proctorio also requested the retraction of a critical article by librarian Shea Swauger—which he and the journal editors refused (Swauger 2020).

This kind of push to stifle discourse is not limited to proctoring software companies, of course. In 2017, the Research, Instruction, and Patron Services Special Interest Section (RIPS-SIS) of the American Association of Law Libraries took down a post by Sarah Lamdan and Yasmin Sokkar Harker that criticized LexisNexis's contracts with ICE from their blog, noting "This post has been removed on the advice of AALL General Counsel" (Baker 2017). Regardless of whether LexisNexis directly requested the removal of the post, its takedown demonstrates the chilling effect of an aggressively litigious corporate environment.

At the same time, attempts by corporate actors to silence dissent, or even the raising of questions, indicate the power of these voices. Indeed, we can see the power of gossip and rumor as fuel for more traditional action. Proctorio's lawsuit against Ian Linkletter provided the opportunity for savvy partners to fight back and build a coalition, resulting ultimately in the UBC Faculty Senate effectively prohibiting use of Proctorio on both the Vancouver and Okanagan campuses (Bates 2021; Reddecliff 2021). Student and faculty advocates worked well over a year on this effort, as documented by the student newspaper, *the Ubyssy*. A fall 2020 presentation from the UBC student government in support of their campaign against proctoring software includes student tweets in making the case that "students hate Proctorio" (Yee 2020).

1. Linkletter's legal documents are available at <http://defence.linkletter.org/>

While gossip may result in backlash, it can also share damning information and enable other forms of active resistance.

Library workers can also engage in productive gossip among students and faculty. Public services and liaison library workers often find themselves in between these two user groups: advising faculty with course assignments or practices, but also directly assisting students who navigate those. In both directions, we can share information and strategies. For faculty, this may look like empathizing about the labor involved in changing pedagogical approaches, then brainstorming alternative tools or at least advocating for greater transparency to learners. For students, this may look like recommendations for how to confront an instructor about overly invasive practices or requirements and sharing networks of concerned students. Given the relational work so many of us do, gossip is a natural fit. We can also draw attention to worthy gossip as it circulates in other venues—for example, sharing with faculty the numerous student complaints about proctoring software being posted to social media, such as those collected by the @Procteario account on Twitter.

Two examples demonstrate how library workers may use gossip effectively. Dorothea Salo recently used public records law to request circulation data from the library where she works, which she then posted via OSF; she has written about this in several blog posts (2021). This was an opportunity both to teach graduate students about public records requests alongside privacy, and to draw attention to troubling—but hardly uncommon—records retention schedules that required the long-term persistence of circulation data. Next, while faculty at CUNY were ultimately unsuccessful in stopping the Turnitin contract discussed above, a group including librarians used a petition campaign to demonstrate faculty resistance, ultimately presenting the results to the Board of Trustees (Walzer *et al.* 2020). Regardless of its impact on decision-makers, a petition is a way to share information and shape perspectives. We can imagine that the more than 1000 faculty who signed the petition will, at the very least, refuse to use Turnitin in their own courses, and may be able to advocate against it more broadly in their academic units.

Gossip and rumour of course require information, as well as people to share it with. For library workers who feel alone in their concerns, they can connect to communities through organizations like the [Library Freedom Project](#), which trains privacy advocates, or the [Digital Library Federation's Privacy and Ethics in Technology](#) working group.

Exaggerated Compliance

Exaggerated compliance means taking requirements or expectations to an extreme, often with a sense of playfulness or redirection of official narratives. By purposefully

not breaking the rules, you can draw attention to how unjust those rules are. In the context of post-9/11 library worker resistance, a warrant canary demonstrates exaggerated compliance. In 2005, librarian Jessamyn West put a sign out on the reference desk at her public library noting that “The FBI has not been here. Watch for the removal of this sign” (West 2005). In drawing attention to the potential for secret searches of library user data by federal law enforcement, the sign also highlights how outrageous such legislation is. The removal of the sign will then indicate to attentive users that the library has been forced to provide user data accordingly.

Warrant canaries continue to be used in online settings as a way to technically follow the rules while also drawing attention to how wrong those rules are. One notable example is the warrant canary of the Riseup Collective, which provides communication tools for social change. When their canary statement was not updated on its regular schedule in 2016, users and broader activist groups grew concerned that the Riseup Collective had been compromised by government law enforcement; indeed, the Collective later posted that they had chosen to comply with warrants from the FBI in two cases (Riseup Collective 2017). As this story demonstrates, warrant canaries are not necessarily an effective way to prevent government requests for data; however, they can be very effective at drawing attention to the potential for such acts.

