Received: 19 April 2021 | Revised: 15 July 2021 | Accepted: 12 September 2021

DOI: 10.1002/asi.24575

RESEARCH ARTICLE

JASIST WILEY

Sins of omission: Critical informatics perspectives on privacy in e-learning systems in higher education

Britt Paris | **Rebecca Reynolds** | **Catherine McGowan**

Department of Library and Information Science, Rutgers, The State University of New Jersey, New Brunswick, New Jersey, USA

Correspondence
Britt Paris, Department of Library and Information Science, Rutgers University, New Brunswick, NJ, USA.
Email: britt.paris@rutgers.edu

Abstract

The COVID-19 pandemic emptied classrooms across the globe and pushed administrators, students, educators, and parents into an uneasy alliance with online learning systems already committing serious privacy and intellectual property violations, and actively promoted the precarity of educational labor. In this article, we use methods and theories derived from critical informatics to examine [anonymized] University's deployment of seven online learning platforms commonly used in higher education to uncover five themes that result from the deployment of corporate learning platforms. We conclude by suggesting ways ahead to meaningfully address the structural power and vulnerabilities extended by higher education's use of these platforms.

1 | INTRODUCTION

As the COVID-19 pandemic hit the United States in March 2020, it created an urgent need to reconfigure "business-as-usual" across many sectors. Higher education, along with primary and secondary schools, rushed to using corporate learning platforms, further entrenching their long-standing and often problematic relationship with massive e-learning vendors. This case study engages information science literature on privacy, surveillance, and educational technology research from the perspective of critical informatics (CI), focusing upon contractual discourse among vendors and one higher educational institution, including terms of use, privacy policies, and other contract language. Our analyses reveal corporate learning technologies as mechanisms of economic capture, surveillance, and control that function as antithetical to pedagogical and privacy goals and can be harmful to students and instructors.

Information privacy encompasses multiple perceptions and behaviors across a range of contexts (Vasalou et al., 2015, p. 918). Sociotechnical systems perspectives propose that the difficulties of defining and enforcing privacy result because today's online information environments are expressed in complex relations between information, its material instantiation, and the myriad ways it can be expressed through these technical systems (Nissenbaum, 2009; Vasalou et al., 2015). Because of these complexities, privacy should be interpreted as highly contextual, and must consider a variety of actors' control over information that exists beyond common notions of privacy as a market-based good (Marwick & boyd, 2014; Nissenbaum, 2009).

Further, technology is a lever of structural power intertwined with the technocratic solutionism that pervades informatics and information science research, in that work often uncritically relies on data to produce normative prescriptions for technical solutions to social problems (Day, 2007; Sawyer & Eschenfelder, 2002; Sweeney & Brock, 2014). In contrast, a growing body of literature in surveillance studies bridges sociology (Benjamin, 2019a, 2019b), labor studies (Stark et al., 2020), Black studies (Browne, 2015), policy studies (Regan & Khwaja, 2019; Zeide, 2017), and CI (Noble, 2016; Sweeney & Brock, 2014), providing numerous examples of how both historical and contemporary surveillance technologies are deployed on less powerful groups to control these groups and extract economic value from them (Benjamin, 2019a, 2019b). Theorization around privacy and ethics has been challenged for neglecting how technology is a sphere of influence used by politically dominant groups to reify and extend their power

over already subordinated groups (Benjamin, 2019a, 2019b; Browne, 2015; Hoffmann, 2019, 2020; Noble, 2016, 2018). Learning technology in higher education is a site of critical concern, binding together issues of technocratic rationality, privacy, and surveillance.

Jones, Rubel, and LeClere (2020) analyze EdTech policies in higher education institutions (HEIs) and propose HEIs should serve as "information fiduciaries" in educational data mining and EdTech systems. This designation, the authors reason, entails a more rigorous commitment to data collection and use policies to protect university stakeholders from surveillance and control creep. Our study builds on this work, exploring the how one institution lives up to serving this fiduciary role, addressing observable dynamics of technocratic rationality manifesting in higher education building from a critical technical discourse analysis (Noble, 2016; Sweeney & Brock, 2014) of publicly available policy and contractual documents between our home university and its partnering e-learning vendors. We explore what value the university exchanges in vendor contracts, privacy and terms statements, and specified and unspecified data management policies and offer a proposed model indicating the nature of some relationships and dynamics among primary dimensions of EdTech features, stated user benefits, and unstated corporate or institutional benefits. The study points to the utility of CI as a conceptual and theoretical information science research domain that promises a robust engagement with social structures and power dynamics in higher education information and learning management contexts, contributing toward information science theory-building, expanding on Feenberg's notion of technical citizenship (2017a).

2 | TECHNOCRATIC RATIONALITY IN EdTech

Even before the COVID-19 pandemic, learning technologies had been advanced as a solution to combat the multiple crises of the university, such as state funding cuts and federal student debt (Feenberg, 2017b) that had forced university assets to be managed as real estate and natural resources investment enterprises subject to whims of volatile markets and technocratic rationing (Newfield, 2016). Besser and Bonn (1996) note that information technology restructures relationships between capital and labor across many sectors, and propose that when technocratic solutions are introduced into learning, it is likely to "shift the balance of power between a fragmented faculty and a strong administration" (p. 881). This study is guided by theories and methods used in CI to understand corporate learning technologies as mechanisms of economic capture, surveillance, and control.

2.1 | Background on CI approaches

Our work builds upon political economy as discussed by Harvey (2003) and Feenberg (2017a, 2019), to understand the technocratic rationality inherent in e-learning practices and policies. Within this realm, we consider Eubanks' (2018) criticism of the discourse of triage within public sectors and Klein's "Shock Doctrine" (2008) that both describe how, after 40 years of neoliberal policy favoring privatization, state defunding pushes public entities into crisis mode, even as market-based competition does little to make these public institutions whole. Funding cuts are used to justify layoffs and liquidation of rights and benefits for people who would provide services, in this case education (Newfield, 2016), and technology is lauded as a cheap, quick, and efficient workaround for lost human labor. All the while, predatory privatization in higher education promises kickbacks to decision-makers and vendors alike (Feenberg, 2017a, 2017b). As we worked with our union to investigate our home institution's e-learning ecosystem and information management policies and practice, it became clear how relevant CI perspectives pertain.

Critical perspectives on EdTech research have also been offered by Selwyn (2012) whose book *Distrusting Educational Technology* builds upon critical technology studies and social informatics theories including Kling and Iacono (1988), Lovink (2012), Popkewitz (2018), taking a fundamentally oppositional (or "pessimistic" per Dienstag, 2009) standpoint to draw helpful lines of sensemaking and critique across the multiple existing fields of EdTech research. Selwyn's book addresses problems of surveillance and data reduction as "dehumanizing and de-professionalizing the relationships between people in an educational context" (2012, p. 58–60). His work also critiques EdTech literatures espousing "disruption" logics as holding fundamental anti-public education agendas, proposing that such accounts, which might have once read as counter-cultural, "now should be seen as profoundly in step with contemporary dominant ideologies" (2013, p. 161). When these logics are engaged uncritically, with an implicit assumption of EdTech primacy (the notion of EdTech as implicitly "better" because it is novel or new), without attention, for instance, to rigorous evidence-based research on EdTech, disruption logics risk potential for disrupting and eclipsing the very learning occurring successfully, with new replacement technology systems that fundamentally detract from the learning experience. He states that while converging post-digital technologies are likely to be associated with another "long wave" of capitalist development (p. 165), Selwyn argues that through thin communitarianism that focuses efforts on achievable improvements in the public

good, and a politicization of EdTech, actors can play more direct roles in ongoing developments. These perspectives fall in line with Feenberg's notion of technical citizenship (2017a), which proposes a mode of "conscious co-production" (11) where the actions of users have an ability to affect the codes and designs that define roles of the users within the technological network. This conscious co-production from below, results when ordinary, nonexperts are enrolled in technological networks in ways that encourage them to develop a situated, practical knowledge of the network itself, and avenues to exercise this knowledge. This situated knowledge and related practices can be cultivated as insider power that can be exercised over technological development, which when exercised with care, can upend unequal power relations, and promote more ethical sociotechnical relationships.

In this study, the CI research paradigm provides (a) an ethical perspective rooted in attending to structural power and oppression beyond the technocratic rationality lens (Greene et al., 2019; Roberts & Noble, 2016); (b) a set of rich critical theories and research methods for discerning the social and structural dynamics at play with e-learning technologies; (c) ways to think about reconfiguring e-learning technology ecosystems to become in greater alignment and solidarity with disenfranchised groups interests (in this case, student and instructors). CI shares normative and analytical orientations to research with social informatics, a "problem-oriented" paradigm developed to empirically investigate technical and organizational aspects of information systems (Sawyer & Eschenfelder, 2002) foregrounding culture and power dynamics. Like science and technology studies (STS), CI investigates social and political assumptions built and reified within technologies (MacKenzie & Wajcman, 1999; Pinch & Bijker, 1984), addressing how meaningful correctives entail not more technology per se, but rather political and social efforts to dismantle harmful systems and offer liberatory alternatives (Benjamin, 2019b; Costanza-Chock, 2020).

