

# Teaching in Higher Education

## Critical Perspectives

ISSN: 1356-2517 (Print) 1470-1294 (Online) Journal homepage: <https://www.tandfonline.com/loi/cthe20>

# The case of Canvas: Longitudinal datafication through learning management systems

Roxana Marachi & Lawrence Quill

To cite this article: Roxana Marachi & Lawrence Quill (2020) The case of Canvas: Longitudinal datafication through learning management systems, *Teaching in Higher Education*, 25:4, 418-434, DOI: [10.1080/13562517.2020.1739641](https://doi.org/10.1080/13562517.2020.1739641)

To link to this article: <https://doi.org/10.1080/13562517.2020.1739641>



Published online: 29 Apr 2020.



Submit your article to this journal [↗](#)



Article views: 111



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)



# The case of Canvas: Longitudinal datafication through learning management systems

Roxana Marachi<sup>a</sup> and Lawrence Quill <sup>b</sup>

<sup>a</sup>Department of Teacher Education, San José State University, San José, CA, USA; <sup>b</sup>Department of Political Science, San José State University, San José, CA, USA

## ABSTRACT

The Canvas Learning Management System (LMS) is used in thousands of universities across the United States and internationally, with a strong and growing presence in K-12 and higher education markets. Analyzing the development of the Canvas LMS, we examine 1) ‘frictionless’ data transitions that bridge K12, higher education, and workforce data 2) integration of third party applications and interoperability or data-sharing across platforms 3) privacy and security vulnerabilities, and 4) predictive analytics and dataveillance. We conclude that institutions of higher education are currently ill-equipped to protect students and faculty required to use the Canvas Instructure LMS from data harvesting or exploitation. We challenge inevitability narratives and call for greater public awareness concerning the use of predictive analytics, impacts of algorithmic bias, need for algorithmic transparency, and enactment of ethical and legal protections for users who are required to use such software platforms.

## ARTICLE HISTORY

Received 31 July 2019  
Accepted 4 March 2020

## KEYWORDS

Data ethics; data privacy;  
predictive analytics; higher  
education; dataveillance

## Introduction

The Canvas Learning Management System (LMS) is used in thousands of universities across the United States and internationally, with a strong and growing presence in the K-12 and higher education markets. Massive amounts of data are gathered continuously on students and faculty often without their awareness or consent. On a regular basis, changes are made to platform design features and analytics without formal announcement or notification.

This paper examines the datafication of higher education through the Canvas LMS. While there is growing interest in educational data-mining in K-12 environments (see Manolev, Sullivan, and Slee 2018) relatively little has been written about the growing markets for parallel and connected technologies across and beyond early learning, K12, and higher education sectors. With markets currently steeped in artificial intelligence and attempts at predictive modeling, longitudinal datasets are an increasingly valuable commodity and ripe for extraction by private companies.

Analyzing the development of the Canvas LMS we examine 1) ‘frictionless’ data transitions that bridge pre-K, K12, higher education, and workforce data 2) the integration of connected third party applications within the LMS, and interoperability or data-sharing

across these applications 3) privacy and security vulnerabilities, and 4) predictive analytics and dataveillance.

We conclude that institutions of higher education are currently ill-equipped to protect students and faculty required to use the Canvas Instructure LMS from data harvesting or exploitation. We challenge inevitability narratives for blind adoptions of such systems and call for greater public awareness among members of college and university communities concerning the use of predictive behavioral and learning analytics, the impact of algorithmic bias, the need for algorithmic transparency, and enactment of both ethical and legal protections for users who are required to use such software platforms in educational settings.

We situate our own discussion between the ongoing debate within the educational technology sector as it attempts to apply its business models to public higher education, the economic advantages afforded to (often cash-strapped) public institutions of higher education, which seek to promote online courses and degrees while simultaneously encouraging faculty to switch to the new platform, and those academic sectors that embrace educational technology and seek to promote its use often for ideological purposes (Apple 2004, 2005, 2007; Boggs and Van Baalen-Wood 2018; Fathema, Shannon, and Ross 2015). We also refer frequently to San José State University, our home institution, as a prime example of a university that finds itself caught between the competing and often conflicting demands of legislators, educational administrators, faculty, parents, and students.

## A brief history of Canvas

The rise of the Internet has fundamentally altered teaching and learning. The possibility of providing online content directly to students of higher education has opened up vast markets for professional certificates, executive education, and degrees beyond the kinds that have historically been granted at colleges and universities. Proponents of Educational Data Management (EDM) claim that it enables real-time assessment of students and materials, and allows institutions to assess the effectiveness of learning strategies, which, in some instances might extend to physically tracking students (through the use of RFID tags in student IDs) and analysing social networks, thereby adapting content to support individuated learning. Using these data to assist in instruction, advising, and resource allocation within institutions is now commonplace (Rubel and Jones 2016).

Initially adopted by the Utah Education Network, Canvas by Instructure is now the most widely used LMS provider in the United States and Canada and is only third to Google and Microsoft in the amount of student data amassed (Menard 2019). It can count not just K-12 schools, colleges and universities among its clients but also high-profile corporations like Cisco, which teamed up with Canvas in 2012 for integration into its Cisco Networking Academy with over one million students worldwide. In fact, Canvas' reach is truly global with an increasing focus since 2013 upon new educational markets in Central and South America, Africa, Europe, and Asia (see Hill 2017).

Started in Utah by two graduate students who designed a Learning Management System as a class project, Canvas' approach was significantly different from that undertaken by early advocates of educational software. Instead of designing a complete system for a single institution and adapting the technology for subsequent clients, the open source approach developed by Canvas offered a suite of services according to need along with a number of third-party applications offered free of charge.

As market observers noted, 2011 marked a significant shift away from ‘academically-facing’ software systems that were hosted on site to cloud based solutions that offered Software as a Service (SaaS). SaaS platforms were considerably cheaper and less complex than one size fits all programs epitomized by learning platforms like Blackboard, which dominated the LMS market from 2004–2011. Early market dominance was assured by Blackboard’s acquisition of competitors like WebCT and Angel. But after 2009, the open source model of software, a growing familiarity with social networking platforms among potential consumers, combined with significant investment from Venture Capital in cloud-based solutions resulted in the entrance of new competitors into the market. Canvas’ parent company, *Instructure*, became a leading disruptor in the field of educational technology. A majority of public colleges and universities in the United States that offer online courses rely upon external companies like Instructure to provide course design and ongoing support; ‘supplying the online platform through which university affiliates interact with students to all-inclusive distance-learning programs rebranded under the institution’s name, and everything in-between’ (Mattes 2017, 2).