Within academic surveillance, similar acts of exaggerated compliance can help draw attention to the absurd or infuriating rules. This can be done at an individual level, for example in a one-shot guest lecture, or at a collective level, in a statement or in repeated boilerplate on the library website. What would it be like if we truly asked students to review the terms of service for each proprietary tool we encourage them to use? Librarians at Cornell University have explored the possibility of incorporating information about data privacy practices of e-resources into the process of logging in to view them (McCracken 2020), something like the [Terms of Service Didn't Read](#) built into their proxy tool. Of course, this would add another step to the process, but it may also raise questions of why the library subscribes to proprietary tools with such invasive data privacy practices. While we often focus on seamlessness in helping users access information, exaggerated compliance requires that we slow down and draw attention to what is at stake.

Vendor negotiations offer another opportunity for exaggerated compliance. Given that colleges and universities often have complicated requirements for licensing, there may be opportunities to incorporate new requirements into that process. As noted in the example from Auraria Library above, this can be difficult—but even in those discouraging moments, there can be opportunities to draw attention to the troubling crisis narratives, and the harmful implications of their so-called solutions.

The Vendor Privacy Scorecard from Library Freedom Project cleverly uses the NISO *Consensus Principles on User's Digital Privacy in Library, Publisher, and Software-Provider Systems* to evaluate popular library database vendors (Library Freedom Project n.d.). Appeals to this kind of guideline make it easier to make the case for adding privacy requirements to licensing requirements to compliance-minded administrators.

A perhaps more fruitful opportunity rising out of exaggerated compliance is in applying pressure to shared governance structures. At many institutions of higher education, the faculty senate supposedly holds power over curricular matters. However, edtech contracts are typically completed by administrative units, often without direct involvement by faculty. Demands by faculty senate to have final say over edtech licensing, or as in the UBC example noted above, to reactively ban particular tools, could be a powerful way to bring scrutiny to the ways these tools are brought to campus, if not to effectively end their use (Chin 2021). Similar resolutions have been implemented at San Francisco State University (2020) and are under consideration at the University of Denver (SPARC 2021).

Conclusion

Crisis surveillance capitalism continues to morph and adapt. Even in the months since we started writing, some universities have begun to suspend proctoring software, and additional information has come out about the practices of Lexis-Nexis/Thomson Reuters. As vaccine rollout continues and institutions begin to promote a so-called return to normal, our exploration of crisis narratives reminds us that “normal” may in fact never have existed, or may have directly contradicted our stated professional values. Academic library workers can continue to use tactics such as rumour/gossip and exaggerated compliance to question, resist, and subvert academic surveillance—whatever the next crisis turns out to be.

ABOUT THE AUTHORS

All authors contributed equally to the writing and revision of this article. The order of authors is alphabetical.

Callan Bignoli is the Director of the Library at Olin College of Engineering in Needham, Massachusetts. She studies and speaks about user experience design, library management, and the social impacts of technology. Callan joined the Library Freedom Project in 2020.

Sam Buechler is the Student Success Library Faculty Resident at Washington State University Vancouver. Their research interests include privacy and surveillance on college campuses, academic library outreach, and critical information literacy. They have been a member of the Library Freedom Project since 2020. (Contact: sam.buechler@wsu.edu)

Deborah Yun Caldwell was the 2018-2021 Diversity Resident Librarian at the University of North Carolina at Greensboro. She serves on the steering committee for the PEGI Project, advocating to ensure access to public government information. Her work explores the intersections of digital

preservation, information stewardship, cultural memory, and the justice of information access. She has been a member of the Library Freedom Project since 2020.

Kelly McElroy is an Associate Professor and outreach librarian at Oregon State University. She has been a member of the Library Freedom Project since 2018.