2.2 | EdTech learning experience quality

While evaluation of e-learning technology affordances is not the focus of this paper, we note that meta-analyses and other comparative research has shown e-learning technologies to exert only modest improvements over face-to-face learning, and in the context of blended learning only; for fully distant e-learning modalities, research has shown either no advantages, or lower score outcomes (Means et al., 2013). Learning sciences approaches tend to be more design-based and developmental, often exploring the ways that technology, instructional innovations, and affordances in situ, can provide advantages in meeting pre-specified, clearly articulated learning objectives with given groups or populations; this research discipline also aims to contribute new theories of learning and instruction as scholarly knowledge. Even among more rigorous evidence-based innovations emerging from the learning sciences and learning analytics scholarly communities (Haythornthwaite et al., 2016; Reynolds et al., 2019), Scheffel et al. (2014) call for reprioritization and centralization of privacy considerations to take greater precedence.

In contrast, more generic template design approaches of commercial learning platforms aiming for replicability, swift mass scale-up, and market domination, tend to be unmoored from research, incorporating shallow analytics practices, models, and algorithms from business analytics fields (Siemens, 2012, 2013). In such platforms, reductionist over-simplified uses of user log file data to compile systems-based learning management system (LMS) analytics metrics (e.g., frequencies of engagement), dashboard data and indicators (e.g., coarse diagnostics of student "engagement" and "learning"), and predictive machine learning and algorithmic tools trained with biased data can lead to students' and instructors' unscientifically rigorous "data-driven decision-making" practices that have consequences such as false inferences in teachers' assessment and evaluation of student learning, and administrators' monitoring of teacher accountability (Gill et al., 2014; Jones, 2019b). It is the scholarly field of learning analytics where legitimate methods of assessment, evaluation, and system design that consider critical questions such as the situated nature of data; biases inherent to systems training datasets, design processes and uses; predictive validity, etc., are seeing refinement, building on scientifically rigorous, critically sensitive, situated, design-based approaches. Jones (2019a) discusses common miscommunication and cross-talk that occurs in various environments where actors use the term "learning analytics." To avoid conflation and confusion, in this paper, we refer to the technologies in question, largely as "EdTech." We refer to systems-based affordances in EdTech by its more specific functionality rather than adopting a "learning analytics" catch-all label. When referring to the scholarly field of "learning analytics," we qualify this term use by adjacently indicating "field" or "scholarly community."

2.3 | Data privacy in e-learning

Sociotechnical studies of learning technologies to-date exploring EdTech's expansive mining of user data (Jones, Asher, et al., 2020; Rubel & Jones, 2016, 2020) have adopted Nissenbaum's (2011) contextual integrity approach to privacy that understands how normative and

ethical orientations to information and privacy in sociotechnical systems depend on the context, and differ among individuals and groups, and change over time. Importantly for the sociotechnical studies of learning technologies, contextual integrity approaches highlight four areas to guide privacy policy: (a) how social and structural concerns suggest what actors' data should be kept private and from what other actors; (b) what and how much information about the student is encapsulated in the data; (c) accounting for benefits and burdens to various actors in a particular context, and finally (d) focusing on how parties are made aware of risks and benefits, as well as levels of selection, option, and choice users are provided to make their participation decision (2011). Studies of privacy in EdTech have operationalized Nissenbaum's contextual privacy to determine problem areas for institutions and e-learning vendors, which include: institutional interests are not aligned with educator and student stakeholder interests (Rubel & Jones, 2016); improper uses of student and instructor data for non-verified "diagnostic" evaluation purposes; increasing use of proprietary, black-boxed machine learning-trained algorithms and lack of transparency on data uses (Mittelstadt et al., 2016); and lack of shared language and disjointed inter-disciplinary meaning-making between researchers and practitioners (Jones, 2019a). These studies investigated the phenomenon of EdTech privacy from multiple vantages and touch upon issues surrounding the political economy of EdTech as it relates to privacy that are more directly addressed by in this article. This article is on similar ground with Zeide (2017), Regan and Khwaja (2019), Polonetsky et al. (2018) and Polonetsky and Tene (2014) whose concerns are around neoliberalism, structural inequality, and the possibility for university stakeholder self-determination regarding EdTech, but our study draws more heavily from Feenberg (2017a, 2017b), Selwyn (2012), and Harvey (2003).

Further, these studies of EdTech privacy show that while EdTech vendors are subject to the federal Family Educational Rights and Privacy Act (FERPA), which affords parents or students over 18 the right to have some control over the disclosure of personally identifiable information (US Department of Education, 2018)—vendors enjoy a "school exception criteria" allowing institutions to disclose student information to vendors without their consent, for "authorized purposes" (Jones, 2019b; Rubel & Jones, 2016). "Authorized purposes" are so broadly construed that Jones (2019b) suggests "It may be that institutions are withholding information about [e-learning vendor] data practices to keep student privacy concerns at bay, concerns that could potentially derail beneficial contracts with vendors" (p. 10). While federal student privacy law allows this loophole, a few states, like California, do require more rigorous protection of student data (Student Privacy Laws, 2021). In this study, we will look only at federal law, as vendors in question operate across many U.S. states. LMS platform use becomes compulsory by students and faculty who are not asked for consent (Jones, Rubel, & LeClere, 2020; Rubel & Jones, 2016). Rubel and Jones (2016) suggest information scientists and policy professionals establish new standards, norms, and practices protecting stakeholder rights, considering FERPA as a "floor, not a ceiling" (p. 154).

2.4 | Surveillance reifies structural inequity

A main thrust of surveillance studies asserts that minoritized groups have never enjoyed the full force of privacy afforded to dominant classes; they have never felt their privacy was regarded as important by decision-makers and technology designers to begin with, let alone in online environments, law enforcement (Benjamin, 2019b; Browne, 2015), workplaces (Stark et al., 2020), and schools (Gilliard, 2017; Swauger, 2020). This constitutes a question of data justice (Authors, 2017; Costanza-Chock, 2020; Dencik et al., 2016). Feenberg (2019) discusses surveillance as a major concern within his proposed "consumption model." Commercial EdTech platforms' use of business analytics data is particularly problematic for certain groups of students (e.g., students of color, student athletes, and women vulnerable to more excessive monitoring) (Benjamin, 2019a, 2019b; Browne, 2015; Jones, Asher, et al., 2020). Many argue that these invasive affordances, like facial recognition technologies, should be dismantled and abolished outright (Benjamin, 2019b).

2.5 | Inequities in intellectual property control

Intellectual property concerns add to the picture of stakeholder vulnerabilities in HEIs' e-learning system policies and practices. Broadly, intellectual property in the U.S. protects individual ideas, performances, or identity markers as a market-based good. However, in recent years, intellectual property has been a legal tool by which powerful entities—publishers, tech companies, and other corporate entities, have become protected as individuals, and allowed to maintain market dominance in an increasingly sparse field of competition (Fallis, 2007).

EdTech systems have direct access to stakeholder-generated content to use toward improvement of educational and algorithmic products and once included in these products, these data become a protected "trade secret" of the company (Jones, Rubel, & LeClere, 2020). While EdTech companies purportedly do not sell their

data assets, and student and instructor content is putatively protected, mergers with private equity firms are a reason for concern. In 2019, Advance Publications purchased TurnItIn, a plagiarism detection company with a massive trove of student intellectual property in the form of written essays, for $1.75 billion (Johnson, 2019). It is unclear how former contractual obligations and protections must be upheld. Further, within institutions, instructor content can be and is co-opted without originators' consent or permission, to pass along to future instructors creating worker precarity. For example, in 2020 video lectures of a professor who died in 2019 were still being used in a later semester in an art history class at Concordia University in Montreal as if the professor were still administering the course—the students only found out their professor was deceased when they tried to find the professor's email address (Bartlett, 2021). These examples show that this is an enormous area of EdTech data practice that is ripe for exploitation and should be attended to closely in university policy. The novel privacy concerns around private equity firms entering the equation are only part of the problems. The commodification of personal information and user-generated data is an accepted practice in the technology sphere, but it is exploitative along the lines of structural inequality and gives economic and informational power to industries and vendors that are already powerful (Feenberg, 2017b; Zeide, 2017).

2.6 | Research questions

RQ: How is structural power reified and extended through the agreements between education technology vendors and [anonymized university]?

a. What value does the university exchange for the vendor contract terms?
b. What is the agreement between education technology vendors and educational institutions regarding user data?
c. How do these agreements articulate and enforce consent?
d. How is privacy regarded in these agreements?
e. How do these agreements dictate the terms of surveillance?
f. How does the agreement between the vendor and institution consider intellectual property?

Addressing these questions offers contributions to the growing CI and data justice scholarly research evidence base offering insights on how technology shapes and is shaped by social structures via institutional policy, discursive, and practice-based formations that extend and reify structural power, perhaps by sins of omission. We propose that our findings contribute modestly but meaningfully to the growing scholarly CI discourse.

3 | MATERIALS AND METHODS

We began our research as department union representatives, to guide our local AAUP-AFT leadership's fact-finding around our institution's EdTech vendor practices, stemming from privacy and surveillance concerns among union membership stakeholders. Some institutions, like the University of California, Los Angeles, operate data policy boards, composed of faculty, library staff, students, and administrators, conducting open meetings to review terms of service and contracts with vendors to ensure that the university advocates for data policy that serves the educational mission of the institution and includes input from the broad swath of university stakeholders with significant transparency (Borgman, 2018; Tsai & Gasevic, 2017). However, [anonymized] University's formal policies around educational technology are not publicly inscribed, documented, clear, nor accessible, without recourse for determining how these policies are enforced. We therefore sought to investigate our university's relationship with vendors through publicly available terms of service, data management and privacy language, and contracts and invoices obtained through open public records acts (OPRA) and requests, as the primary data sources. This engaged research is bounded to our home university, to better understand what is happening within one university and provide a basis for enacting change within our home university, with the suggestion that other interested individuals at other universities may replicate our methods in their own investigations. We formalized our efforts into a systematic research study as we aggregated the collection of documentation.

3.1 | Research design

Examination of policy documents as data sources occur frequently in information policy scholarship (Brown & Klein, 2020; Sanfilippo et al., 2020), critical legal theory (Crenshaw, 1989; Zalesne, 2013), and Black feminist standpoint epistemology (Collins, 1990). We combine the case study method with *discourse analysis* to compare language within extant policy documents; past work has employed this combination of methods for instance to understand how organizations that comprise the analytical units of the case study, determine and enforce policy (Allan et al., 2009; Sanfilippo et al., 2020). The case study method can reveal analytically significant problems related to power imbalances, such as discursive deception

in policy documents, and the mismatch between promises and actual material processes among stakeholders. In case study, comparisons can also be made among the analytical units. In our study, each of the top 10 vendors contracted by [anonymized] University comprises the analytical units of comparison, and within each unit, sub-units include varying source types of available extant data.

As with Brown and Klein's (2020) case study comparing data collection policies at various universities, we used Allan et al.'s (2009) policy discourse analysis (PDA) coding process—a multilayered approach that examines policy language as a marker of discourse, through an iterative combination of deductive and inductive coding (p. 58). This interactive cycling between policy data and theory surfaces how subjects in different positions of power articulate their position, practices, and goals vis-à-vis the documents, and highlights how "power functions in post-secondary institutions by drawing attention to what is stated and what is not" (Brown & Klein, 2020, p. 7; Allan et al., 2009). Our study further extends PDA, to systematically incorporate critical questions about power and control found in critical technocultural discourse analysis (CTDA) (Sweeney & Brock, 2014) which is derived from critical discourse analysis (Fairclough, 2013). We use a coding scheme of pre-derived critical questions in the third wave, described below, to layer in this added dimension of CTDA, to the PDA.

Our work also builds upon Rubel, Jones, and Leclerc (2020) in this journal, who analyze three universities' EdTech policies and propose HEIs as "information fiduciaries" in educational data mining and EdTech systems deployment. This designation, the authors reason, entails a more rigorous commitment to data collection and use policies to protect university stakeholders from surveillance and control creep (Kitchin, 2014). Our study explores the ways in which one institution lives up to serving this fiduciary role, providing an in-depth case analysis of their policies, across multiple vendors-including analysis of OPRA-obtained contractual documents not previously addressed as data sources in this arena. We integrate the CI analytic frame, considering how business vendor contracts, policies, and terms of service become imbued with complex relations of power given diverging interests and roles of the parties to their generation and use: vendors, institutions, and end user constituents (including students, instructors, staff, and senior administrators). We concur with and adopt Jones & Asher et al. (2020) ideal and build on this discourse in explicating sociotechnical dynamics among actors in a complex higher education institutional ecosystem composed of numerous conflicting interests (Feenberg, 2017a, 2017b) through the lens of privacy, consent, and surveillance. The actors who played a role as "stakeholders" in the ecosystem studied, are as follows.

- [anonymized] University's AAUP-AFT union leadership including co-presidents, and past president
- University's union membership
- Corporate vendors (Table 1)
- Local HEI decision-makers including the university Chief Information Officer (CIO)
- [anonymized] University, a U.S. public university
- Instructors
- Staff
- Students
- Parents
- Researchers

We refer to these parties throughout the results and findings. While we focus on textual and document analysis only in this study, our ongoing stakeholder roles as union representatives, instructors, students, and researchers, engaging in communications, teaching, and service with and among these actors, provide us with additional knowledge of this field site, necessarily influencing our interpretations. We also have interests that have influenced the critical interpretive lenses we have chosen to situate the work in, given our concern over justice for the rights of less powerful actors.

One author comes to this work as an insider—a former practitioner in learning technology design, development, and evaluation. The other two are outsiders to educational technology research and work but are interested in issues of data privacy and justice. At union meetings in 2018–2020, union members were eager for more information on questions of EdTech equity, privacy, surveillance, and data collection and uses given their observations of what were perceived as rights violations, and lack of university transparency. Concerns grew in the pandemic and given our expertise, the authors embarked on initial fact-finding about contracts, university and vendor relationships, and student and faculty privacy rights. We initially conceptualized this work with an assumed outcome of pragmatic institutional policy shifts. As our inquiries took shape and we also explored the scholarly literature for context, we saw the opportunity to systematize our approaches into a research agenda. Throughout the process, we had conversations with leaders and stakeholders that offered support for our study findings, and our union affiliation was disclosed and was the condition for access to these union role-based conversations which were not recorded. They are thus omitted from our systematic method and results; instead, we focus on documentary evidence.

TABLE 1 List of platforms and value propositions

List of platforms in wave 1	Value proposition, per vendor website
Canvas	Cloud-based LMS that is student-centered and easy to use
Kaltura	Cloud video software that creates virtual classroom through video publishing to be accessed synchronously or asynchronously
Microsoft Teams[a]	Project management and virtual office setting combining Microsoft software portfolio
Big Blue Button	Open-source web conferencing system allows free customization, and no software downloads are required
Respondus Lockdown Browser[a]	Custom browser for exams and remote proctoring, most keyboard and mouse functions are disabled to prevent cheating unless specified for use by instructor
WebEx[b]	Video conferencing software allowing simple one-click feature to join a meeting
YouTube[b]	Free video sharing platform, viewers do not need an account for access
ProctorTrack[a]	The only app to continuously verify identity and provide browser lockdown during testing
TurnItIn	Plagiarism detection service, simple upload; compares uploaded student work to published articles and major journals, Wikipedia, and historical student submissions
UDoIt[b]	Open source, cloud-based Canvas plug in (learning technology integration) that allows institutions to create ADA accessible classes.

Abbreviations: ADA, Americans with Disabilities Act; LMS, Learning Management System.

[a]Indicates that we received returns on the vendor that controls the particular platform.

[b]Indicates that we did not receive open public records act returns.

As researchers, we hold a critical perspective which focuses our attention on power dynamics and institutional arrangements. To ensure an appropriate researcher standpoint, we collected documents from multiple sources to increase validity of the evidence base (Mcculloch, 2004). In Brown and Klein's (2020) study, we analyzed and coded documents individually, and discussed alignments and discrepancies. In so doing, we considered and reflexively discussed our subject positions and roles as researchers and stakeholders with relation to the inquiry (Glesne, 2014).

3.2 | Data collection

First, we compiled a list of 10 platforms based on those most widely used by the university, which we confirmed with the [anonymized for review] office of instructional development. See Table 1 for the list of vendors and value propositions as indicated by vendor product materials.

For each, we collected and analyzed publicly available general information on the vendors, their privacy policies, terms of service agreements, information security policies that were generally found as sub-sections of either privacy policies or terms of service agreements. We examined Securities and Exchange Commission Filings for those companies that are publicly traded and scoured the web for these vendor's labor practices to better understand how these companies operate and generate profit. Where applicable, we analyzed reputable news stories on controversy surrounding platforms and reviews of each platform from reputable sources on e-learning technology. We completed [State anonymized] OPRA requests for [University's] contracts for each platform in question as well as invoices and receipts for payments to these vendors for their services. Contracts and invoices for seven of the 10 EdTechs were returned via OPRA. Nonreturns are asterisked in Table 1. Our results comprise these seven EdTechs per Table 2 which includes available data source types—a census of the given sources available. In our capacity as AAUP-AFT representatives, we also spoke with university information technology service leaders to verify some of our factual observations, but these conversations are not included in our results here.

3.3 | Analysis

We analyzed the data attending to Feenberg's conception of stakeholder ecosystems, and CI's understanding of structural power as co-constitutive with technological processes, focusing on how these interrelated considerations manifest in the deployment of seven learning technologies. We employed three waves.

3.3.1 | Wave 1: Discerning vendor affordances and value propositions

Here we engaged in an inductive and deductive coding round analyzing product affordances. We selected the top e-learning vendors and reviewed product websites, exploring affordances for their value propositions to stakeholders, and general functionality (Table 1). Data sources used for this analysis mostly comprised "general online information" and "critical news sources." We then inductively generated an emergent set of categories as

TABLE 2 Available data sources by vendor

Vendor	General information	Privacy policy	Terms of service	Security	Labor	SEC filings and profit	Contracts	Invoices	Outside news sources	Other
Instructure Canvas	x	x	x	x	x	x	x	x	x	Reviews and internal community message board and letters
Verificient ProctorTrack	x	x	x	x		x	x	x	x	External reviews
Big Blue Button	x	x	x	x		x	x		x	External demos and reviews
Instructure Kaltura	x	x	x	x			x	x	x	
Respondus Lockdown Browser	x	x	x	x		x	x	x	x	External reviews
Microsoft	x	x	x	x		x	x	x	x	External reviews, internal blogs
TurnItIn	x	x	x	x		x	x	x	x	

TABLE 3 Wave 1 product affordances

Intro (or) what is it?
Solutions it provides
Stakeholder groups
Value proposition to each group
Similar tools
Technical aspects
How does it work? Algorithms, ML, datasets, etc.
Data management
Data collection
Data classification
Data storage
Data sharing and accessibility
User experience
User accessibility
User utility

TABLE 4 Categories used to analyze profit and policy, labor, and terms of service elisions and discrepancies, inherent within institutions and e-learning vendor relationships

Profit and policy
Affiliate companies
Relation to affiliates
Background and identity of C-suite and decision-makers
How are profits derived?
Profit trajectory
Value creation: Who and how
Labor
Training
Employee pay
Employee contracts
Working conditions
Terms of service
Privacy
Security
FERPA compliance

Abbreviation: FERPA, Family Educational Rights and Privacy Act.

codes in a large spreadsheet table, listed in Table 3 and analyzed each product, adding memos and notes for each category, across vendors. Our results helped us identify stakeholder data vulnerabilities given for instance vendors' stated data management practices.

3.3.2 | Wave 2: Analyzing profit, privacy, policy terms in e-learning vendor relationships

Waves 2 and 3 are informed by Brock's CTDA—a "bifurcated approach for studying Internet phenomena integrating interface analysis with user discourse analysis" (p. 1) that can be applied to critically analyze a plethora of ICT artifacts and platforms. For wave 2, we developed categories (Table 4) that help frame analysis on *who* benefits from these partnerships and *how*, as well as *who* stands the most to lose and *how*. For this wave, we drew upon mostly contracts, terms of service, privacy policies, and invoices, but also reviewed SEC filings and labor information, when it was available online. For the vendors in question, we compared data and privacy addenda tied to privacy clauses that are added to adhere to European General Data Protection Regulation (GDPR). We captured any GDPR-specific mentions in our summary reports, and then when comparing the clauses in the contracts we found no differences (between the website clauses and the contract clauses), and in all cases, the contracts referred us back to the website that mentions the privacy and data rights terms of service (ToS) clauses.

For each category, we analyzed existing sources by vendor and wrote notes indicating our observations, triangulating and verifying our observations across the three authors. The process resulted in 20 memos and notes, ranging from 500 to 2,000 words each. Across the seven vendors (and multiple data sources), our critical analysis memoing and notetaking round just for the categories listed in Table 4, averaged 300 words per vendor, with wide variation across each vendor, correlated to extent of data availability per Table 2.

We also wrote memos indicating gaps in data and what they implied. Overall, 60 of 105 total cells were filled with observational data fieldnotes, 35 of which constituted categories pertaining to internal labor conditions within the vendor companies—rarely disclosed by commercial entities. In the end, we only lacked data for 10 cells, not counting the labor category.

3.3.3 | Wave 3: CI Analysis and emerging categorical themes

In the third wave of analysis, we aimed to contextualize imbalances of power as demonstrated in the policy documents and synthesize these concerns into broader categories. In this work, we applied critical theory that attends to political economic power relations (Feenberg, 2017a; Harvey, 2003). We developed and used a list of question prompts (Table 5) to inform our interpretations of the notes and memos drafted across vendors, explained in Tables 3 and 4. These question prompts are adapted from [Author's] collaborative work on community tools to report police misconduct (Author, 2017), environmental justice databases, and serve as interpretive codes for synthesis of notes and memos.

As we completed this wave, we found that five main themes emerged, presented in the Results section.

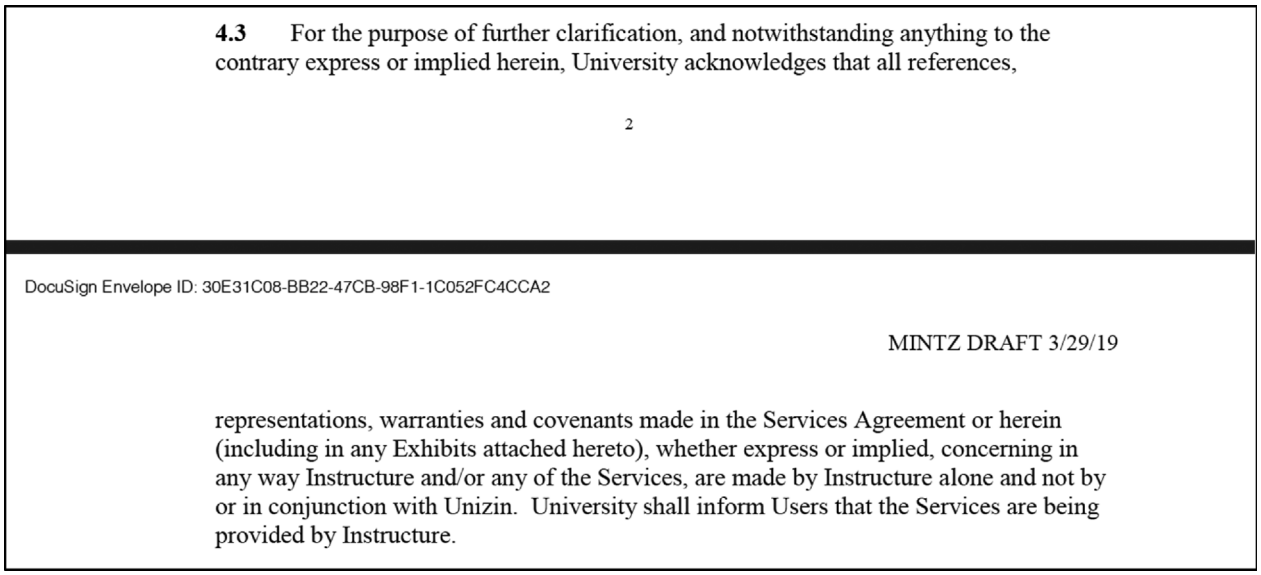
4 | RESULTS

Below, we elaborate each categorical theme, including illustrative evidence. Evidence shows how agreements between our university and the vendors in question leave a great deal of leeway to be exploited by these vendors, and possibly by vendors' third-party named and unnamed partners, or by the universities themselves (see Supplemental chart for expanded details).

4.1 | Opacity around vendors' use of data

This theme derived from language around data sharing and management, privacy policies, and user consent and refers to how each vendor discloses only minimal, opaque information as to how they use the data they collect from users. The publicly available information on how vendors use the data is sparse, opaque, and broadly permissive (Jones, 2019b; Jones, Rubel, & LeClere, 2020; Mittelstadt et al., 2016). The terms of service and university contracts with all seven platforms suggested that data are stored and shared, as indicated in our analyses of data storage, management, and sharing, but this information, as well as what they do with data and why, is vague, at best. Each vendor in our study indicated they have different infrastructural partners, like cloud hosting services. Three of the vendors in question, Canvas, ProctorTrack, and Big Blue Button stated they use Amazon Web Services for cloud hosting. However, across all platforms, details on what other entities user data are shared with beyond vague language around infrastructural "partners," as well as which specific data are shared, are left unarticulated.

For example, our university's contract with Instructure's Canvas exists in partnership with Unizin, a nonprofit technology consortium of universities, brought together to provide "data services, digital content solutions, vendor partners, and community" (Instructure and Unizin, 2019 p. 1). The data leveraged by this consortium of 25 U.S. HEIs are incredibly valuable for vendors (Jones, Rubel, & LeClere, 2020). The Unizin Canvas contract gestures toward the fact that



4.3 For the purpose of further clarification, and notwithstanding anything to the contrary express or implied herein, University acknowledges that all references,

2

DocuSign Envelope ID: 30E31C08-BB22-47CB-98F1-1C052FC4CCA2

MINTZ DRAFT 3/29/19

representations, warranties and covenants made in the Services Agreement or herein (including in any Exhibits attached hereto), whether express or implied, concerning in any way Instructure and/or any of the Services, are made by Instructure alone and not by or in conjunction with Unizin. University shall inform Users that the Services are being provided by Instructure.

the university enables Unizin "to provide certain proprietary and third-party services now and in the future to Unizin Members, including University" (Instructure and Unizin, 2019). However, in Section 4.2 of the contract, Unizin clarifies that it is *not* providing any services to [University]. Section 4.3 specifies that [University] is only supposed to state that the services are provided by Instructure, not in conjunction with Unizin, seemingly separating Unizin from services and data collection, see below:
(Instructure and Unizin, 2019)

In terms of data management and privacy, Section 11 of the contract notes that in case of termination of the contract with Instructure's Canvas and their dual contract with Unizin, the university will no longer be able to access or extract the data; not that the data will be removed, destroyed, or protected. Overall, these vague terms suggest that student and instructor data and metadata are being intentionally collected, stored, and used by Canvas' partnership with Unizin for various purposes, none of which are clearly delineated in the terms or contracts and thus are not enforceable. This is a cause for concern as Instructure has been sold to a private equity firm (Canvas Community & Concerned Stakeholders, 2019) notorious for exploiting valuable assets, like data, and simultaneously Instructure's Canvas has become the primary LMS at [University] phasing out other open-source competitors, namely, Sakai (Stiesi, 2018).

4.2 | Loopholes in FERPA compliance

Language in contracts between the university and the vendors around FERPA compliance suggested that the university misses opportunities to inform students and instructors of the ways their data can and will be used by vendors, neglects gathering meaningful consent from students and instructors, and allows vendors the legal loopholes to collect and store student data with impunity. As with Jones' (2019b) and Jones, Rubel, and LeClere's (2020) findings that EdTech FERPA compliance is uneven at best and negligent at worst, our analysis showed that EdTech systems' FERPA compliance is poor across the board. ProctorTrack and TurnItIn defer FERPA compliance to the student privacy pledge, an EdTech industry-branded student privacy pledge that skirts enforceable privacy requirements (Rubel & Jones, 2016), leaving the potential for vendors to exploit these poor protections. Kaltura documentation made no mention of FERPA compliance, but as it is a subsidiary of Canvas, we can extrapolate that its FERPA terms are similar to, or at the very least compatible to Canvas'. Respondus and Big Blue Button note that the institution is responsible for gaining consent of users. University contracts with EdTech

TABLE 5 Critical Informatics Analysis

Critical synthesis
What assumptions about exploitation exist?
Where is this demonstrated?
Who is harmed and how?
Other similar tools? Better or worse?
Risks and harms of data management?
Data management risks posed to whom?
Do risks and benefits of the technology found in policy language reify existing structures of power?
If the answer to the above is yes, then, how?

vendors allow FERPA compliance to be dissociated from university oversight, and release vendors from liability for privacy breaches. Strikingly, Canvas' FERPA compliance was at once poor, as they collect and share private data and metadata, while satisfying the law, because they use the school official exception loophole in FERPA. Another such example is Microsoft. As a technology company, Microsoft is widely understood to be among the best in terms of protecting users (Ranking Digital Rights, 2019). However, we see that there are glaring problems with how contracts with Microsoft understand and ensure privacy.

Microsoft complies with many global, national, and industry-specific privacy regulations, including Health Insurance Portability and Accountability Act (HIPAA), GDPR, and FERPA (Mazzoli, 2021). This declaration and admission that there are laws that must be adhered to makes it stand above the rest of the platforms we analyzed. However, we see that its compliance with FERPA is in its designation as a "school official" with "legitimate educational interests" in customer data that includes any records provided by the school's uses of Microsoft cloud services. It gives a range of types of personally identifiable information it collects and shares with its cloud hosting partners, which would generally be inadmissible under FERPA. Microsoft's terms of service make no mention of how their school official exception is defined or verified in any broad or specific agreements with institutions, or how violation of either party would be enforced. Moreover, it does not account for how the many sources of data it collects could be easily reaggregated to identify individuals.

In each case that admits to using the "school official exception" we contend, as Jones (2019b) does, that it is the university's responsibility to inform students and instructors of their terms with the vendors, and to allow them to consent to participation. This does not occur at the university in question. There are opportunities to institute a process by which this happens on a negotiated, case-by-case basis at the university.

4.3 | Terms of service and privacy policies release vendor from liability

Related to the loose and nonspecific language around FERPA, most of the terms of service and privacy terms completely released each of the EdTechs from liability for privacy breaches. While Microsoft is more explicit in their terms of service than the rest of the platforms we reviewed, they still leave a lot to be desired. Our findings that offload all liability to the student and the institution in their university contracts and publicly available terms of service were similar to Jones and his colleagues (Jones, 2019a; Jones, Rubel, & LeClere, 2020). For all vendors we analyzed, the vendor's terms of service noted that if anything went wrong, in the case of a security breach of the data or information shared with the vendor, the vendor would not be held liable.

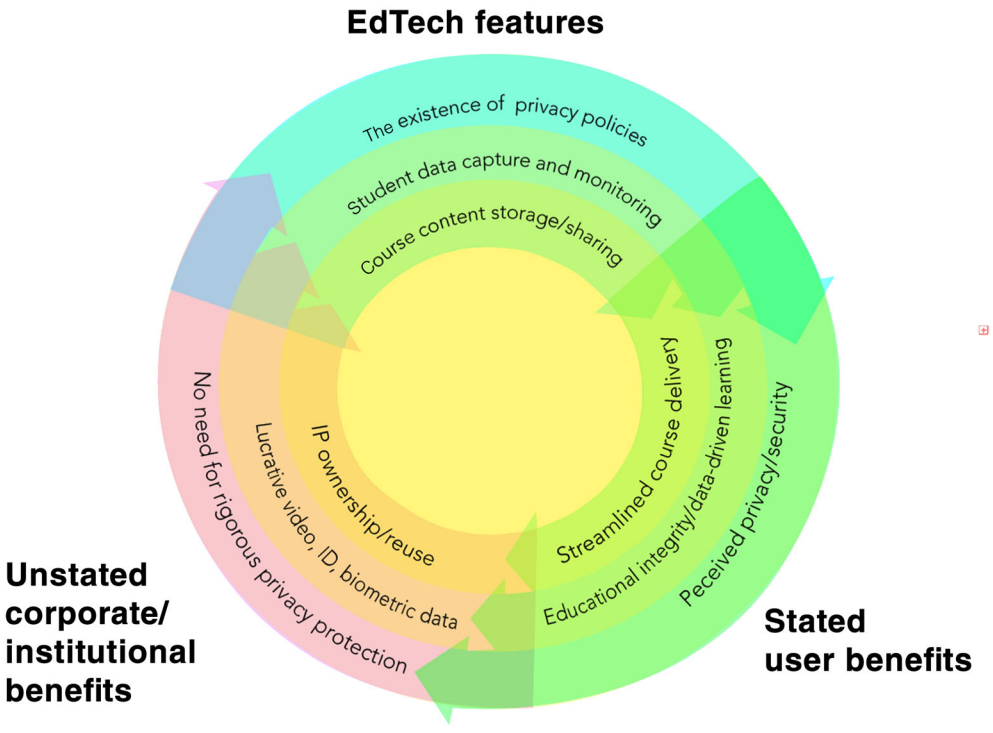


FIGURE 1 Cascading affordances flowing from and contributing to EdTech design [Color figure can be viewed at wileyonlinelibrary.com]

One such example is LockDown Browser contracted to the university through a surveillance company named Respondus that features both this application and test-taker monitor oversight. Lockdown Browser is capable of disabling broader functions of a student's computer and facilitates the ability for LockDown Browser to disable keyboard shortcuts, print screen functions, right-click, screen-sharing, remote desktops, dual screens, and messaging (Respondus, 2019). The only functions available within LockDown Browser are to navigate forward and backward within the exam, refresh a page, or stop. The student cannot exit the exam until it has been submitted for grading.

Respondus does not clearly provide terms of service for users of each of their products. Instead, it specifies terms of service only for Respondus Monitor (Respondus, 2021), an add-on to LockDown Browser. Monitor is a webcam feature that enables remote proctoring during an exam. To verify student identity, Respondus collects sensitive and personally identifiable "student information including name, grade, course name, and photos that show identification cards" (Respondus, 2021). Respondus Monitor's terms of service agreement specifies the role of the institution as the sole entity for addressing and holding liability for any privacy or security concerns of the student:

> e. DISCLAIMERS. Your Institution disclaims responsibility or liability for the accuracy, content, completeness, legality, reliability, operability or availability of information or data in the Respondus Monitor Service or Software. Your Institution further disclaims any responsibility for the deletion, failure to store, mis-delivery, or untimely delivery of any information or data. Your Institution disclaims any responsibility for any harm resulting from downloading or accessing any information or data through Respondus Monitor. You will bear all risk associated with any information or data you access. Your access or use of any information or data provided by Respondus Monitor or third parties is conditioned on your agreement to these Terms including these disclaimer provisions. Further disclaimers applicable to your relationship with your Institution, as well as with Respondus, are set forth below in the DISCLAIMER section under REQUIREMENTS OF RESPONDUS AND LICENSE PROVIDED BY RESPONDUS.
>
> (Respondus, 2021)

Beyond being a technology of surveillance that can be misused in a number of ways, Respondus' Lockdown Browser not only collects multiple types of private data, intellectual property, and even biometric data with impunity, beyond making these data available for research (Respondus, 2021), it is unclear how these data are used. Their nebulous terms of service puts the onus on the institution to get student and instructor consent for the undefined multiplicity of data they may collect. At [University anonymized], this consent is not collected, and if it is, it is not freely given.

4.4 | Questionable ownership terms around intellectual property

Language around data management and almost nonexistent language around intellectual property constitutes big questions for who owns and has rights to reuse student and instructor intellectual property.

A consistent finding in our analysis was that image data and audiovisual content, as well as student and instructor course content is easily collected and shared but not well-protected (Brown & Klein, 2020; Jones, Rubel, & LeClere, 2020). In the contracts and terms of service, Canvas states that "your content is yours", meaning users (students and instructors) can selectively allow access to their content to various other individual users, but they leave unsaid that as proprietors of the platform, Canvas always has access to the data and can do what they want with it. This is made clear as the contracts and terms of service state that content can be accessed by Canvas and their business affiliates. Moreover, the university can access instructor data at will (Brown & Klein, 2020). TurnItIn's terms state that copyright issues are avoided through the fair use clause within Section 107 of the U.S. Copyright Act. ProctorTrack, Lockdown Browser, and BigBlueButton, and Microsoft mention intellectual property only to note that content, image data, and states that audiovisual streams would be collected, stored, and shared with named and unnamed partners. This is a problem not only because it violates the privacy of user information and activity, the value generated from user information and activity can and likely will be used to enrich corporate owners and partners while foreclosing on alternatives that might better suit the needs of student and instructor users.