As Hill (2011) noted, (SaaS) models offered advantages over on-site LMS platforms, namely, the ability to mine and report data, and to use the latter to support outcomes-based (rather than enrollment-based) funding models for public institutions.

### Canvas in higher education

In 2012, SJSU switched to Canvas’ cloud-based LMS, joining almost three hundred other college campuses in the United States. After an almost year long process involving thirty-six faculty and technical staff, the LMS Advisory Committee recommended Canvas as the LMS of choice. It was also a good deal more cost effective than Desire2Learn in 2012 which cost the university \$361,198 in 2012 compared to \$216,178 for Canvas in 2014.

The most recent statistics available for Canvas usage at San José State University are from 2018. During the two-week Winter Intersession, 106 Canvas courses were offered on Instructure; 3692 courses were provided in Spring, 444 in Summer, and 4,057 in Fall 2018. This represents a gradual increase in adoption from the previous year. In addition, in Fall 2018, a Canvas User Satisfaction survey (4278 participants) noted the following: 32.9% of students use Canvas through their smartphones and 45.4% through a laptop, and a majority (>60%) report satisfaction with the LMS.

The following sections unpack a set of interrelated concerns for consideration by members of both K12 and higher education communities that have adopted or that require employees and/or students to use Instructure’s Learning Management System.

### Frictionless learning

Instructure’s cloud-based products extend from the K-12 market, to college, and beyond through employee development programs offered through its Bridge software used by corporations and public institutions for training purposes. According to its website, Instructure ‘has connected millions of instructors and learners at more than 4,000 educational institutions and corporations throughout the world’ and is ‘the world’s fastest growing learning platform for K-12 and higher ed,’ a feat made possible, in part, through its reliance on Amazon Web Services for data storage and scalability.

According to Billings (Amazon Web Services 2015), in early 2015, Instructure adopted AWS analytic tools as a key feature that allowed Instructure to be ‘creative in a very “frictionless” way.’

The absence of ‘friction’, as described in an introductory AWS-Instructure partnership video is important to highlight, as scholars of emerging technologies have called for more focused and critical analyses of such practices. Gilliard (2018) uses the term explicitly in an essay titled ‘Friction-Free Racism’ referring specifically to platforms that ascribe identity through data,

The ability to define one’s self and tell one’s own stories is central to being human and how one relates to others; platforms’ ascribing identity through data undermines both. These code-derived identities in turn complement Silicon Valley’s pursuit of ‘friction-free’ interactions, interfaces, and applications in which a user doesn’t have to talk to people, listen to them, engage with them, or even see them. From this point of view, personal interactions are not vital but inherently messy, and presupposed difference (in terms of race, class, and ethnicity) is held responsible. Platforms then promise to manage the ‘messiness’ of relationships by reducing them to transactions. The apps and interfaces create an environment where interactions can happen without people having to make any effort to understand or know each other. (Gilliard 2018)

Instructure highlights many features of its system across both K12 and higher ed sectors prominently in online marketing materials. While it is unknown without thorough analysis if the designs embedded within the LMS are subject to equity blind spots, one could argue that the root structures of mass data extraction and analytic use across applications are tools of digital exploitation, and thus aligned with critiques espoused by Benjamin (2019) and Gilliard (2018).

Some of the tools promoted by Instructure as *Canvas Features* (2019) include quiz statistics, on-the-spot assessments using mobile devices, polling, IOS and Android app integrations, notifications connected to email, text, and/or social media accounts, audio and video recording and transfer, learning object repositories, capacity to download and upload files, Learning Tool Integrations (LTI), open APIs which would allow ‘talking’ with other software programs, web conferencing, and customizable profile pages that encourage students to share personal information about themselves (Instructure 2019). While many of these tools are assumed to facilitate learning, some may not be accessible to all students or may fail to take into account external challenges that students may be experiencing that could lead to inequitable and/or incorrect conclusions being made about their course engagement and/or learning. Madden and colleagues (2017) highlight privacy, poverty, and big data as a ‘matrix of vulnerabilities’ that converge in ways that exacerbate data harms likely to be experienced by members of under-resourced communities.

Many educators would agree that community building and the sharing of personal stories can be powerful ways to strengthen collaborative learning. Users of the Canvas LMS are not, however, sharing personal details with one another in a closed classroom environment. Rather, they are sharing them directly into Amazon Web Services servers, and potentially a host of third party applications and clients that are also connected to the Instructure LMS.

Recognizing the potential for abuse resulting from predictive analytics more broadly, Crawford and Schultz (2014) describe the need for a framework to redress predictive privacy harms that can emerge from the inappropriate inclusion and predictive analysis of an individual’s personal data without their knowledge or express consent. They note that poor execution of Big Data methodology may create additional harms by rendering

inaccurate profiles that impact an individual's life and livelihood and further highlight the expansion of the range of data that can be personally identifying,

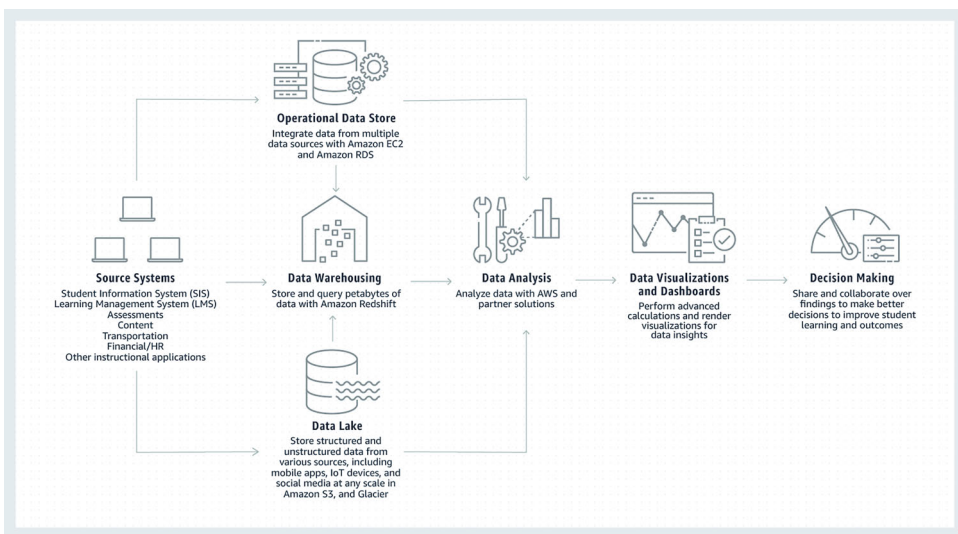
By primarily analyzing metadata, such as a set of predictive and aggregated findings, or by combining previously discrete data sets, Big Data approaches are not only able to manufacture novel PII, but often do so outside the purview of current privacy protections. Existing regulatory schema appear incapable of keeping pace with these advancing business norms and practices. (94)