REFERENCES

- Academic Senate, San Francisco State University. September, 2020. "Resolution on Third Party Proctoring." Accessed August 31, 2021. <https://senate.sfsu.edu/resolution/resolution-third-party-proctoring>.
- Adams, Susan. 2021. "This \$12 Billion Company Is Getting Rich Off Students Cheating Their Way Through Covid." *Forbes*. January 28, 2021. <https://www.forbes.com/sites/susanadams/2021/01/28/this-12-billion-company-is-getting-rich-off-students-cheating-their-way-through-covid/>
- Alden, Charlotte, and Andrew Ha. 2020. "Proctorio Sues UBC Staff Member for Tweets Sharing 'Confidential' Information about the Software." *The Ubyyssey*, September 3, 2020. <https://www.ubyssey.ca/news/proctorio-sues-linkletter/>.
- Almeida, Nora. 2020. "The Labour of Austerity: Absurdity, Performative Resistance, and Cultural Transformation." *Canadian Journal of Academic Librarianship* 6: 1–25. <https://doi.org/10.33137/cjal-rcbu.v6.34008>.
- American Library Association. 2006. Library Bill of Rights. <http://www.ala.org/advocacy/intfreedom/librarybill>
- American Library Association. 2017a. Code of Ethics of the American Library Association. <http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/proethics/codeofethics/Code%20of%20Ethics%20of%20the%20American%20Library%20Association.pdf>
- American Library Association. 2017b. Privacy and Confidentiality: Library Core Values. <https://www.ala.org/advocacy/privacy/toolkit/corevalues>
- Benjamin, Ruha. 2019. *Race After Technology: Abolitionist Tools for the New Jim Code*. Cambridge: Polity.
- Biddle, Sam. 2021. "LexisNexis to Provide Giant Database of Personal Information to ICE." *The Intercept*, April 2, 2021. <https://theintercept.com/2021/04/02/ice-database-surveillance-lexisnexis/>
- Briney, Kristin A. 2021. "Citation Omitted: A Story of Re-identification." *Data Ab Initio*, April 1, 2021. <http://dataabinitio.com/?p=1012>
- Buolamwini, Joy, and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." In *Conference on Fairness, Accountability and Transparency*, 77–91. PMLR. <http://proceedings.mlr.press/v81/buolamwini18a.html>.
- Canadian Radio-television and Telecommunications Commission (CRTC). 2021. "Broadband Fund: Closing the Digital Divide in Canada." March 19, 2021. <https://crtc.gc.ca/eng/internet/internet.htm>
- Chin, Monica. 2021. "University will stop using controversial remote-testing software following student outcry." *The Verge*, January 29, 2021. <https://www.theverge.com/2021/1/28/22254631/university-of-illinois-urbana-champaign-proctorio-online-test-proctoring-privacy>
- DeMarco, Joseph. "Foreign Interference in Academia." Presentation at Cybersecurity Landscape - Protecting the Scholarly Infrastructure, Online, October 22, 2020. <https://www.snsi.info/news-and-events/cybersecurity-landscape/&sa=D&source=editors&ust=1618425147113000&usg=AOvVaw3P-u-yJymnZI4WWoeXdCsK>.
- DiVittorio, Katy and Lorelle Gianelli. 2021. "Ethical Financial Stewardship: One Library's Examination of Vendors' Business Practices." *In the Library With the Lead Pipe*. <http://www.inthelibrarywiththeleadpipe.org/2021/ethical-financial-stewardship/>
- Drabinski, Emily. 2006. "Librarians and the Patriot Act." *Radical Teacher*, 77: 12–14. <http://www.emilydrabinski.com/wp-content/uploads/2012/06/PatriotAct.pdf>