Our investigation raised a few interlocking problems in the realm of intellectual property in Kaltura, a cloud video software service that claims to create a virtual classroom. It allows both live video streaming and asynchronous video storage and use, and can be integrated with LMS such as Canvas, and others. Kaltura's privacy policy does not specify where data are stored or the specific duration for data retention. Kaltura's websites link to third-party apps, including social media platforms such as Facebook and Twitter. The terms note that information collected through these connections can be utilized for marketing purposes (Kaltura, 2020). Finally, educational institutions can create customized video portals to create a single portal for all archived videos called Kaltura MediaSpace Video Portal. Within the video portal, recorded videos are searchable, video galleries can be created, library content can be organized, and videos can

be broadcasted live and captured for storage. Access to this content can be managed by user type (domain, geolocation, IP addresses, internal networks) and by timeframe (always available, specific dates and times) (Kaltura, 2020) Instructors are never asked to consent to their intellectual property encapsulated in the video and virtual classroom data becoming property of the University, Kaltura, or being shared. Under these terms, one can see how an instructor's asynchronous virtual classroom or audiovisual materials could be reused by the university or third parties to create online courses that never have to credit or compensate the creator, as with the 2020 example of the professor whose video content was reused by the university even after he was deceased (Bartlett, 2021). There are no assurances otherwise.

4.5 | Insidious surveillance

Insidious surveillance derived from our focus on privacy terms, terms of service, and language around data management, and data sharing. The sharing of sensitive student data, specifically biometric and video data, and content, presents palpable problems standing in the way of data justice (Benjamin, 2019a; Browne, 2015; Dencik, 2016) because it invites surveillance of students and instructors. This surveillance may take the form of analytics-driven student "assessments" made available to instructors, as Canvas, TurnItIn, and ProctorTrack does, that can be misinterpreted and misused. Like Respondus' Lockdown Browser, ProctorTrack engages in explicit surveillance of remote student activity. As with Kaltura, it collects and stores video data, but does so in an acutely harmful application. ProctorTrack uses facial recognition technology, monitors student browsers, keystrokes, and hand placement to enable automated remote proctoring. ProctorTrack is like other remote proctoring systems as it offers several levels of intervention from basic browser locking to fully automated monitoring to live proctoring. The student is required to complete the onboarding process which entails creating a profile with a photo of the student, a photo of the student holding their student ID, and a photo of the student's knuckles—these elements serve to confirm the ID of the student for each test taken.

The instructor can specify the level of prohibitions during the test. These range from disabling copy and paste functions, the use of multiple monitors, requiring a room scan, and allowing tools such as calculators, books, notes, or earphones. Students can also be filmed via their webcam during the testing session for the ProctorTrack algorithm to review for violations. ProctorTrack records "1,800 impressions per minute" (Verificient Technologies, 2015) while the student completes a test; these impressions are analyzed by ProctorTrack's proprietary algorithms to identify potential instances of cheating. After a student has completed the test, a report of all flagged incidents or "violations" is created for review by the instructor. Verificient, like most companies complies with law enforcement investigations when subpoenaed; however, the granular detail that is recorded about students, for example, video data, ID information, and other biometric data, among all the other negative potentials for use of this technology and the data it collects. We question the ethical utility of any technology that could potentially be used to mis-judge or cause harm to students.

The egregious shortcomings in surveillance, privacy, and protection of intellectual property of the EdTechs in question found in the above analytical themes seven learning systems and software in this study suggest that for the most part, [anonymized] University has not deeply considered their contracts and affiliations with these market-driven solutions for online learning, or if they have performed some accounting of these systems, the documentation is nonexistent and suggests a lack of knowledge or interest around the various data justice issues that manifest in the way their agreements are structured at present.

5 | DISCUSSION

Even assuming the University's and the vendors' best intentions, our analysis of documents reveals persistent and harmful elisions of privacy protections. Jones' (2019a) indicates universities may choose to enter these contracts with vendors that remove mechanisms of dissent and refusal from students and instructors because these contracts are lucrative to universities and vendors. Our case study surfaces ample evidence that the institutional decision to pursue these contracts benefits vendors, while stripping students and instructors of privacy rights and self-determination over their own data and intellectual property rights, under the "school exception" loophole.

Klein's (2008) "shock doctrine" in the frame of the rhetoric of various crises of the university may access the deeper truth of how Harvey's (2003) technocratic rationality manifests in the privatization of public education in unfurling events such as the COVID-19 pandemic. Amid the subsequent 2020 civil uprising against racial injustice there has been a growing backlash against surveillance technology generally and facial recognition technology, as it disproportionately negatively affects people of color, women, and gender non-conforming people, is ineffective at detecting and identifying individuals, and is primarily used in military and law enforcement for the ends of control and punishment (Benjamin, 2019a; Browne, 2015). The continued institutional contract with ProctorTrack which

can be used to formally and informally control and discipline students and instructors (Jones, Asher, et al., 2020; Stark et al., 2020) causes us to question whether the university administrators are aware of or interested in remediating the severe data justice (Dencik et al., 2016) issues brought by surveillance and punishment technologies.

While we concur with Rubel, Jones, and Leclerc's (2020) assessment that student data collection and use must be rigorously guarded by HEIs as information fiduciaries, when considered from a CI-informed ecosystem approach, we propose that student data (metrics, bibliometric data, content) is just one consideration among many. Instructors and university staffers' data and intellectual property should also be rigorously protected and institutional and vendor roles in doing so must be defined explicitly vis-à-vis instructor rights to their own content.

Figure 1 below maps a generalized cascade of affordances building on Feenberg's notion of cascading innovations and social change (2019) and shows how "technocratic rationality" in e-learning further weakens already-tenuous student and instructor control over their educational practices. The mere existence of privacy policies sufficed for University administrators to accept these contractual terms. As a result, vendors are not compelled to reconceptualize their technical models that glean student and instructor data, monitoring, and course content and their business models that derive value from this data. Higher education's uncritical acceptance likely perpetuates this cycle of exploitation.

The epistemological frameworks used in CI center the needs and desires of those most harmed by the deployment of technological apparatuses to reconfigure sociotechnical systems (Collins, 1990; Noble, 2016). Users (students, instructors, staffers, and lower-level administrators) should be trusted to control their own involvement, which in some cases, might entail refusal, which should not come at the cost of participation outright. In that vein, Feenberg's (2017a) critical theory of technology supports calls for refusal and governance from the bottom-up, discussing how "cascades of innovations" reveal a negotiation among forces of influence that shape future affordances. This process may consolidate power for the already powerful; or it can be a juncture to change the distribution of power around a particular technology.

The mere existence of privacy policies, albeit poorly devised ones, seems to suffice for the university to enter contracts with EdTech vendors, and thus lacking specific, or in most cases, any terms, the vendors are never held to account. Promoting options for instructor and student self-determination in the negotiation of cascading affordances hold promise as Feenberg (2017a, 2017b), Selwyn (2012), and CI scholars (Benjamin, 2019a; Brock, 2018; Costanza-Chock, 2020; Hoffmann, 2019; Noble, 2016; Sweeney & Brock, 2014) show. There comes a point at which exploitative systems lose legitimacy as they reveal their nature (Feenberg, 2019), and the present may be such a moment. Rather than take a solely pessimistic perspective around the related problems of EdTech data privacy, ownership, surveillance, and control, we recognize that EdTech privacy is just one area in which various stakeholders can with intersecting, adjacent, and even oppositional interests can mobilize to deliberate on and push for innovative, ethical solutions. These problems of EdTech privacy might be a uniting interest that can draw various interest groups together—students, instructors, parents, Union leadership, state representatives, and even University administration in a constellation that could promote Selwyn's (2013) thin communitarianism for education. EdTech privacy might possibly be a topic that is well-suited for opening public deliberation across interest groups around the public role of education, and pushing for modest state and institutional support to promote public education, and to advocate for Feenberg's "technical citizenship" (2017a) where technological development and deployment value user self-determination, in this case, around privacy and related concerns, in the design and control of technical systems.

To this end, we propose a set of EdTech policy reforms that could be taken by our university, with the modest hope that, with more research and engagement in this area, such a model might serve for meaningful change across institutions. Groups of stakeholders should build upon known past measures to push for solutions that will facilitate student and instructor user groups' agency, such as:

- Establishing independent data privacy and protection boards that take an adversarial position in scrutinizing corporate contracts as already exist at other universities (Borgman, 2018) that give more transparent control over contracts to more diverse university stakeholders through democratic boards;
- Adopting opt-in informed consent for all participants and platforms; considering FERPA as a "floor, not a ceiling" (Jones, 2019b; Jones, Rubel, & LeClere, 2020) regarding mechanisms to protect privacy;
- Taking a proactive and courageous stance to ending state and corporate surveillance of students that includes refusal to enter exploitative contracts (Benjamin, 2019a; Gilliard, 2017; Selwyn, 2013; Swauger, 2020; Williamson, 2020); and
- Public subsidies and university support for research-based design work in educational technology to create small-scale, cooperative, open-source educational tools (Teasley & Kelly, 2020; University of Michigan IT Services, 2021).

While we see that many market-based e-learning systems are expensive, extractive, and opaque; smaller scale, more localized evidence-based systems can be more transparent and return agency to learners and instructors. Positive exemplars for such integrated approaches include the University of Michigan's design efforts, where Information Technology and Services (University of Michigan IT Services, 2021) features tools, apps, and dashboards developed by researchers at University Michigan's Institute for Data Science for university use such as the MyLA student dashboard which students control and use themselves for their own self-monitoring (Teasley & Kelly, 2020). Other positive exemplars include learning sciences advances occurring in the areas of Research Practitioner Partnerships (RPPs per Penuel & Gallagher, 2017) and design-based implementation research (per Fishman, Penuel, Allen, Ching & Sabelli,2013). These approaches emphasize designing learning innovations in deep collaboration with and in participation and consultation with education practitioners, for instance with solutions emerging collaboration with teachers, schools, districts, etc. at the K-12 level, who can be seen as more responsible privacy arbiters and institutional 'fiduciaries' acting in the interest of stakeholders if given this agency more deliberately, and in line with Rubel, Jones & LeClere (2020).

Following such examples, universities contribute to the public good by cultivating a technological design culture of meaningful engagement with users and emphasis on user self-determination that includes nuanced and well-informed discussions of exploitation and power, as well as the ability to refuse and dismantle harmful educational technology. Within these discussions, there are many questions of whose knowledge, needs, and power should be privileged and how to create a space in which these discussions can happen in meaningful ways that do not generate or compound harm (Collins, 1990; Costanza-Chock, 2020; Noble, 2016). These are conversations that higher education advocates should demand of our HEIs, and that we must participate in, while honoring that our voice is one of many.

6 | CONCLUSION

Our analysis indicates legitimate privacy concerns in our empirical site of exploration including issues of consent and data ownership across all platforms we reviewed, particularly with Canvas and Kaltura's vague terms around who has access to data and who can reuse that data and how, as well as ProctorTrack's invasive monitoring and lack of privacy assurances amounts to unwanted and unchecked surveillance. The possible harms of university and corporate exploitation of student and instructor data disproportionately impact individuals who are less powerful. We also highlighted policy conflicts including loopholes in federal laws and incompatibility among state laws around student privacy that makes it difficult to reign in corporate EdTech's questionable data practices. The analytical themes and implications found in this study at [anonymized] University suggest that reorienting this institution toward more thoughtful, people-centered, evidence-based, equitable, and sustainable learning analytics use, requires more robust intellectual property protections for students and instructors, and greater institutional transparency in all dealings, especially when it comes to student data.

Building from our analysis herein, our suggestions for institutional EdTech policymaking might include stipulations such as requiring meaningful university oversight and negotiation in contracts with EdTech vendors, and in some cases, refusal to participate with certain vendors unless the terms are changed to support the rights and needs of student, staff, and instructor users; university transparency about EdTech contracts and practices, and university accountability to stakeholders in decision-making around EdTech adoption and deployment. Fostering this type of oversight around EdTech is one step in the direction of reconfiguring a university system that serves and promotes the public interest.

Using the case study methodology, paired with a combination of PDA and CTDA allows us to see how political and economic power intervenes in agreements with seven major EdTech vendors as these technologies are deployed and used by one HEI. In this paper, we have shown a set of methods and considerations that can be used to do similar work within other institutions or that can be replicated to form the basis of comparative work across institutions. The insights we have gleaned here can be helpful in justifications for pushing back against the uncritical adoption of EdTech and could be replicated within individual HEIs or expanded upon to compare other institutions to uncover new or related problems, as well as to support or find novel solutions. Future critically engaged research might use subsequent analyses from across institutions and industries to build movements curtailing technology's reliance on market-driven ideals that lead to exploitative sociotechnical relationships. This demonstration of a CI approach is one of only a handful in this field, but as crises wear on and tech is positioned as the most logical or the only solution, these types of analyses are ever-more important.

REFERENCES

Allan, E. J., Iverson, S., & Ropers-Huilman, R. (2009). *Reconstructing policy in higher education: Feminist post-structural perspectives*. Routledge.

Britt, P., Dillon, L., Pierre, J., Pasquetto, I. V., Marquez, E., Wylie, S., Murphy, M., Brown, P., Lave, R., Sellers, C., Mansfield, B., Fredrickson, B., & Shapiro, N. (2017, September). Pursuing a toxic agenda. 100 days and counting, environmental data governance initiative. https://100days.envirodatagov.org/pursuing-toxic-agenda/

Bartlett, T. (2021, January 26). Dead man teaching. *The Chronicle of Higher Education*. https://www.chronicle.com/article/dead-man-teaching

Benjamin, R. (Ed.). (2019a). *Captivating technology: Race, carceral technoscience, and liberatory imagination in everyday life*. Duke University Press Books.

Benjamin, R. (2019b). *Race after technology: Abolitionist tools for the new Jim code* (1st ed.). Polity.

Besser, H., & Bonn, M. (1996). Impact of distance independent education. *Journal of the American Society for Information Science*, *47*(11), 880–883. https://doi.org/10.1002/(SICI)1097-4571(199611)47:11<880::AID-ASI14>3.0.CO;2-Z

Borgman, C. L. (2018). Open data, Grey data, and stewardship: Universities at the privacy frontier. *Berkeley Technology Law Journal*, *33*(2), 365–412.

Brock, A. (2018). Critical technocultural discourse analysis. *New Media & Society*, *20*(3), 1012–1030. https://doi.org/10.1177/1461444816677532

Brown, M., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. *The Journal of Higher Education*, *91*(7), 1149–1178. https://doi.org/10.1080/00221546.2020.1770045

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Canvas Community, & Concerned Stakeholders. (2019, December 26). *Letter to instructure*. https://ethicaledtech.info/wiki/Meta:Letter_to_Instructure

Collins, P. H. (1990). *Black feminist thought: Knowledge, consciousness, and the politics of empowerment*. Unwin Hyman.

Costanza-Chock, S. (2020). *Design justice: Community-led practices to build the worlds we need*. MIT Press.

Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *The University of Chicago Legal Forum*, *140*, 139–167.

Day, R. E. (2007). Kling and the critical: Social informatics and critical informatics. *Journal of the Association for Information Science and Technology*, *58*, 575–582. https://doi.org/10.1002/asi.20546

Dencik, L., Hintz, A., & Cable, J. (2016). Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, *3*(2), 1–12. https://doi.org/10.1177/2053951716679678

Dienstag, J. F. (2009). *Pessimism: Philosophy, ethic, spirit*. Princeton University Press.

Fairclough, N. (2013). Critical discourse analysis. In J. P. Gee & M. Handford (Eds.), *The Routledge handbook of discourse analysis*. Routledge.

Fallis, D. (2007). Toward an epistemology of intellectual property. *Journal of Information Ethics*, *16*(2), 34–51. https://doi.org/10.3172/JIE.16.2.34

Feenberg, A. (2017a). A critical theory of technology. In U. Felt, R. Fouché, C. A. Miller, & L. Smith-Doerr (Eds.), *Handbook of science and technology studies* (pp. 635–663). MIT Press.

Feenberg, A. (2017b). The online education controversy and the future of the university. *Foundations of Science*, *22*(2), 363–371. https://doi.org/10.1007/s10699-015-9444-9

Feenberg, A. (2019). The internet as network, world, co-construction, and mode of governance. *The Information Society*, *35*(4), 229–243. https://doi.org/10.1080/01972243.2019.1617211

Fishman, B. J., Penuel, W. R., Allen, A.-R., Cheng, B. H., & Sabelli, N. (2013). Design-Based Implementation Research: An Emerging Model for Transforming the Relationship of Research and Practice. *Yearbook of the National Society for the Study of Education*. 112, (136–156).

Gill, B., Coffee-Borden, B., & Hallgren, K. (2014). *A conceptual framework for data-driven decision making*. Mathematica Policy Research Reports https://ideas.repec.org/p/mpr/mprres/c811d94086af410aa2cf67190626c66f.html

Gilliard, C. (2017). Pedagogy and the logic of platforms. *EDUCAUSE Review*, *52*(4), 64–65.

Glesne, C. (2014). *Becoming qualitative researchers: An introduction* (5th ed.). Pearson.

Greene, D., Hoffmann, A. L., & Stark, L. (2019, January 8). Better, nicer, clearer, fairer: A critical assessment of the movement for ethical artificial intelligence and machine learning. Proceedings of the 52nd Hawaii International Conference on System Sciences. 2122–2131. https://doi.org/10.24251/HICSS.2019.258

Harvey, D. (2003). The fetish of technology: Causes and consequences. *Macalester International*, *13*, 1–29.

Haythornthwaite, C., Andrews, R. N. L., Fransman, J., & Meyers, E. M. (2016). Introduction. In *The SAGE handbook of e-learning research* (2nd ed., pp. 2–18). SAGE.

Hoffmann, A. L. (2019). Where fairness fails: Data, algorithms, and the limits of antidiscrimination discourse. *Information, Communication & Society*, *22*(7), 900–915. https://doi.org/10.1080/1369118X.2019.1573912

Hoffmann A. L. (2020). Terms of inclusion: Data, discourse, violence. *New Media & Society*, 32–48. http://dx.doi.org/10.1177/1461444820958725

Instructure and Unizin. (2019). *[Anonymized] University Canvas Unizin contract*.

Johnson, S. (2019, March 6). Turnitin to be acquired by Advance Publications for $1.75B. *EdSurge News*. https://www.edsurge.com/news/2019-03-06-turnitin-to-be-acquired-by-advance-publications-for-1-75b

Jones, K. M. L. (2019a). "Just because you can doesn't mean you should": Practitioner perceptions of learning analytics ethics. *Social Science Research Network*. https://papers.ssrn.com/abstract=3372591

Jones, K. M. L. (2019b). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education*, *16*(1), 24. https://doi.org/10.1186/s41239-019-0155-0

Jones, K. M. L., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (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*(9), 1044–1059. https://doi.org/10.1002/asi.24358

Jones, K. M. L., Rubel, A., & LeClere, E. (2020). A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal*

of the Association for Information Science and Technology, *71*(10), 1227–1241. https://doi.org/10.1002/asi.24327

Kaltura. (2020). Privacy policy. *Kaltura*. https://corp.kaltura.com/privacy-policy/

Klein, N. (2008). *The shock doctrine: The rise of disaster capitalism* (1st ed.). Picador.

Kling, R., & Iacono, S. (1988). The mobilization of support for computerization: The role of computerization movements. *Social Problems*, *35*(3), 226–243. https://doi.org/10.2307/800620

Lovink, G. (2012). *Networks without a cause: A critique of social media* (1st ed.). Polity.

MacKenzie, D., & Wajcman, J. (1999). *The social shaping of technology* (2nd ed.). McGraw Hill Education/Open University.

Marwick, A. E., & Boyd, D. (2014). Networked privacy: How teenagers negotiate context in social media. *New Media & Society*, *16*(7), 1051–1067. https://doi.org/10.1177/1461444814543995

Mazzoli, R. (2021). Compliance offerings for Microsoft 365, Azure, and other Microsoft services. *Microsoft*. https://docs.microsoft.com/en-us/compliance/regulatory/offering-home

Mcculloch, G. (2004). *Documentary research: In education, history and the social sciences* (1st ed.). Routledge.

Means, B., Toyama, Y., Murphy, R. F., & Baki, M. (2013). The effectiveness of online and blended learning: A meta-analysis of the empirical literature. *Teachers College Record*, *115*(3), 1–47.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. *Big Data & Society*. *3*(2), 1–21. https://doi.org/10.1177/2053951716679679

Newfield, C. (2016). *The great mistake: How we wrecked public universities and how we can fix them*. Johns Hopkins University Press.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2011). A Contextual approach to privacy online. *Daedalus Journal for the Academy of Arts & Sciences*, *4*(2011), 32–48.

Noble, S. U. (2016). A future for intersectional black feminist technology studies. *Scholar & Feminist Online*, *13*(3), 1–2.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism* (1st ed.). NYU Press.

Penuel, W. R., & Gallagher, B. J. (2017). *Creating Research-Practice Partnerships in Education*. Cambridge, MA: Harvard Education Press.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. *Social Studies of Science*, *14*(3), 399–441. https://doi.org/10.1177/030631284014003004

Polonetsky, J., & Tene, O. (2014). Who is reading whom now: Privacy in education from books to MOOCs. *Social Science Research Network*. https://papers.ssrn.com/abstract=2507044

Polonetsky, J., Tene, O., & Selinger, E. (2018). Consumer privacy and the future of society. *Social Science Research Network*. https://papers.ssrn.com/abstract=3158885

Popkewitz, T. S. (Ed.) (2018). Critical studies in teacher education. In *Its folklore, theory and practice*. Routledge. https://doi.org/10.4324/9780429450150

Ranking Digital Rights. (2019). *2019 ranking digital rights corporate accountability index*. Ranking Digital Rights https://rankingdigitalrights.org/index2019/companies/microsoft/index/

Regan, P. M., & Khwaja, E. T. (2019). Mapping the political economy of education technology: A networks perspective. *Policy Futures in Education*, *17*(8), 1000–1023. https://doi.org/10.1177/1478210318819495

Respondus. (2019). *Lockdown browser v. locked browser plug-ins: A bare knuckle fight*. https://web.respondus.com/wp-content/uploads/2019/07/ldb-vs-plugins.pdf

Respondus. (2021). Terms of use: Respondus monitor. *Respondus*. https://web.respondus.com/tou-monitor-admin/

Reynolds, R., Chu, S., Ahn, J., Buckingham Shum, S., Hansen, P., Haythornthwaite, C., Huang, H., Meyers, E. M., & Rieh, S. Y. (2019). Inaugural issue perspectives on information and learning sciences as an integral scholarly nexus. *Information and Learning Science*, *120*(1/2), 2–18. https://doi.org/10.1108/ILS-01-2019-138

Roberts, S. T., & Noble, S. U. (2016). Empowered to name, inspired to act: Social responsibility and diversity as calls to action in the LIS context. *Library Trends*, *64*(3), 512–532. https://doi.org/10.1353/lib.2016.0008

Rubel, A., & Jones, K. M. L. (2016). Student privacy in learning analytics: An information ethics perspective. *The Information Society*, *32*(2), 143–159. https://doi.org/10.1080/01972243.2016.1130502

Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., & Egelman, S. (2020). Disaster privacy/privacy disaster. *Journal of the Association for Information Science and Technology*, *71*(9), 1002–1014. https://doi.org/10.1002/asi.24353

Sawyer, S., & Eschenfelder, K. R. (2002). Social informatics: Perspectives, examples, and trends. *Annual Review of Information Science and Technology*, *36*(1), 427–465. https://doi.org/10.1002/aris.1440360111

Scheffel, M., Drachsler, H., Stoyanov, S., & Specht, M. (2014). Quality indicators for learning analytics. *Educational Technology & Society*, *17*(4), 117–132.

Selwyn, N. (2012). *Education and technology: Key issues and debates*. Continuum International Publishing Group.

Selwyn, N. (2013). *Distrusting educational technology: Critical questions for changing times* (1st ed.). Routledge.

Siemens, G. (2012). Learning analytics: Envisioning a research discipline and a domain of practice. *Proceedings of the 2nd International Conference on Learning Analytics and Knowledge* (LAK '12), 4–8. https://doi.org/10.1145/2330601.2330605

Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist*, *57*(10), 1380–1400. https://doi.org/10.1177/0002764213498851

Stark, L., Stanhaus, A., & Anthony, D. L. (2020). "I don't want someone to watch me while I'm working": Gendered views of facial recognition technology in workplace surveillance. *Journal of the Association for Information Science and Technology*. *71*(9), 1074–1088. https://doi.org/10.1002/asi.24342

Stiesi, R. (2018, November 8). Sakai, Blackboard to be phased out as Rutgers selects Canvas for official software. *The Daily Targum*. https://dailytargum.com//article/2018/11/sakai-blackboard-to-be-phased-out-as-rutgers-selects-canvas-for-official-software

Student Privacy Compass. (2021). *State student privacy laws*. Student Privacy Compass https://studentprivacycompass.org/state-laws/

Swauger, S. (2020). Our bodies encoded: Algorithmic test proctoring in higher education. *Critical Digital Pedagogy. Hybrid Pedagogy*. https://cdpcollection.pressbooks.com/chapter/our-bodies-encoded-algorithmic-test-proctoring-in-higher-education/

Sweeney, M. E., & Brock, A. (2014). Critical informatics: New methods and practices. *Proceedings of the American Society for*

Information Science and Technology, *51*(1), 1–8. https://doi.org/10.1002/meet.2014.14505101032

Teasley, S. D., & Kelly, H. (2020). How a new focus for learning analytics could transform the relationship between learning and employment. *Rapid Community Report Series*. https://repository.isls.org//handle/1/6848

Tsai, Y. -S., & Gasevic, D. (2017). Learning analytics in higher education – challenges and policies: A review of eight learning analytics policies. *Proceedings of the Seventh International Learning Analytics & Knowledge Conference*, 233–242. https://doi.org/10.1145/3027385.3027400

University of Michigan IT Services. (2021). *ITS teaching & learning group*. University of Michigan https://its.umich.edu/teaching-learning

US Department of Education. (2018, March 1). *Family educational rights and privacy act (FERPA)*. US Department of Education (ED). https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Vasalou, A., Joinson, A., & Houghton, D. (2015). Privacy as a fuzzy concept: A new conceptualization of privacy for practitioners. *Journal of the Association for Information Science and Technology*, *66*(5), 918–929. https://doi.org/10.1002/asi.23220

Williamson, B., Bayne, S., & Shay, S. (2020). The datafication of teaching in Higher Education: critical issues and perspectives. *Teaching in Higher Education*, *25*(4), 351–365. https://doi.10.1080/13562517.2020.1748811

Zalesne, D. (2013). Racial inequality in contracting: Teaching race as a core value. *Social Science Research Network*. https://papers.ssrn.com/abstract=2511405

Zeide, E. (2017). The structural consequences of big data-driven education. *Social Science Research Network*. https://papers.ssrn.com/abstract=2991794

SUPPORTING INFORMATION

Additional supporting information may be found in the online version of the article at the publisher's website.

How to cite this article: Paris, B., Reynolds, R., & McGowan, C. (2021). Sins of omission: Critical informatics perspectives on privacy in e-learning systems in higher education. *Journal of the Association for Information Science and Technology*, 1–18. https://doi.org/10.1002/asi.24575