The next section describes key structures and processes by which data are collected and used within Canvas for the kinds of predictive harms described by Crawford and Schultz (2014).

## Interoperability from K-12 to higher education

The determination to provide a 'frictionless' or 'seamless' user experience is supported by the notion of interoperability, a term rooted in military weapons systems development and the ability to share information between systems (Department of Defense 2020). Introduced by Instructure in 2013, interoperability was made possible through Canvas' Open Apps site, effectively an app library built around Canvas which allows administrators, teachers, and students to install third party apps in the LMS. To date, 370 apps are available from third-party providers including access to content providers such as the Khan Academy, video conferencing programs such as Zoom, note taking applications like Evernote, and apps like ASPIR-EEDU which monitors the performance of instructors ('overall log-in time' through Canvas, 'timeliness of grading', 'snippets of grading feedback and other performance data').

Given Canvas' longitudinal reach with capacity to harvest data from multiple levels of school systems that sign on to the LMS, we explored AWS documents indicating how data are shared. Amazon Web Services' description of K12 and primary education tools indicates that by 'using the AWS Cloud, schools and districts can get a comprehensive picture of student performance by connecting products and services **so they seamlessly share data across platforms**' [Emphasis added].



‘Putting Data To Work For Students’ <https://aws.amazon.com/education/K12-primary-ed/>.

Several hundred educational technology companies also partner with Amazon Web Services through a program called *EdStart* whereby cloud data storage services and resources are provided by Amazon to entrepreneurs with educational technology software products.

Given extensive reporting on the vast, burgeoning markets for integrated data (Christl 2017; Russell et al. 2018), it is unclear which data collected by the AWS EdStart members would be protected from subsequent matching or inclusion into big data predictive analytics. AWS EdStart has a broad global reach with 48 edtech partner companies based in Europe, the Middle East and Africa, and 116 companies based in the Asia-Pacific region for a total of 316 edtech members overall within its data network. While promises may be made of compliance with COPPA/FERPA data privacy laws, once data are collected and/or combined across international borders, companies would not necessarily be required to abide by laws from the host country where data were gathered. These cross-border data flows could theoretically be stored into international servers capable of transfer, and/or sale without oversight or scrutiny.

One of the key advantages of open source software, according to Instructure, is the ability this gives to students, teachers, and administrators to use apps provided by third-party affiliates. Conveniently, such a structure also funnels a massive amount of data to Instructure datasets. Ease of data sharing is featured prominently in Bridge’s materials promoting ‘Learning and performance in a single, pain-free experience.’ Focusing on the cumbersome and delaying nature of needing to enter systems through multiple logins, Bridge highlights the ease of data access:

The last thing you want is for your people to have to log in and out of separate systems and platforms. Bridge allows you to seamlessly access everything within a single platform for a cohesive experience. (Instructure Bridge [video], 2019)

In recent years, universities have also begun integrating student evaluations of instructors into their menu of third-party apps accessible through Canvas. *CoursEval*, a program managed by *CampusLabs* is an external course evaluation app integrated into San José State University’s Canvas Instructure LMS. Course evaluation procedures that previously involved sealed envelopes, campus mailboxes, and confidentiality provisions that wouldn’t allow for the removal of faculty dossiers from department offices, have now been transferred to online spaces with data that appear open to analysis by third-party entities and by cloud hosting LMS and AWS data servers. The Canvas Data tool documents a parsing and aggregation of more than 280 million rows of Canvas usage data daily (Instructure 2020).

It is unclear what access is given to whom to engage in the analytics described. If instructors are the only ones with access to their student data, as FERPA would suggest, they would not be the ones to analyze the 280 million rows of Canvas usage data generated daily. If administrators or other data analysts are accessing student/and or faculty data, they would be doing so without knowledge or consent of users, most of whom are given the impression that the LMS is protecting their data from outside use.

Notions of data-sharing are also subject to different interpretations depending on perspective and context. As Benjamin observes,

Data sharing, for instance, sounds like a positive development, streamlining the bulky bureaucracies of government so the public can access goods and services faster. But access goes both ways. If someone is marked ‘risky’ in one arena, that stigma follows him around much more efficiently, streamlining marginalization. (2019, 13)

At the time of the writing of this manuscript, Instructure is in the midst of being purchased by a private investment equity firm, Thoma Bravo, for an estimated two billion dollars. In the span of one week in February 2020, the Instructure board voted against the sale, Dan Goldsmith indicated intent to step down as CEO (with no indication of a successor), and edtech investment analysts have described what will still be an eventual company purchase as a ‘takeover’ (Deveau 2020; Hill 2020). What remains unclear is the fate of the student and faculty data as a result of this pending purchase or any other. Data privacy concerns and questions related to the Instructure acquisition have been outlined in a public letter co-signed by dozens of individuals working at colleges and universities that use the Canvas LMS (Young 2020). The letter references legal scholars who have noted the vulnerability of student data to exploitation in private markets. Russell et al. (2018) have written about the commercial availability of student lists for purchase ‘on the basis of ethnicity, affluence, religion, lifestyle, awkwardness, and even a perceived or predicted need for family planning services’ (i). With no federal privacy laws governing student data brokers, student data can be collected, sold, and bought without any apparent legal protections from widespread exploitation.

### Privacy and security vulnerabilities

According to the Instructure website, the Canvas platform allows for third parties to test its software for vulnerabilities. To that end, Instructure runs open security audits on Canvas with the results published annually. The flip side of this, however, is that the use of third-party affiliates often leaves institution IT departments in a peculiar position. Do they bear the responsibility to effectively monitor the educational data that is collected by third-party affiliates? Official statements from Instructure seem to suggest otherwise. In an interview in 2013, an official for Instructure noted the following: ‘Third party integrations have existed, but they’ve required the IT department to make them work. With Canvas App Center, we want to let anyone install an app with one click and begin personalizing their learning experience with these tools’ (Cited in Empson 2013).

What these third parties do with student information is, of course, the question. The foundation of the open-source business model, the reason why so many platforms can offer their services for a relatively minimal amount of investment, is that the educational data collected serve as ‘leads,’ not just one time but multiple times for different vendors. Contact information, academic interests, and educational background are an invaluable component of targeted marketing programs within the educational sector (Mattes 2017).

While some safeguards exist to protect student data privacy, there is a standing tension between the goals of public education and private enterprise. As Reidenberg and Schaub (2018) note:

Data confidentiality and access principles further challenge Big Data programs in education. In the United States, confidentiality is required for a student’s educational records, and families have the ability to assure data integrity with access and correction rights (see 20 U.S. Code §1232 g). By contrast, Big Data programs rely on data sharing rather than

confidentiality. Multiple vendors gain access to detailed metrics, for example, online reading patterns, and, if metadata about student interactions is captured, possibly social dynamics. Similarly, the multiplicity of data sources and dynamic processing undermine the ability of learners and their families to assure data integrity through access and correction.

As of this writing, the most recent privacy policy provided by Instructure is dated August 1st, 2018 and addresses both the Instructure and Canvas websites.

To make our Site, Apps, and Services more useful to you, our servers (which may be hosted by a third party service provider) collect information from you, including browser type, operating system, Internet Protocol (IP) address ... domain name, and/or a date/time stamp for your visit. We also use cookies and web beacons (as described below) and navigational data like Uniform Resource Locators (URL) to gather information regarding the date and time of your visit and the solutions and information for which you searched and which you viewed. Like most Internet services, we automatically gather this data and store it in log files each time you visit our Site, use our Apps, or access your account on our network. **We may link this automatically-collected data to personally identifiable information.** [Emphasis added]

In an April 2017 online question answer session regarding External Apps (LTIs), the Canvas Doc Team indicated that third parties work closely with Canvas to acquire data sets and that by default, most user information is anonymized, however that ‘this can be changed’ (Instructure 2019). Further, Instructure seems especially keen to vaunt the ease of data use within Amazon Web Services (AWS). Wade Billings, Director of IT Services for Instructure notes in a 2015 promotional video that:

... one of the main benefits of being on Amazon Web Services is that the ‘security is baked into the platform, so regardless of if I’m a small organization or a large enterprise, I get the benefit of those intrinsic security controls there, and I don’t have to build them, I don’t have to buy them, I don’t have to do anything extra. They’re just there. (Amazon Web Services 2015)

However, the AWS system appears to contain formidable blind spots of vulnerability to data hacking. Between 2017 and 2019, several security breaches made high profile news. Reporting on a 2018 hack that left Tesla’s Amazon cloud vulnerable to cryptocurrency mining, Matousek stated that:

AWS accounts, along with business and government websites and servers, have become vulnerable to ‘cryptojacking’ schemes in which hackers break into them to mine cryptocurrency, which has become increasingly lucrative in the past year. ‘Given the immaturity of cloud security programs today, we anticipate this type of cybercrime to increase in scale and velocity,’ RedLock CTO Gaurav Kumar said in a statement to Business Insider. (Matousek 2018)

Nonetheless, cloud based data systems are vulnerable to hacking, so Instructure’s claims that security is baked in to the system appear to be both overstated and given evidence to the contrary, unfounded.

According to a 2018 analysis of student privacy conducted by Common Sense Media, Canvas scored 36 out of a possible 100 with respect to student privacy largely because it is unclear whether student data collected on the LMS will be sold to third parties, shared for advertising purposes, or whether the data harvested will permit third parties to create advertising profiles used in targeted advertising. Data within the Instructure platform itself may also be vulnerable to authorization changes by students.<sup>1</sup>

Finally, a May 2019 security analysis of the Canvas Instructure Android App conducted by UC Berkeley researchers at the *International Computer Science Institute* indicated specific gaps in data privacy with a designation that the app ‘transmits sensitive data.’ The three device identifiers documented to have been ‘transmitted during testing’ include Advertising IDs,<sup>2</sup> Android IDs,<sup>3</sup> and Device Descriptions<sup>4</sup> (Canvas Student Android App Security Analysis, AppCensus 2019).

According to the Canvas Administrative Guidelines available on the SJSU website (eCampus 2014), student privacy is paramount. In accordance with the Policy for Privacy of Electronic Information and Communications (UP F97-7) and Family Educational Rights and Privacy Act (FERPA) guidelines, Canvas courses are password-protected, so that students meet in a private online classroom space. Students do not have access to other students’ personal information, such as student ID or email address. The system allows students to send emails to one another without revealing the email address. Students are able to view other students’ Display names, which appears in activities that are participated in within the course. Students have the ability to adjust their Display name to their own personal preference. Besides the Display name, Canvas keeps a record of each student’s Full and Sortable name, which is only accessible by the instructor, teaching assistant, and administrator.

However, despite the fact that the Family Educational Rights and Privacy Act (FERPA) guidelines concerning student privacy were updated in 2008 to reflect the new ecosystem being created by online program managers, there are standing tensions.

The Department of Education permits education records and personally identifiable information to be released to third-party vendors *without consent* provided that these third-parties remain under the direct control of the institution. Under FERPA, contractors are also designated as ‘school officials with legitimate educational interests.’ As such, they must be listed in an institution’s Annual FERPA notification. In addition, the latest and most robust piece of legislation to protect consumer privacy, the California Consumer Privacy Act (2018) which is set to come into effect in 2020, will not apply to not-for-profit educational institutions.

It is unclear whether, by virtue of being integrated into Canvas, a third-party app would be allowed access to other aspects of a user’s course content or other online behaviors on Canvas. Moreover, given the shared platform, it is also unknown whether Canvas would have access to teacher evaluation surveys or other data that school administrators would be able to access for personnel reviews.

## Biometric data

Yet another form of information being swept into Instructure systems includes biometric data. An April 2017 video recorded question/answer session featured Hilary Scharton, VP of Product Strategy for Instructure. In response to a question concerning the sign in and logout procedures among students who were inadvertently able to sign in to other students’ accounts using the same devices, Scharton noted:

... we’re actually doing some work right now as part of a partnership that we’re doing with Apple, um, where we’re enabling the fingerprint login ID, on IOS devices, and this is what the workflow would look like ... you have a class set of devices, right and your last class leaves and your next one comes in, um, the student from last hour didn’t log out of Canvas.

When the new student picks up the device, opens it up, um, Canvas will ask for your fingerprint, to authenticate you, as you're opening the Canvas app, and if your fingerprint doesn't authenticate, then you'll be taken back to the login screen. So either fingerprint ID with your fingerprint and user name, or to put in your login credentials ... which is really cool, I think that's awesome, especially for our elementary friends. (Canvas LMS video, 32:44)

Such processes for biometric authentication open a host of additional questions regarding data privacy. Will parents be given the option to opt in or out of biometric scanning of their children's personal information? Or will schools be given the right to grant access en masse? Will biometric data gathered on handheld devices in elementary settings be merged with data when students move through middle, high school, college, and work settings? And to what extent would users be informed of how those data would be used? If biometric authentications are being used to enable Canvas logins for elementary students, will they also be used for high school and college age students?

Zeide (2017) provides important critiques of the consequences of big data in education, including undermining of traditional intellectual privacy and safety of classrooms, highlighting the shift in pedagogical decision making from educators to technology providers, constraining teachers' academic autonomy, obscuring student evaluation, and reducing the capacity for parents', students' (and we would argue, instructors') ability to participate or challenge education decision-making.

She further notes data driven tools as defining what 'counts' as education by mapping concepts creating content, determining metrics, and setting desired learning outcomes of instruction. At work here are significant 'shifts [that] cede important decision-making to private entities without public scrutiny or pedagogical examination' (2017, 164).

In a promotional video developed by Amazon Web Services, Ivy Tech Community College representatives indicated that they 'can predict with 83% accuracy which students are likely to fail, all for 95% less than the next closest solution' (Amazon Web Services 2019, 00:42). The question then becomes how they will act on these data. Will students who fit similar characteristics be profiled and eliminated from enrollment decisions because of their so-called 'risk' in not succeeding?

## Predictive analytics and dataveillance

Lupton and Williamson (2017) make useful distinctions between the shift in education settings from surveillance to dataveillance where the latter involves the routine collection and analysis of data. They describe a new ecosystem of dataveillance beginning in primary school with apps like ClassDojo (used in over 180 different countries and over 90% of K-8 classrooms in the US, according to the ClassDojo website), which encourages teachers to award points for good behavior and deduct them for deviant performance indicators. Dojo points constitute a digital economy within a classroom, where points may be traded for Classroom Dollars used for the 'purchase' of individual items (virtual or real) or even a 'no homework pass.' Beyond the classroom, the authors note, there are a suite of apps that monitor and collect information on physical activity that use self-tracking apps and the use of wearable technologies to encourage appropriate behaviors alongside messages about well-being.

The authors point out that the kind of total surveillance that now pervades educational institutions comes with inherent risk:

... people's life chances and access to opportunities are increasingly becoming shaped by the types of social sorting afforded by dataveillance. People have few opportunities to challenge the inferences and predictions that are made by algorithmic calculations. (786)

Academic cultures of dataveillance are spanning the developmental spectrum and now rapidly colliding with changes in data policies of learning management systems that are moving precisely toward the problematic kinds of big data use that scholars have been warning about. JoAnna Redden, Co-Director of the Data Justice Lab at Cardiff University, has documented six specific forms of data harms that are resulting from the use of big data analytics. These include targeting based on vulnerability, misuse of personal information, discrimination, data breaches, political manipulation and social harm, and data and system errors (Redden 2017).

The LMS market, and Instructure in particular, is undergoing a transformation poised to make student and faculty data across all educational levels more vulnerable to such harms. The four leading LMS providers in the United States (Instructure, D2L, Blackboard, and Moodle) have switched focus towards corporate markets for employee training. To that end, Instructure acquired Portfolium for \$43 million, an ePortfolio platform, a 'student success network' that links student achievement through information concerning achievements and competencies directly to potential employers. According to official figures, Portfolium was acquired by Instructure in 2019, is a member of the Amazon Web Services EdStart program, and serves over 4.6 million students in over 3,600 colleges, universities, and high schools. The additional move announced in 2019 was Instructure's move towards greater emphasis on data analytics and artificial intelligence. The DIG platform now being discussed by Instructure will rely on artificial intelligence to apply predictive modeling to the student experience.

At a recent investors meeting, the CEO of Instructure, Dan Goldsmith, described his vision of predictive analytics to include correlation 'across universities and curricula' in order to 'start making recommendations and suggestions to the student or instructor in how they can be more successful.' The suggestions Goldsmith provided as examples are behaviorally specific and appear to shift the core responsibility of guiding teaching and learning away from instructors and toward software directives. He states:

...watch this video, read this passage, do problems 17–34 in this textbook, spend an extra two hours on this or that. When we drive student success, we impact things like retention, we impact the productivity of the teachers, and it's a huge opportunity.

Our DIG initiative, it is first and foremost a platform for [Machine Learning] ML and [Artificial Intelligence] AI, and we will deliver and monetize it by offering different functional domains of predictive algorithms and insights. Maybe things like student success, retention, coaching and advising, career pathing, as well as a number of the other metrics that will help improve the value of an institution or connectivity across institutions. (Hill 2019)

Missing from Goldsmith's analyses, however, are decades of research studies in the field of educational psychology in higher education that yield evidence-based strategies to address the host of challenges in strengthening learning within institutions of higher education (Spelt et al. 2009). Also missing is an analysis of associated harms that may be incurred from false predictions, data loss, data breaches, and/or flawed analytics with affiliated interventions (Madden et al. 2017; Redden 2017).

## Conclusions and recommendations

There is no doubt that public institutions of higher education are undergoing historically significant changes due in large part, to a culture shift; from the ‘culture of the book’ to the ‘culture of the screen’ (Postman 1993). A new digital ecology is emerging with the ability to monitor the progress of students from a very young age, through high school, college, and into the corporate space.

The cult of numbers and evaluation that has emerged has done so within a decades-long lack of public investment in higher education and a perceived sense of crisis (see Uluorta and Quill 2009). Technology has been seized upon by policy advocates as a relatively cost-effective fix to endemic social issues. Quantification is regarded as an objective, scientific, and value neutral way to remedy perceived inefficiencies within public institutions, and the net effect is to undermine complex human learning interactions in the name of democratic principles, like transparency. Institutions, departments, and individual faculty are continually measured and students, parents, and other faculty may draw upon these data to assess performance and potential. The result:

... it forces education institutions which are no longer able to evade the opinions and judgments of their clientele to take a more customer – and service-led approach. The dictates of quality, transparency and accountability lend an air of illegitimacy to any attempt to avoid scrutiny and evaluation. The modern transparency principle inevitably opens the door to more and more evaluations, which can interfere considerably with institutional routines and established practices. (Mau 2019, 91)

The purported ‘personalization’ of educational provision via LMS technologies results in the creation of a new, highly surveilled environment of competitive individualism, which reflects an increasing concern with status insecurity. Education within this social context is reimagined. However, ‘the security afforded by objectivized status information is purchased at the cost of intensified status competition’ (Mau 2019, 4). The individual is not free to choose but instead compelled to choose within highly circumscribed circumstances of being a rational autonomous agent.

Improving one’s life chances under these conditions depends upon the personalization of education at the cost of privacy and, ironically, decreased transparency concerning the use of personal data. The citizen is now an entrepreneurial self, someone who is always ready to adopt new techniques for self-management and improvement. Within the current dynamic, this leaves almost no room for alternative imaginings of self, citizens, and society. Crudely, what cannot be measured is no longer relevant. As Lynch (2017) notes:

The data collected by [Learning Management Systems] is aggregated by a number of entities. Educational institutions maintain online records of class data and of student performance. Third-party service providers retain records of tool usage that include detailed scores and personal profiles along with clickstream data recording students’ tutorial actions, written essays or other problem solutions, and even requests for help. Platform providers ... can even integrate these records across tools and link them to external profiles to provide a detailed picture of what students do and how they do it. (250)

Contractors for online educational services have expanded beyond the simple provision of a software platform for educational ‘content’ to provide a whole range of services: from admission to the continual tracking of student performance, referring students to

academic counselors if problems arise, to recruitment services post graduation (Mattes 2017). Canvas has positioned itself as a strategic partner for educational districts or even statewide adoptions from K-12 through college.

With that in mind, we offer the following conclusions and recommendations:

First, while there is a shift occurring within institutions of higher education to accommodate the new realities of university life within the digital age, there is a potential conflict between what might be termed ‘the public good’ of the university, and profit motives of private capital. In its crudest form, the Return on Investment (ROI) for venture capital is much shorter than a similar ROI for public institutions such as universities. Educational leaders are encouraged to consider the funding behind research on educational solutions. Independent, non-industry funded studies are less likely to be influenced by bottom line sales that would be tied to metrics of effectiveness.

Second, the LMS market is highly competitive and there is currently no common set of standards for platform design. SJSU adopted Blackboard, Desire2Learn, and Canvas in quick succession. It experimented with Udacity and MOOCs and found itself in the center of a national scandal over teaching in an online format that split the faculty and administration, and prompted the founder of Udacity to admit that the product it had promoted at SJSU was ‘lousy.’ Educational leaders are encouraged to ask critical questions about independent, long term evidence of effectiveness prior to adopting newly hyped educational innovations.

Third, universities run the risk of failing to serve the very communities they promise to assist by turning too quickly to technology to resolve problems of poor instruction, large class sizes, lack of public funding, and declining graduation rates. Standardization, conformity, and adherence to a methodology better suited to the bureaucracy than the classroom (it is Learning *Management* Systems, after all, that we are discussing) is the order of the day. Ironically, these dehumanizing processes are pushed amidst claims of supporting ‘personalization.’ Educational leaders are encouraged to recognize the doublespeak inherent in claims that learning management systems personalize learning.

Fourth, public universities have quickly come to rely upon the new ecology for auditing purposes. It is simply not an option for most faculty to opt out of the platform (see Fathema, Shannon, and Ross 2015). With compulsory education in many K12 settings, it may well be a requirement for students and teachers whose districts have adopted the LMS to use the platform.

Fifth, the fact that some aspects of learning are easier to measure than others might result in simplistic, surface level elements taking on a more prominent role in determining what counts as success. As a result, higher order, extended, and creative thinking may be undermined by processes that favor formulaic adherence to static rubrics. An additional problem is that evidence for the effectiveness of commercial systems to actually improve learning outcomes is limited despite ubiquitous hype for such solutions.

Sixth, lessons may also be learned from other areas such as medicine that have faced a parallel tsunami of digitally based solutions. At the 2016 conference of the American Medical Association, Dr. James Madara, President of the AMA described key challenges in the field of medicine as health technologies were rapidly proliferating into medical spaces. While acknowledging that many innovations increased possibilities for improved care, Madara also noted a large sector that actually made matters worse, ‘from ineffective electronic health records, to an explosion of direct-to-consumer digital health products, to

apps of mixed quality - it's the digital snake oil of the early twenty-first century' (American Medical Association 2016).

A question for higher education administrators to consider is whether the solutions being marketed to them are indeed solutions or what Madara refers to as 'digital snake oil'. In the spirit of critical thinking that is so enthusiastically encouraged by administrators in higher education settings, we suggest healthy doses of critical inquiry into actual evidence of claims made by proponents of AI systems in education. Dataveillance concerns in education are integral to a foundational understanding of data markets and analytics that would lead individuals to be subject to predictive policing (Ferguson 2017), vulnerable to data harms (Madden et al. 2017), algorithmic bias (Eubanks 2018), and unwitting victims of surveillance capitalism (Zuboff 2019).

Seventh, education about algorithmic bias, predictive harms, and the need for algorithmic transparency will be an important step in moving higher education institutions toward ethical data practices that include full disclosure about the ways that education community members' data will be used (see ACM 2017).

Students, as the key constituents being served in higher education, are the ones who will be most affected long term by the use of their data. Student voice will be central to building awareness and demanding privacy rights. Future inquiries on the datafication of higher education should focus on the extent to which students have been provided full disclosure of data use (including algorithmic transparency) and to map processes by which they can make collective requests for data to not be gathered on their moment-to-moment online behaviors.

San José State University has a rich history of social justice and student activism for human and civil rights. Such a culture rooted in ethics yields important challenges for members of the academic community attuned to dataveillance processes that funnel millions of data points daily from Canvas Instructure into Amazon Web Services servers. Aiming for true alignment with equity and social justice values of the university would appear to be compromised given the reality of where we are sending personal data. While we send data to Amazon Web Services, the employees who work at AWS are demanding that,

... Amazon remove Palantir, Peter Thiel's big data firm, which has contracts with ICE and law-enforcement agencies, from Amazon Web Services. 'Our company should not be in the surveillance business,' the letter reads. 'We should not be in the policing business; we should not be in the business of supporting those who monitor and oppress marginalized populations. (Kosoff 2019)

Finally, as academics, we need to ask why industry researchers are not held to the same ethical standards to which we are held to ensure protection of human subjects in research. We close with a reminder that while it may appear a daunting task years after processes have ushered in the datafication of higher education, inevitability narratives need not apply. Educational leaders can choose to require stronger data protections, or to discontinue harmful contracts with edtech products that exploit user data.

## Notes

1. In 2017, a student discovered how to un-mute his 'muted' grade and made a YouTube video documenting the exploit. (CanvasLMS 2017). <https://community.canvaslms.com/thread/16830-student-discovered-his-muted-grade>.

2. Advertising ID: ‘Transmitted during testing’ Explanation: ‘The Android Advertising ID (AAID) is used for tracking and behavioral advertising. You can modify the settings of your phone to reset this identifier, to prevent tracking over time, or opt-out of behavioral advertising altogether.’
3. Android ID: ‘Transmitted during testing’ Explanation: ‘The Android ID is a random serial number that is created when you first configure your phone. It is a globally unique identifier that could be used to track you over time and across apps, and can only be reset by performing a factory reset of your phone.’
4. Device Descriptions: ‘Transmitted during testing’ Explanation: ‘This refers to a list of your phone’s current configuration parameters, including a description of your phone’s hardware and software. While this is often used by developers to collect performance data and detect software bugs, it could also be used to construct a unique “fingerprint” of your device for tracking purposes.’

## Disclosure statement

No potential conflict of interest was reported by the author(s).

## ORCID

Lawrence Quill  <http://orcid.org/0000-0002-7020-6106>

## References

- ACM. January 12, 2017. “Statement on Algorithmic Transparency and Accountability and Principles for Algorithmic Transparency and Accountability.” Association for Computing Machinery US Public Policy Council. [https://www.acm.org/binaries/content/assets/public-policy/2017\\_usacm\\_statement\\_algorithms.pdf](https://www.acm.org/binaries/content/assets/public-policy/2017_usacm_statement_algorithms.pdf).
- Amazon Web Services. 2019. “Education Partner Solutions.” Canvas By Instructure Partner Page. <https://aws.amazon.com/education/partner-solutions/>.
- Amazon Web Services [Youtube Channel]. August 4, 2015. “Instructure Delivers Online Learning Globally Using AWS.” Video clip at 2:49. <https://aws.amazon.com/solutions/case-studies/instructure/>.
- American Medical Association. June 16, 2016. “AMA CEO Outlines Digital Challenges, Opportunities Facing Medicine.” AMA Press Release. <https://www.ama-assn.org/press-center/press-releases/ama-ceo-outlines-digital-challenges-opportunities-facing-medicine>.
- AppCensus. 2019. *Canvas Student Android App Analysis. The Usable Security and Privacy Group*. U.C. Berkeley: International Computer Science Institute. Accessed May 9, 2019. <https://search.appcensus.io/app/com.instructure.candroid/195>.
- Apple, Michael. 2004. “Creating Difference: Neo-Liberalism, neo-Conservatism and the Politics of Educational Reform.” *Educational Policy* 18: 12–44.
- Apple, Michael. 2007. “Education, Markets, and an Audit Culture.” *International Journal of Educational Policies* 1: 4–19.
- Apple, Michael, Jane Kenway, and Michael Singh. 2005. *Globalizing Education – Policies, Pedagogies, & Politics*. New York: Peter Lang.
- Benjamin, Ruha. 2019. *Race After Technology*. Cambridge: Polity Press.
- Boggs, Christine, and Meg Van Baalen-Wood. 2018. “Diffusing Change: Implementing a University- Wide Learning Management System Transition at a Public University.” In *Leading and Managing e-Learning*, edited by A. A. Piña, V. L. Lowell, and B. R. Harris, 115–129. New York: Springer.

- CanvasLMS [Youtube Channel]. April 12, 2017. "Ask Me Anything Hilary Scharton, VP Product Strategy K-12." Session details at <https://community.canvaslms.com/events/1943>. Video clip 33:44 from <https://www.youtube.com/watch?v=yE8YNWXva8A>.
- Christl, Wolfie. 2017. "Corporate Surveillance in Everyday Life: How Companies Collect, Combine, Trade, and Use Personal Data on Billions." Cracked Lab Institute for Critical Digital Culture, Vienna, Austria. [https://crackedlabs.org/dl/CrackedLabs\\_Christl\\_CorporateSurveillance.pdf](https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf).
- Common Sense Media. 2018. *Canvas Evaluation*. <https://privacy.common sense.org/evaluation/canvas>.
- Crawford, Kate, and Jason Schultz. 2014. "Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms." *Boston College Law Review* 55 (1): 93–128. <http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4>.
- Department of Defense. January, 2020. "Interoperability." 110–111. Department of Defense Dictionary of Military and Association Terms. <https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf>.
- Deveau, Scott. February 18, 2020. "Instructure Accepts Higher Takeover Offer From Thoma Bravo." *MSN.com*. <https://www.msn.com/en-us/finance/companies/instructure-accepts-higher-takeover-offer-from-thoma-bravo/ar-BB100m7p>.
- eCampus [SJSU]. March 5, 2014. "eLearning and Instructional Support: Canvas Administrative Guidelines." San José State University. [http://www.sjsu.edu/ecampus/docs/eCampus\\_Administrative\\_Guidelines\\_3.5.14.pdf](http://www.sjsu.edu/ecampus/docs/eCampus_Administrative_Guidelines_3.5.14.pdf).
- Empson, Rip. April 12, 2013. "Instructure Launches App Center To Let Teachers, Students Install Third-Party Apps Across Learning Platforms." *TechCrunch*. <https://techcrunch.com/2013/04/12/instructure-launches-app-center-tolet-teachers-students-install-third-party-apps-across-learning-platforms/>.
- Eubanks, Virginia. 2018. *Automating Inequality: How High Tech Tools Profile, Police, and Punish the Poor*. New York: St. Martin's Press.
- Fathema, Nafsanieth, David Shannon, and Margaret Ross. 2015. "Expanding the Technology Acceptance Model (TAM) to Examine Faculty Use of Learning Management Systems (LMSs) In Higher Education Institutions." *MERLOT Journal of Online Learning and Teaching* 11 (2): 210–232.
- Ferguson, Andrew. 2017. *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. New York: New York University Press.
- Gilliard, Chris. October 15, 2018. "Friction-Free Racism: Surveillance Capitalism Turns a Profit by Making People More Comfortable with Discrimination." *Real Life*. <https://reallifemag.com/friction-free-racism/>.
- Hill, Phil. 2011. "Emerging Trends in LMS / Ed Tech Market." *eLiterate*. <https://eliterate.us/emerging-trends-in-lms-ed-tech-market/>.
- Hill, Phil. 2017. "Movement of Canvas LMS to Global Markets." *eLiterate*. <https://mfeldstein.com/movement-canvas-lms-global-markets/>.
- Hill, Phil. March 11, 2019. "Instructure: Plans to Expand Beyond Canvas LMS into Machine Learning and AI." *eLiterate*. <https://mfeldstein.com/instructure-plans-to-expand-beyond-canvas-lms-into-machine-learning-and-ai/>.
- Hill, Phil. February 18, 2020. "Instructure CEO Dan Goldsmith Resigns and New Approach For Bravo Acquisition." *PhilOnEdTech*. <https://philonedtech.com/instructure-ceo-dan-goldsmith-resigns-and-new-approach-for-bravo-acquisition/>.
- Instructure. 2019. "Canvas Features." <https://www.instructure.com/canvas/features/higher-education?newhome=canvas>.
- Instructure. 2020. "Canvas Data." <https://www.instructure.com/canvas/features/higher-education?newhome=canvas>.
- Instructure Bridge. 2019. "Bridge Puts People First - Just Like You." Quote from promotional video. <https://www.instructure.com/bridge/products/bridge-suite-b?newhome=bridge>.
- Kosoff, Maya. 2019. "Amazon Workers to Jeff Bezos: 'Stop Weaponizing Our Tech.'" *Vanity Fair*, June 18, 2018. <https://www.vanityfair.com/news/2018/06/amazon-workers-to-jeff-bezos-stop-weaponizing-our-tech>.

- Lupton, Deborah, and Ben Williamson. 2017. "The Datafied Child: The Dataveillance of Children and Implications for Their Rights." *New Media & Society* 19 (5): 780–794.
- Lynch, Collin. 2017. "Who Prophets from Big Data in Education? New Insights and New Challenges." *Theory and Research in Education* 15 (3): 249–271. doi:10.1177/1477878517738448.
- Madden, Mary, Michele Gilman, Karen Levy, and Alice Marwick. 2017. "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans." *Washington University Law Review* 95 (1): 53–125. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2930247](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2930247).
- Manolev, Jamie, Anna Sullivan, and Roger Slee. 2018. "The Datafication of Discipline: ClassDojo, Surveillance and a Performative Classroom Culture." *Learning, Media, and Technology* 44: 1. <https://tandfonline.com/doi/abs/10.1080/17439884.2018.1558237>.
- Matousek, Mark. February 20, 2018. "Tesla's Amazon cloud account was hacked and used to mine cryptocurrency." *Business Insider*. <https://www.businessinsider.com/hackers-teslas-amazon-cloud-to-mine-cryptocurrency-2018-2>.
- Mattes, Margaret. 2017. "The Private Side of Public Higher Education." *The Century Foundation*, 1–23. <https://tcf.org/content/report/private-side-public-higher-education/>.
- Mau, Steffen. 2019. *The Metric Society – On the Quantification of the Social*. Cambridge: Polity Press.
- Menard, Justin. May 20, 2019. "EdTech Companies with the Most Student Data." *ListEdTech*. <https://www.listedtech.com/blog/edtech-companies-with-the-most-student-data>.
- Postman, Neil. 1993. *Technopoly: The Surrender of Culture to Technology*. New York: Vintage.
- Redden, Joanna. December 7, 2017. "Six Ways (and counting) That Big Data Systems are Harming Society." *The Conversation*. <https://theconversation.com/six-ways-and-counting-that-big-data-systems-are-harming-society-88660>.
- Reidenberg, Joel, and Florian Schaub. 2018. "Achieving Big Data Privacy in Education." *Theory and Research in Education* 16 (3): 263–279.
- Rubel, Alan, and Kyle Jones. 2016. "Student Privacy in Learning Analytics: An Information Ethics Perspective." *The Information Society* 32 (6): 143–159.
- Russell, N. Cameron, Joel Reidenberg, Elizabeth Martin, and Thomas Norton. 2018. "Transparency and the Marketplace for Student Data." *Virginia Journal of Law and Technology*, Forthcoming. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3191436](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3191436).
- Spelt, Elizabeth, Harm Biemans, Hilde Tobi, Pieternel A. Luning, and Martin Mulder. 2009. "Teaching and Learning in Interdisciplinary Higher Education: A Systematic Review." *Educational Psychology Review* 21: 365–378. <https://link.springer.com/article/10.1007%2Fs10648-009-9113-z>.
- Uluorta, Hasmet, and Lawrence Quill. 2009. "In Pursuit of the Knowledge Worker: Educating for World Risk Society." *International Studies in the Sociology of Education* 19 (1): 37–51.
- Young, Jeffrey. February 18, 2020. "As Instructure Changes Ownership, Academics Worry Whether Student Data Will Be Protected." *EdSurge*. <https://www.edsurge.com/news/2020-01-17-as-instructure-changes-ownership-academics-worry-whether-student-data-will-be-protected>.
- Zeide, Elana. 2017. "The Structural Consequences of Big Data-Driven Education." *Big Data* 5 (2): 164–172. [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2991794](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2991794).
- Zuboff, Shoshanna. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.