- Easterling, Keller. 2014. *Extrastatecraft: The Power of Infrastructure Space*. Verso Books.
- Estabrook, Leigh S. 2003. "Public Libraries and Civil Liberties: A Profession Divided." https://web.archive.org/web/20030201222005/http://alexia.lis.uiuc.edu/gslis/research/civil_liberties.html
- Farkas, Meredith. 2013. "Accountability vs. Improvement: Seeking Balance in the Value of Academic Libraries Initiative." *OLA Quarterly*, 19(1): 4-7. <http://archives.pdx.edu/ds/psu/9598>.
- Feldstein, Michael. 2021. "The Chegg Situation is Worse Than You Think." February 6, 2021. <https://eliterate.us/the-chegg-situation-is-worse-than-you-think/>
- Future Ready. 2021. "Students of Color Caught in the Homework Gap." <https://futureready.org/homework-gap/#facts>
- Galperin, Eva. Class lecture to Library Freedom Institute, Zoom, 3 July 2018.
- Grande, Sandy. 2018. "Refusing the University." In *Toward What Justice?: Describing Diverse Dreams of Justice in Education*, edited by Tuck Eve and K. Wayne Yang. New York: Routledge.
- Hardy, Richard J. 1982. "Preventing Academic Dishonesty: Some Important Tips for Political Science Professors." *Teaching Political Science* 9, no.2): 68–77. <https://doi.org/10.1080/00922013.1982.9942904>
- Hanson, Cody. 2019. "User Tracking on Academic Publisher Platforms." *Cody Hanson* (blog). April 2019. <https://www.codyh.com/writing/tracking.html>
- Harwell, Drew. 2020. "Mass School Closures in the Wake of the Coronavirus Are Driving a New Wave of Student Surveillance." *The Washington Post*, April 1, 2020, sec. Technology. <https://www.washingtonpost.com/technology/2020/04/01/online-proctoring-college-exams-coronavirus/>
- Heinbach, Chelsea, Brittany Paloma Fiedler, Rosan Mitola, and Emily Pattni. 2019. "Dismantling Deficit Thinking: A Strengths-based Inquiry Into The Experiences Of Transfer Students In And Out Of Academic Libraries." *In the Library with the Lead Pipe*. <http://www.inthelibrarywiththeleadpipe.org/2019/dismantling-deficit-thinking/>
- Jones, Kyle M. L. 2018. "What is a Data Double?" *Data Doubles*. May 1, 2018. <https://datadoubles.org/2018/05/01/what-is-a-data-double/>
- Jones, Kyle M. L., Andrew Asher, Abigail Goban, Michael R. Perry, Dorothea Salo, Kristin A. Briney, and M. Brooke Robertshaw. 2020. "'We're Being Tracked at All Times': Student Perspectives of Their Privacy in Relation to Learning Analytics in Higher Education." *Journal of the Association for Information Science and Technology* 71, no.9): 1044-59. <https://doi.org/10.1002/asi.24358>
- Jones, Kyle M. L., Michael R. Perry, Abigail Goban, Andrew Asher, Kristin A. Briney, M. Brooke Robertshaw, and Dorothea Salo. 2019. "In Their Own Words: Student Perspectives on Privacy and Library Participation in Learning Analytics Initiatives." *Proceedings of the Annual Meeting of the Association of College & Research Libraries*. <https://www.ala.org/acrl/sites/ala.org/acrl/files/content/conferences/confsandpreconfs/2019/InTheirOwnWords.pdf>
- Kaba, Mariame. 2021. *We Do This 'Til We Free Us*. Chicago, IL: Haymarket Books.
- Ko, Amy J. 2019. "Teaching, Power, Consent, and Paternalism." *Medium*, July 31, 2020, sec. Bits and Behavior. <https://medium.com/bits-and-behavior/teaching-power-consent-and-paternalism-b9c226152caa>
- Klein, Naomi. 2007. *The Shock Doctrine: The Rise of Disaster Capitalism*. New York: Metropolitan Books/Henry Holt.
- . 2020. "Screen New Deal: Under Cover of Mass Death, Andrew Cuomo Calls in the Billionaires to Build a High-Tech Dystopia." *The Intercept*, May 8, 2020. <https://theintercept.com/2020/05/08/andrew-cuomo-eric-schmidt-coronavirus-tech-shock-doctrine/>
- Lamdan, Sarah. 2019. "Librarianship at the Crossroads of ICE Surveillance." *In the Library with the Lead Pipe*. <http://www.inthelibrarywiththeleadpipe.org/2019/ice-surveillance/>

- Lee, Shereen. 2020. "Proctorio CEO Releases Student's Chat Logs, Sparking Renewed Privacy Concerns." *The Ubysey*, June 30, 2020. <https://www.ubyssey.ca/news/proctorio-chat-logs/>
- Library Freedom Project. n.d. "Vendor Privacy Scorecard." Accessed April 18, 2021. <https://libraryfreedom.org/wp-content/uploads/2021/03/Library-Freedom-Vendor-Scorecard-110719.pdf>
- Magnus, Ebony, Jackie Belanger, and Maggie Faber. 2018. "Towards a Critical Assessment Practice." *In the Library with the Lead Pipe*. <http://www.inthelibrarywiththeleadpipe.org/2018/towards-critical-assessment-practice/>
- McCracken, Peter. "Data Abuse: Is There a Sustainable Solution to Help Notify Users of Egregious Data Abuses?" Presentation, American Library Association Midwinter Meeting, Philadelphia PA, 26 January 2020.
- Morozov, Evgeny. 2013. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs.
- Noble, Safiya Umoja. 2012. "Searching for Black Girls: Old Traditions in New Media." PhD diss., University of Illinois Urbana-Champaign. <http://hdl.handle.net/2142/42315>
- . 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: University Press.
- Patil, Anushka, and Jonah Engel Bromwich. 2020. "How It Feels When Software Watches You Take Tests." *The New York Times*, September 29, 2020, sec. Style. <https://www.nytimes.com/2020/09/29/style/testing-schools-proctorio.html>
- Proctorio Team, The. 2020. "Response From Proctorio." *Inside Higher Ed*. Last updated April 30, 2020. <https://www.insidehighered.com/blogs/university-venus/response-proctorio>
- Public Books (podcast). 2020. "Episode 3: Societies Online" (with Alice Marwick). August 3, 2020. <https://www.publicbooks.org/episode-3-societies-online/>
- Riseup Collective. 2017. "Riseup Moves to Encrypted Email in Response to Legal Requests." Riseup.Net. February 16, 2017. <https://riseup.net/en/about-us/press/canary-statement>
- Rocher, Luc, Julien M. Hendrickx, and Yves-Alexandre de Montjoye. 2019. "Estimating the Success of Re-identifications in Incomplete Datasets using Generative Models." *Nature Communications*, 10, no. 3069. <https://www.nature.com/articles/s41467-019-10933-3>
- Roitman, Janet L. 2014. *Anti-Crisis*. Durham, NC: Duke University Press.
- Salo, Dorothea. 2021. "Public-Records Requesting My Own Library Records." June 1, 2021. <https://dsalo.info/public-records-requesting-my-own-library-records/>
- Seeber, Kevin. 2016. "The Failed Pedagogy of Punishment: Moving Discussions of Plagiarism Beyond Detection and Discipline." In *Critical Library Pedagogy Handbook Volume 1*, edited by Nicole Pagowsky and Kelly McElroy, 131-138. Chicago: ACRL.
- Seeger, Matthew, and Timothy L. Sellnow. 2016. *Narratives of Crisis: Telling Stories of Ruin and Renewal*. Palo Alto, CA: Stanford University Press.
- Soria, Krista M., Jan Fransen, and Shane Nackerud. 2017. "The Impact of Academic Library Resources on Undergraduates' Degree Completion." *College & Research Libraries*, 78, no. 6: 812-23. <https://doi.org/10.5860/crl.78.6.812>
- SPARC. 2021. "Higher Education Reckons with Concerns Over Online Proctoring and Harm to Students." August 27, 2021. <https://sparcopen.org/news/2021/higher-education-reckons-with-concerns-over-online-proctoring-and-harm-to-students/>
- Stewart, Briar. 2020. "How COVID-19 Worsens Canada's Digital Divide." *CBC News*. September 23, 2020. <https://www.cbc.ca/news/canada/british-columbia/covid-19-highlights-urban-rural-digital-divide-1.5734167>

- Swauger, Shea. 2020a. "Our Bodies Encoded: Algorithmic Test Proctoring in Higher Education." *Hybrid Pedagogy*, April. <https://hybridpedagogy.org/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/>
- . 2020b. "Software That Monitors Students During Tests Perpetuates Inequality and Violates Their Privacy." *MIT Technology Review*, August. <https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/>
- Waltzer, Luke, Lisa Rhody, and Roxane Shirazi. 2020. "Testimony to the CUNY Board of Trustees in Opposition to the Resolution to Approve a Contract with Turnitin for Plagiarism Detection Software, December 14th, 2020 Meeting." CUNY Academic Works, https://academicworks.cuny.edu/gc_pubs/670/
- West, Jessamyn. 2005. *The FBI Has Not Been Here*. Photo. <https://www.flickr.com/photos/iamthebestartist/16173093/>
- Yee, Georgia. 2020. "A Call to Action Against the Usage of Proctorio." Accessed April 8, 2021. <https://www.ams.ubc.ca/wp-content/uploads/2020/10/214-21-A-Call-to-Action-Against-the-Usage-of-Proctorio.pdf>
- Yousefi, Baharak. 2017. "On the Disparity Between What We Say and What We Do in Libraries." In *Feminists Among Us: Resistance and Advocacy in Library Leadership*, edited by Shirley Lew and Baharak Yousefi, 91-105. Sacramento, CA: Library Juice.
- Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs.