

6-22-2020

Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents

Michael Brown

Iowa State University, brownm@iastate.edu

Carrie Klein

George Mason University

Follow this and additional works at: https://lib.dr.iastate.edu/edu_pubs



Part of the [Curriculum and Social Inquiry Commons](#)

Recommended Citation

Brown, Michael and Klein, Carrie, "Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents" (2020). *Education Publications*. 192.

https://lib.dr.iastate.edu/edu_pubs/192

This Article is brought to you for free and open access by the School of Education at Iowa State University Digital Repository. It has been accepted for inclusion in Education Publications by an authorized administrator of Iowa State University Digital Repository. For more information, please contact digirep@iastate.edu.

Whose Data? Which Rights? Whose Power? A Policy Discourse Analysis of Student Privacy Policy Documents

Abstract

The proliferation of information technology tools in higher education has resulted in an explosion of data about students and their contexts. Yet, current policies governing these data are limited in their usefulness for informing students, instructors, and administrators of their rights and responsibilities related to data use because they are based on antiquated conceptions of data and data systems. To understand how data privacy policies conceptualize and represent data, privacy, student agency, and institutional power, we conducted a policy discourse analysis of 151 university policy statements related to student information privacy and the responsible use of student data from 78 public and private post-secondary institutions in the U.S. Three common discourses emerged: educational records are static artifacts, privacy solutions are predicated upon institutional responsibility and student agency, and legitimate educational interest in data are institutionally defined and broadly applied. We explore the assumptions, biases, silences, and consequences of these discourses and offer counter-discourses to begin a foundation for the development of privacy policies in a new data age.

Keywords

Learning analytics, student data, student privacy policy, FERPA, GDPR

Disciplines

Curriculum and Social Inquiry

Comments

This is a manuscript of an article published as Brown, Michael, and Carrie Klein. "Whose data? which rights? whose power? A policy discourse analysis of student privacy policy documents." *The Journal of Higher Education* 91, no. 7 (2020): 1149-1178. Posted with permission. See supplemental files at the bottom of the page for index.

Introduction

In the last decade, the rapid development of information technology has resulted in an explosion in information about students, their behaviors, and their contexts, what is often referred to as learning analytics (LA) data (i.e., educational big data; Society for Learning Analytics Research [SOLAR], 2018). Data mining techniques and the use of LA based technologies has made it possible for vast amounts of student data – within and beyond the classroom - to be harvested, stored, analyzed and repurposed. Both the production and the consumption of LA data have transformed organizational practices, opening pathways for new kinds of data collection, analysis and reporting that were previously impossible (Picciano, 2012). As a consequence “social actors can now use more data, can use it in targeted ways and in real-time” (Souto-Otero & Beneito-Montagut, 2016, p. 18) to improve organizational processes and outcomes. Analytic tools that predict grades, academic difficulty, or suggest majors allow institutions to shape and even constrain individual decision-making (Klein & Brown, 2019).

The expansion of data collection, storage, and computational capacity by post-secondary institutions has occurred alongside the rise of accountability movements, academic capitalism, and marketization as driving ideologies in American higher education (Fisher, Metcalfe, & Field, 2016; Slaughter & Rhoades, 2004). Within this context, neoliberal governance of educational organizations is enacted through numbers, where institutions reduce “complex processes to simple numerical indicators and rankings for purposes of management and control” (Shore & Wright, 2015, p. 22). This dependency on quantitative data to know and report is tied to neoliberal tendencies to view technology as a superior objective mechanism for improving organizations (Harvey, 2007).

LA initiatives are data hungry, pushing institutions towards new and expanding data collection activities. Institutions can now collect data beyond classroom and learning management systems (LMS) to include tracking of student interaction locations, campus services and resource

use, and co-curricular engagement (e.g. Bowman et al., 2019). Information systems, by their nature, implicate organizations and their actors in the process of data collection and analysis in order to “monitor, regulate, and sanction” individual and institutional action and outcomes (Rutledge, 2013, p. 215). This big data approach to managing the educational enterprise potentially underestimates the social context of education and the complexity of student lives (Selwyn, 2019). Data driven systems may “exacerbate discriminatory decision-making in favor of those social groups most represented in the systems’ datasets” (Selwyn, 2019, p. 13).

This expansive accumulation of data about students and their contexts plays into an age-old dilemma in American civil society over the struggle between the rights of the individual and the needs of social institutions: how one should be known and what of ourselves we have the autonomy to reveal and conceal (Igo, 2018). How students become known by the institution and what institutions do with those representations occurs with little student engagement (Johnson, 2018), and few privacy policies exist that specifically address what data are being collected from students and how that data are being used to inform organizational processes and outcomes. Rather, data privacy policies governing student data collection and use have lagged behind technological and cultural changes in higher education (Prinsloo & Slade, 2016), perhaps in part because of decreased participation in institutional governance (Kezar & Eckel, 2004) and an increase in the managerial class in higher education who rely upon data (Slaughter & Rhoades, 2004).

Given the changing nature of modern data collection toward LA technologies and the movement by higher education institutions toward the investment of time, energy, and capital in LA initiatives, a better understanding of the scope, protections, limitations, and potential harm of current privacy policies in the age of datafication is needed (Slade & Prinsloo, 2013; Steiner, Kickmeier-Rust, & Albert, 2016). The purpose of this study is to understand how postsecondary institutional data privacy policies conceptualize and create discourses that represent data and privacy.

Through this process, we aim to uncover how institutions' interest in expanding student data records complicates a student's ability to control how they will be known by the institution, and the ways through which data collection and analysis may create the potential for differential harm.

Using policy discourse analysis (PDA), we identified the hidden assumptions, silences, and unintended consequences within data privacy policies (Allan, 2008; Bacchi, 1999; Blackmore, 1999), that prescribe or limit individual agency and magnify institutional power.

We used the following guiding questions:

1. How are data and data privacy conceptualized in policies governing student data?
2. What privacy policy problems and solutions are represented in these policies?
3. How are the roles, responsibilities, power, and agency of students, institutions, and other relevant actors represented in policies governing student data?
4. Which discourses are employed to shape these images, problems, and solutions? Which are absent?

Background

Parents, students, and policymakers have long been concerned with how educational institutions record information. The original Family Education and Privacy Rights Act (FERPA) was prompted not by concerns about disclosure of student information, but rather fears of “secret gatekeepers, arbitrary categorizations, and bureaucratic errors that, unchecked, could become permanent liability” with the goal of limiting the amount and kinds of information that could end up in a student's file (Igo, 2018, p. 250). The closed and cloaked nature of educational records presented a concern for students and parents. Inaccurate information or biased judgements about students would linger as educational data creating a ‘records prison’ that follows students throughout their school career, surveilling their actions and informing their access to educational opportunity (Igo, 2018).

The implementation and subsequent revisions of FERPA has asserted a role for the institution as a steward of records and clarified that students' primary role is in ensuring accuracy of their records and determining what, when, and with who the institution can disclose information (Parks, 2017). The exception to students' consent to disclose is when institution's purport a legitimate educational interest in the record. Over time

large-scale data collection and analysis has become so commonplace in higher education that escaping it entirely is nearly impossible. Participation in the system of higher education in the United States now implicitly requires that students consent to sharing their personal information with third parties with little transparency or control over their own information. Big data and learning analytics continue to shift the balance of power over student privacy away from students and toward institutions (Parks, 2017, p. 27)

Institutions are left to make determinations about what is legitimate, what is educational, and what students need to be informed about, without student participation in that decision making.

With the advent of LA tools and LA driven interventions, institutions potentially place even more faith in the role of educational data for organizing student life. For example, researchers at the University of Arizona have developed a machine learning model to predict student retention based on trace data from student identification card swipes. Researchers aim to use this data to develop 'targeted interventions' based on a students' daily routines (Blue, 2018). Identifying students' potential to be retained from how and where they show up in data systems requires students to conform to normative patterns of engagement where stepping out of the digital ecosystem could have consequences which are not communicated to students.

The disciplinary potential of big data technologies is expressed through what Anagnostopoulos, Rutledge, and Jacobsen (2013) call informatic power. Informatic power combines both strategic and logistic power as it ties systems of incentives and sanctions to measurement and computing technologies (Anagnostopoulos, et al., 2013). Mathematical models and computing

technologies produce performance measures that appear transparent—as objective representations of the “complex process of teaching, learning, and schooling” (Anagnostopoulos, et al., 2013, p. 7).

Yet, algorithmic measures are often imbued with bias and the potential for misuse and harm. The most egregious recent example of the expression of informatic power in American higher education was Mount Saint Mary’s president Simon Noonan’s plan to use predictive LA to “drown the bunnies” by encouraging students identified as at risk to withdraw early in the year (Johnson, 2018, p. 135). Noonan resigned from his position soon after his comments were revealed, but the potential still exists for institutions to classify students in ways that limit agency and infringe on students’ ability to determine how they should be known by the institution.

Noonan’s approach is an extreme manifestation of the way that analytic technologies are used to shape student behavior. Although often referred to as nudging, these strategies more closely resemble a digital practice of redlining students’ educational opportunity structures (Gilliard & Culik, 2016). Digital redlining involves “a set of education policies, investment decisions, and IT practices that actively create and maintain class boundaries through strictures that discriminate against specific groups” (n.p.). Similar to the ways that redlining created material physical difference in access to institutions like schooling through restricting home ownership, institutions can use digital data to “reinforce the boundaries of race, class, ethnicity, and gender” (Gilliard & Culik, 2016, n.p.). Through course recommender and early warning systems, institutions can direct students to behaviors that improve institutional outcomes at a potential cost to individuals’ autonomy and self-determination. These patterns can reflect biases about race and gender without incorporating data about students’ identities as in the recent controversy over the Apple card approving women for systematically smaller lines of credit (Knight, 2019).

Digital redlining, like other forms of algorithmic discrimination, happens in ways that are hidden from the view of students within the black box of data collection and analysis. Digital

redlining is a reflection and extension of the ways that race, property, and oppression are intricately linked in the formation and function of American higher education institutions (Patton-Davis, 2016). Throughout their history, American higher education institutions have “enacted normalizing judgements” by restricting student movement and engaging in surveillance of student behavior in order to produce docile student bodies, efforts that disproportionately impact minoritized students (Stewart, 2017, p. 1043).

Ruha Benjamin (2018) refers to the digital technologies that sort, rank, and distribute institutional resources as the “anti-Black box.” Anti-Black box technologies link “the race-neutral technologies that encode inequity to the race-neutral laws and policies that serve as powerful tools of white supremacy” (p. 62). The outcomes of these technologies- the classifications and recommendations they make- appear objective, but are founded upon discriminatory historical data and reflect the bias of their technical designers. “Database design,” Benjamin (2018) asserts, “is an exercise in worldbuilding” (p. 145). But rarely are students invited into the decision-making process regarding the institutional worlds they inhabit or the surveillance systems that increasingly inform those worlds. Anti-Black box technologies draw upon the sociotechnical networks of people, policies, and technologies which facilitate measurement, evaluation, and governing that reinforce existing institutional logics of extraction and accumulation for marketization and commercialization (e.g. Benjamin, 2018; Cohen, 2018; Zuboff, 2015). As a consequence, institutional actors can (mis)use data to create inequitable interventions and outcomes (including tracking students into specific courses, curricula, fields, and pathways) based on the encoded biases of anti-Black box technologies.

Few recourses appear to exist for individuals to protest these systems and their reach. However, recent work on data justice has sought to create mechanisms through which organizations and individuals can pushback against the dominance of socio-technical systems. Data justice

illuminates the structures like embedded norms, opportunities, and privileges that can be “perpetuated, exacerbated, and mitigated by information systems” (Johnson, 2014, p. 272). This perspective and a recent framework for its use by Taylor (2017), allows organizations and individuals to identify desired and equitable outcomes and craft responses to data use and collection. Taylor’s (2017) data justice framework is based on three pillars: visibility of technical systems, voluntary engagement with technology, and non-discrimination. These pillars focus on issues of informatic power by encouraging organizations to establish policies and practices that ensure individual access to information, representation, and privacy (e.g., how individuals are represented, profiled, and surveilled as a part of categorized groups); to ensure individual autonomy in technology-related choices (including the choice not to use or be used by technologies) and in sharing in the benefits of data collection and use; and to ensure the ability and power of individuals to challenge and be free from algorithmic bias.

The pillars of data justice are a necessary, but often missing component in organizational policies. Given higher education’s inherent duty of care towards its students, crafting institutional policies that reflect principles of data justice is a necessary corrective (Prinsloo and Slade, 2015). If we use LA data as part of our educational missions, than the duty of care should be extended to the collection, use, and policies that govern students’ LA data.

Conceptual Framework

To provide a foundation for this study, we relied on policy discourse analysis (PDA) and the emerging literature on data politics and data governance (e.g. Ruppert, Isin, & Bigo, 2017; Selwyn, 2015, 2016; Williamson, 2016). PDA allows for a better understanding of “the discursive shaping of policy problems” and “how embedded assumptions may contribute to consequences of policy solutions that may not have been explicitly intended” (Allan, Iverson, & Ropers-Huilman, 2010, p. 3). The literature related to the emergence of data politics in social life helps conceptualize the

unique and evolving social dimension of LA and underscores the need for new approaches to the privacy policies that govern post-secondary use of student data.

Methodological Tradition: Policy Discourse Analysis

PDA is a hybrid methodology that employs critical discourse and textual analysis techniques from post-structuralist and feminist perspectives, allowing for deeper and more complex understandings of the embedded meanings in policy texts (Allan, 2008, 2018). Discourses are artifacts of language, both written and spoken, that produce and are produced by the contexts in which they exist (Allan, 2008). These socially constructed texts create boundaries for individuals through which they are able to interpret, make sense of, and react to environmental contexts. Through subject positions (e.g., conceptual identities, narratives, or repertoires created for individuals through discourse) practices emerge within educational policies that profoundly influence individual cognition and action and highlight the ways that power functions in post-secondary institutions by drawing attention to what is stated and what is not (Allan, 2008; Mills, 1997). Policies and their associated discourses are not neutral. Rather, they mirror the environments in which they exist, resulting in policies that are imbued with social ideologies, inequities, and imbalances (Allan, 2008).

Allan (2008, 2018) argues that the benefit of PDA is that it can illuminate and problematize taken-for-granted policy problems and solutions to encourage change and social justice by working to understand, emancipate, and destabilize postsecondary policies (p. 40). PDA identifies and critiques dominant social structures that influence policy and discourse development, as a means toward emancipating policies and leveraging empowerment and equity among individuals working within those policies and their structures. Policies are generally considered to be “the dynamic and value-laden process through which political systems operate to solve problems at the institutional level” (Allan, Iverson, Ropers-Huilman, 2010, p. 4). Understanding the discourses that policy

documents generate can illuminate organizational thinking, and in this case, the institutional politics of post-secondary data governance.

Guiding Perspective: Data Politics

We approach the study of policy (and policy language) as a system of social organization (Martinez Alemán, 2015). Through policy we can identify the ways that institutions organize some issues into institutional politics and organize others out of political contest (Pusser, 2015), in part through the enactment of strategic and logistic power in policy language. Data politics draws our attention to the political struggle between institutions and students over the collection and use of an individual's data, regardless of whether that struggle is represented as political in policy language. This contest is not benign as the extractive function of analytic technologies is to produce a surplus of behavioral data which can be converted (and repurposed) into predictive products that shape individual action as determined by technological and institutional actors (Zuboff, 2015; Zuboff, 2019), leaving unresolved the rights and entitlements of students to their representations. Whether students enter into this relationship as equal partners is a matter of policy, but more often these relationships do not result in an even value exchange (Zuboff, 2019). The logic of data extraction prioritizes the goals of the organization and sidesteps the regulatory role of the state and pressures from social movements by keeping extraction and harm hidden from view (Zuboff, 2019).

The architecture of institutional data systems and the normative practices of judgement about students they facilitate happen in the background of institutional life (Williamson, 2018). Informatic power and the attendant logic of accumulation of data that it requires (Zuboff, 2015),

determines what is measured, and what is passed over; how resources and people are allocated and organized; who is valued in what roles; what activities are undertaken – and to what purpose. The logic of accumulation produces its own social relations and with that its conceptions and uses of authority and power (p.75).

The data politics that emerge in this moment are concerned with the political struggle over data production and the impact of datafication on individual and collective work. Data politics as an

analytical framework trains our attention to three areas: the apparatus of data assemblage (Dixon-Román, 2016), the experiences of data subjects (Ruppert, Isin, & Bigo, 2017), and the hidden architecture of datafication (Williamson, 2018). The apparatus of data assemblage we focus on in this study is organizational policies governing data use. The individual subjected to the consequences of data work- the focal data subjects- are students. Through our analysis we identify the power relations embedded in the hidden architecture of data work by considering the apparatus and the subject.

Methodology

We conducted a PDA of 151 university policy statements related to student information privacy and the responsible use of student data from 78 public and private post-secondary institutions in the U.S. We collected texts from member-organizations of the American Association of Universities (AAU), the University Innovation Alliance (UIA), and from participant institutions of the 2016 Convention for Learning Research in Higher Education (CLRHE) focused on Student Data and Records in the Digital Era. We included these organizations in our sampling strategy because research universities in the AAU often set the template for academe (Bok, 1990), and because UIA members have committed to using student data to improve student success, which often involves sharing educational records. We expected institutions belonging to any of the three groups (there was overlap, see appendix A) to be engaged in internal conversations about student privacy and responsible use of student data. We did not include Canadian and British institutions who were part of these groups, as they were not subject to U.S. privacy regulations related to educational records.

Texts for this study included organizational policy statements related to data privacy, use, storage, and access (see appendix B). Texts were obtained from institutional websites and student handbooks. All institutions had a publicly available version of at least one of the documents. For

institutions that did not have all documents on their website (or where conflicting versions of the document were available) the first author contacted an institutional representative to clarify if additional resources were available. Policies collected included FERPA, the European Union's recent General Data Protection Regulation (GDPR), and internal governance documents that outlined how institutional data was to be managed. The majority of documents were FERPA related ($n=81$). Rarely, an institution would have more than one FERPA policy for different audiences (i.e. parents, students, faculty). We reviewed 54 policies that provided targeted guidance either for students or faculty and staff about the implications of GDPR implementation for data privacy. The remainder of the policies described data governance plans, procedures, and related roles ($n=16$). Many documents overlapped. Often FERPA language was included within a data governance documents describing how and why data were restricted.

Per the norms of PDA and of qualitative inquiry, we systematically coded texts (Allan, 2008; Saldaña, 2015, Strauss & Corbin, 1990) using the qualitative analysis software system, Dedoose. We used Allan's (2008) three-phase PDA analytic coding process that uses a "multilayered approach that examined presences as well as absences in the text" through deductive and inductive coding (p. 58). We were able to compare how and how often policy language and terms were used within and across policies and institutions. Initial deductive coding was informed by our research questions and existing literature and theory. Our second round of inductive coding was informed by the deductive codes and emergent from new insights and absences we discerned via initial analysis (see appendix C). Code examples included: policy problems, solutions, student consent, institutional responsibility, pro-forma language, institutionally focused messaging and student agency. From these codes, we created themes related to data and data privacy discourse representation, positionality, production, and absence that we describe in the findings section of this paper.

Credibility and Validity

To address credibility and validity, we employed a number of methods. We worked to collect documents from multiple sources to understand and consider the contexts informing the study (McCulloch, 2004). We analyzed and coded documents texts separately to determine where there was alignment or discrepancy in our interpretation of the data and our analysis (Patton, 2002). After we completed our initial coding, together we reviewed those codes and discussed our interpretations of them. Finally, we worked to both consider and take into account our lenses as researchers, our subject positions related to the inquiry, and our roles as research instruments by engaging in ongoing and reflexive conversations related to our analysis and interpretation of the data (Glesne, 2006).

As researchers, we hold a post-modern perspective on organizational theory and organizational work in higher education. We are also interested in interrogating learning systems and their analytical applications, which naturally trains our attention on power dynamics and individual/institutional tensions. We come to this research as insiders- former practitioners in assessment and evaluation and in project management and policy development, which shapes where and how we look for data discourses.

Limitations

The study is limited to the documents we collected, which, as is the nature of document analysis studies, may not provide a holistic view of higher education organizational conceptions of data and data privacy. Also, our analysis of the data privacy documents in this study is influenced by our positionality as researchers. As discussed, our post-modern epistemological perspectives influence our interpretation of these documents and the discourses, representations, and productions therein. Finally, the documents we analyzed are specific to the organizations we included and therefore not generalizable beyond this specific analysis. That being said, the findings from this study provide useful insight into the ways in which data and data privacy are conceptualized, represented, and promulgated in postsecondary settings.

Findings

We identify three subject positions that create narratives and repertoires for institutional work and student experiences related to data privacy. We also identify two silences that align institutional practices with the expression of informatic power. We illustrate the subject positions followed by the dominant silences that exist in the policy documents to draw attention to the ways that institutions have crafted student data privacy policy discourses to provide significant latitude in determining how students are known and how that knowledge is acted upon. The political contest over an individual's right to be known by the institution leaves institutions with significant power and resources and individual's with little ability to push back on institutional policy, data collection and surveillance. We argue that the subject positions and silences that are present in current privacy policies work as sensemaking mechanisms that shape organizational members' conceptions of data privacy and its boundaries and that create the potential for privacy violations and harm.

Subject Positions

The various subject positions we identified speak to the bureaucratic nature of data privacy policies. Our findings indicate that privacy policies are rooted in outdated assumptions related to data collection and use in higher education and fail to recognize the changing nature of data and privacy issues in modern higher education. Specifically, current data privacy policies position students as informed, agentic partners in their education; position data as static artifacts to be managed by the institution; and positions data stewardship as a means of protecting the institution against risk and liability. While seemingly benign, within the complex environment of higher education and given the changing nature of data collection and use in higher education, these subject positions limit student agency, obscure data realities, and favor institutional over individual interests.

Subject position #1: Students are informed agentic partners. In policies, students are described as informed, agentic, and “full partners in the educational enterprise” (Brandeis

University). Texas A&M University asserts that they “operate under the premise that the educational process is a cooperative venture between a student and the University.” Students are empowered to provide or withhold consent in some circumstances and to initiate grievances related to their records. Institutions are charged with responsibilities related to the protection of student data including informing students and staff about FERPA and managing access to student data (including exceptions to consent).

These images of students as partners belie the fact that, through policy, students’ agency is often limited to ensuring that their education records are accurate, whereas institutional responsibility has a broader reach and assumes student understanding of their rights. Institutions are empowered to make choices about when and where consent is required for data release. Further, through their collection and storage of data institutions become *de facto* custodians in perpetuity of expansive digital records. It is unclear if students would consent to any or all of their information being stored indefinitely (even beyond their active relationship with an institution) if they were more clearly informed. For example, very few policies describe when, where, and how data are collected and converted into educational records, or if records might ever be destroyed.

No policies described how students could participate in governance of student data/educational records. Instead, students’ rights were individual and described their ability to interface with the institution. Politics are elided here, as an interest group (students) is decomposed into individual actors. Individuals can control some aspects of how they are known by the institution, largely as a result of public policy like FERPA or GDPR, but are not afforded the opportunity to determine how students- as an interest group- are able to control how they become known.

For example, the University of Kansas identifies multiple ways through which a student becomes known to the institution, “Information may be collected in a variety of ways, paper or

electronic, including but not limited to, Web sites, surveys, email, information requests, databases, etc., as required to support University activities.” The policy reports that:

Information collected, regardless of the method of collection or format, may be used only to carry out the authorized business of the University. The University shall make reasonable efforts to limit the Private Information it collects to only that information strictly relevant to accomplish a clearly defined institutional purpose.

However, the process by which an informed agentic student partner might contribute to identifying a clear, defined institutional purpose is not addressed. Similarly, the institutional purpose is not articulated. The intent of these documents focuses less on helping students understand their rights and outlining their methods for redress and more on explaining to internal stakeholders how student privacy was institutionally constructed. Many institutions used legalistic and opaque language in their policies (e.g., ‘promulgated’), which potentially limits students’ ability to participate as equal partners in the management of their data.

It is also worth noting that students are treated rather monolithically as informed agents. The policy literature contains no recognition, that we observed, that students might have different kinds of relationships to institutions and that institutional legacies of access and equity (or lack thereof) might create partnerships that are more or less complex. To acknowledge that data collection and archiving facilitates the kind of surveillance that allows for digital red lining, for example, impacting different groups of students in differentiated ways, would require an acknowledgement that student-institution relationships are lopsided and biased.

Subject position #2: Data are represented as static institutional artifacts. Most often policies represented data as a static artifact of the relationship between the student and the institution. UC Davis provides a common definition of an education record, stating that it pertains to any data generated from students "in their capacity as students." Data becomes a student record through its relationship to educational practices and experiences. In traditional legacy systems, these

data were often limited to demographic, admissions, enrollment, and performance data stored on an institutional mainframe.

Institutions treat nearly all aspects of student life (e.g., course work, employment, mental health, and campus involvement) as relevant educational experiences. Unlike in legacy systems, contemporary data analytics systems allow for every engagement with digital tools to produce trace records of student behavior, including location and engagement data from internet protocol (IP) pings and identification card swipes. Some FERPA and responsible use of data statements acknowledge that this ambient data collection occurs, placing surveillance data from a mouse-click within the same realm as individual educational records; however, most do not.

Policy documents most often represented educational records as historical and summative in nature, and as an institutional responsibility (and arguably a burden) to be managed. These policy representations are still rooted in legacy conceptions of data, meaning that there was an absence of policy language geared towards the realities of modern data work. Only a few institutions already engaged in the development of enterprise level LA initiatives, like ASU, Georgia State University, and Pennsylvania State University, stated that predictive testing based on student data could be used both internally and in partnership with external actors. In general, statements that spoke to the specific management needs of modern data systems were limited as were statements that acknowledged the speed and volume with which student data are collected.

Compounding how data are conceptualized and represented is how those conceptions and representations are communicated via data policies. Data protection policies were generally written with institutional actors in mind, rather than students. Meaning that, even among statements in student-targeted venues, like student handbooks, it was rare for institutions to acknowledge that they retained data indefinitely or to explain for what purposes that data might be used.

Moreover, legacy policies do often not acknowledge how non-legacy analytics data are used in practice. Arizona State University (ASU), which is engaged in a number of data-driven initiatives, provides an atypical example of a policy acknowledging that educational records and data traces may be subjected to subsequent analytics. “Logs of [user behavior] information may be retained. We may contract with non-ASU service providers to help us better understand Users.” For ASU, like many other higher education organizations, LA data are no longer merely static records, rather they are resources that can be recombined, repurposed, and reused to inform institutional priorities long after a student has left an organization.

The other exception in the policy corpus was the supplemental notices or institutional guidance produced in response to the GDPR. In nearly all of the policy documents, institutions went to great lengths to explain why students were not subject to these regulations. This was surprising, as nearly all of the AAU institutions either had students, faculty and staff from the European Union (EU) or programs and campuses that were housed within the EU. We expected that public policy would prompt some reflection and revision of institutional policy given this reality. The one significant change we observed in policies that were revised after the enactment of the GDPR was the way in which students were discursively represented. In these documents, the source of data are often referred to not as a student (or even an individual), but as a ‘Data Subject’ (language most likely lifted from the EU’s GDPR). University of Illinois provides a prototypical example in their supplemental notice related to the GDPR policy, “you are a ‘Person’ or ‘Data Subject’—meaning a natural person, not a corporation, partnership or other legal entity” (p. 1).

To be a Data Subject, individuals simply need to interact with an organization in a way that produces data. That data becomes an artifact that can be moved around the organization, doing different kinds of organizational work, creating logistical challenges and liabilities, independent of the person. In this process ‘you, a person’ becomes the subject of data work (Ruppert, et al., 2017).

However, subjects, as opposed to students or persons, have different rights and entitlements in policy documents. When institutions view individuals as ‘subjects’ they inevitably flatten out representations of those individuals, relying upon aggregated representations of individuals (Scott, 1998)- treating students as an aggregate. Subjects- in the sense of governance- do not participate in politics in the same way as citizens do (Scott, 1998), nor would they be able to leverage the pillars of data justice. The flattening out of student representation through conceptualizing data as a static record is tied to institutional considerations of risk and liability, because this discourse works to separate data from its subject (i.e., students) by making these data de-contextualized resources to be managed.

Subject position #3: Data are resources with risk and liability to be managed. Although institutions express a need for data about students to fulfill their educational mission, in policy documents data were discursively represented as resources containing risk and liability to be mitigated. Data were appended a variety of descriptive labels to classify their potential level of risk to the institution. Data are regulated or unregulated, restricted or unrestricted, sensitive or suitable for directories. FERPA policies often specify remedies for how students can manage the disclosure of unregulated data, like directory information, or instances where the student can direct the institution to share restricted data with other organizations or individuals, but the situations in which redress is possible are narrowly defined and therefore presumably rare.

Risk for or from what is rarely specified, despite the real material consequences to the institution and to individuals that might come from disclosure of sensitive information. Iowa State, for example, describes sensitive information that is nonetheless shared with different actors. Data could be shared that is otherwise restricted because, “the Data Governance Committee determined that [restricting access]...would significantly reduce faculty/staff/student

effectiveness when acting in support of Iowa State University's mission." Attention to student risk is attenuated by the utility of the data to the institution.

Having established a problem of liability and risk, institutions solve this problem by expanding the administrative class, assigning responsibility to Data Privacy Offices or Officers (DPOs). Stanford University's Privacy Office identifies their primary objective as "protect[ing] the integrity of data collected, created, transmitted, released and stored by Stanford affiliates and entities" (Stanford, n.d.). It is worth drawing attention to this distinction- that the office protects the integrity of data and not individuals. Privacy offices were rare - more common was a privacy officer within the unit of the chief information or technology officer. While these roles in their mission acknowledged students as key stakeholders and stakeholder engagement in data governance, the focus in policy documents involved how data was accessed and shared, rather than the implications for students of data use. This makes intuitive sense as institutional agents are charged with protecting the interests of the institution. The location of these offices also potentially trains privacy officers' attention on information technology resources, health information (in systems with hospitals and medical schools), and intellectual property rights.

Silences

We now turn our attention to the silences we observed in the policy documents. First, policies are silent on why students should be known to the institution. For what purpose should students be potentially put at risk? Second, we observe a the contrast between how data systems are often conceptualized as static and how they are enacted as dynamic technologies. A focus on silences allows us to understand how privacy policies work to protect institutions and position them with power while limiting protections for students and their data and creating the potential for harm, especially among students who are the target of digital redlining and anti-Black box technologies.

Silence #1: Why should students be known? For what legitimate interest? Left unaddressed in the policy documents we reviewed was the compelling institutional interest for pervasive data collection and archiving. If data presents a liability to the institution and the student, there must be a countervailing rationale for why the institution needs to acquire this data and why students (despite the potential risk of disclosure) should willingly participate in systems of data collection. The historical approach to data collection and archiving closely aligns with the credentialing and accreditation process. Institutions needed to be able to accurately identify students and accurately represent their institutional accomplishments. However, in the era of surveillance capitalism, neo-liberal logics of accumulation and extraction encourage institutions to expand what they collect, store, and act upon (Zuboff, 2019). In higher education's current accountability context, there is an increasing desire and sense of responsibility to know and to measure student interactions as a means to better inform institutional outcomes (Hora, Bouwman-Gearhart, & Park, 2017). However, to acknowledge that a logic of accumulation is guiding organizational work and priorities would be to betray other institutional responsibilities, like the duty of care that institutions have towards their students (Prinsloo & Slade, 2017; Slade & Prinsloo, 2015).

The lack of clear purposes for data extraction also creates space for the kind of anti-Black box technologies that purport to make data objective and actionable. If institutions do not enumerate their purposes, than a technology of questionable utility (and ethics) cannot be excluded from use on a policy basis. Anti-Black box technologies exacerbate existing practices of white supremacy and minoritization, producing differential outcomes for Black, Latinx, AAPI, Indigenous students, and any other group outside algorithmic norms (e.g. Eubanks, 2018; Noble, 2018). Policies may treat students monolithically, but their effects are differentiated and exacerbated by existing inequity.

Without clear boundaries around when, where, and with whom student data will be shared, an expansive definition of legitimate educational interest in student records emerges in the policy documents. This expansive definition of legitimate interest inevitably results, even among institutions with data governance plans and privacy officers, in power imbalances between LA users (i.e., institutions) and its producers and subjects (i.e., students). Further, while institutions give access to student data to legitimate actors (a term coined but not defined by FERPA legislation), students do not have clear rights to control that access and use. Specifically, the rights to control whether and how they are represented, to participate in informed engagement, and to be free from discriminatory algorithms, interventions, and outcomes – tenets of data justice for those whose data are used and acted upon (Taylor, 2017) – are limited or absent in current policy.

In the policies we reviewed, nearly any institutional actor, even a third-party vendor, has a legitimate educational interest in student data. Arizona State University¹, for example, provides a wide cross spectrum of users with legitimate educational interest access to dashboards that aggregate and visualize data about students and their behaviors (see Wishon and Rome, 2012, for a discussion). Throughout the FERPA documents we reviewed, we observed no demarcation or categorization between what is and what is not ‘legitimate’.

A typical example is provided by Northwestern University where determinations about legitimate educational interest are:

made by the person responsible for the maintenance of the record. This determination will be made scrupulously and with respect for the individual whose

¹ Arizona State University belongs to the small group of institutions who employed Chief Information Security officers or Chief Privacy Officers. These institutions tended to have policies that offered more diverse representations of data privacy, student privacy rights, and clearer policies for how students can manage their data concerns. Institutions like Stanford and University of California, Los Angeles, who both employed Privacy Officers, made a distinction between data, educational records, and students’ privacy rights concerning both. Educational records, per FERPA, were part of the larger data governance process but were subject to distinct (and more stringent) forms of scrutiny in the approval request process than other forms of data.

records are involved. “A legitimate educational interest” requires that the individual seeking access is doing so for the purpose of performing a job function.

Such an approach might seem unnecessarily broad, but as Pennsylvania State University asserts, institutions need to balance the rights of individuals with “the institution’s need for relevant information to the fulfillment of its educational missions.” This tension, between the needs and perspectives of the institution versus those of the individual, occurred throughout the documents and across institutions. The existence of this tension and the absence of clarity regarding who has access to and ownership over institutional becomes more problematic when how that data are used is also obscured.

Silence #2: Legacy representations, dynamic systems. Within the corpus of policy documents, there was little discussion of contemporary forms of data use. Instead, the representations of data in the policies we reviewed treat data as static objects. Data are stored, maintained, and accessed through a laborious process in policy document representations. The FERPA policy at John Hopkins University suggests the university will:

decline to make copies of education records when the parent of a student and/or a student lives within a normal commuting distance from the school and when the task of preparing copies presents itself as unduly burdensome or interferes with the normal duties and operations of personnel.

Such an approach envisions records in their physical form, the reproduction of which is time consuming. Nowhere in policy documents did we observe discussion of the kinds of technologies used to capture, store, or analyze data about students and their behaviors. Institutional data servers, trace data, and ambient data collection about student behavior through the use of card swipes and two factor authentication - while pervasive on most campuses- are not represented in the policy literature we reviewed.

The portrait of data systems presented in the policy literature - even legacy systems - is incomplete. All of the policies we reviewed represent what is possible among institutional actors (e.g., students, FERPA stewards, registrars, and institutional researchers). This narrow focus on

social interactions over technological systems misses the practices and harms that technology can afford individual actors. Policies at most describe student redress processes, the timeframe for university response, and the possible outcomes of the process. These requirements are often statutory details translated for a local FERPA or GDPR policy. Student agency is limited to the period after harm has occurred.

What most institutions and their policies avoid is an acknowledgement that campuses are now data rich environments, where interactions with nearly any aspect of institutional life produces a data trace that is captured as part of the dynamic ongoing educational record. Beyond how these data are used, policies also avoid discussions of what relationship these data have to the user, what entitlements or rights to the data exist, and where data are housed and for what duration. This reality makes impossible student engagement with technology - a pillar of data justice (Taylor, 2017) – and the subsequent right to determine whether, how, and if their data are used.

Discussion

Current data policy realities result in what Ruppert and colleagues (2017) refer to as the uneven negotiation of data politics. Student data policies become an artifact of the ways in which informatic power between students and institutions is unevenly distributed, even when policies explicitly outline students' rights and responsibilities as stewards of their data. Without insight into how their data are being used, students have no ability to object (or to organize their objections) because the potential targets of those objections are obscured. Institutions structure the architecture of data work (and data systems) in such a way that they are invisible to students (Williamson, 2018), which makes criticizing or pushing back against data work difficult.

We entered into this work hoping to better understand the ways that student privacy and student data were discursively represented in policy documents in an age of datafication and LA adoption. Returning to our guiding research questions, students are represented in the policy corpus

as informed agentic partners, and data privacy is represented primarily as a concern of the institution, not the individual. Privacy problems and solutions are designed to respond to static legacy data systems. Roles, responsibilities, power, and agency of students, institutions, and other relevant actors are often left unaddressed, unless specified under federal or international law. For example, it is unclear what role students can have as informed agentic partners in the educational enterprise when the enterprise is increasingly organized around practices and policies that facilitate data extraction, occurring far from view.

While other political contests within the institution (like debates about curriculum, representation, and access) may result in visible expression of concern and organizing, expressions of informatic power are designed to appear like the way of things. Policies work to organize contests about data and student data representation out of institutional politics. The current arrangement of collection, analysis, and archiving of student data are so abstracted from the campus life it informs that the actions outlined in policies appear as non-decisions - byproducts of the taken for granted status quo (Pusser, 2015). We argue this invisibility is intentional, violates the visibility tenet of data justice, and disproportionately affects minoritized students.

The policies we reviewed rely upon discourses to mobilize informatic power on behalf of institutional interests. Across the corpus of policy documents, the social aspects of data were depoliticized. To acknowledge that data extraction and use was a political activity would mean that institutions would also need to acknowledge connected forms of harm that students are potentially subject to- the normative judgements that constrain student choice and position marginalized students as outliers. Enumerating the ways that institutions would attempt to prevent digital redlining would require an acknowledgement of white supremacy, the dereliction of a duty of care that institutions have to students, and the increased role that marketization and commercialization play in all aspects of campus life.

As Ruppert, Isin, and Bigo (2017) assert, data enacts that which it represents. When data become part of the architecture of institutional life, it enacts institutional power. To acknowledge that a problem exists with the way that informatic institutional power is expressed is to allow for a solution within governance systems. Both institutional and public policy documents lack meaningful enforcement provisions (Parks, 2017) leaving institutions the space to accrue power and act upon students. This is not a new problem, but we argue it is a problem exacerbated through datafication. Students are described as equal partners, but are provided no discursive methods for redress. Data politics are organized out of institutional data policies, despite an acknowledgement that collecting data produces risk and that data use requires the expansion of the administrative ranks to manage data resources.

The emergence of a logic of data extraction over the last decade has produced a “new social relations and politics that have not yet been well delineated or theorized” (Zuboff, 2015, p. 76). Current policy language provides space for institutions to engage in uneven value exchanges. LMS and advising management tools often do not provide students the option to opt out of data collection nor do any of the policies we reviewed. As institutions increasingly focus on their ability to control risk and position themselves for competition in student choice markets (Slaughter & Rhoades, 2004), the ability to develop (and eventually commercialize) student data as a commodity encourages the extraction of information regardless of students’ preferences. Students, who have little control over their data or their representations, are potentially the “raw material awaiting commodification in an emerging political economy of informational capitalism” (Cohen, 2018, p. p 213).

Our work suggests that institutions have not revised their policies in ways that reflect current practices of data use. By failing to develop policies that engage with the political dimensions of data use, institutions further the depoliticization of data use as the “modern technological society renders

all ideology obsolescent” (Hall, 2017, p. 87). Politics are reduced to the given state of affairs, and grievances are private and discrete matters (Ferguson, 2018). There is no space for a true governance process in these policies because policies are silent on violations of an individual’s right to privacy. As a consequence, for example, marginalized, minoritized, and historically underrepresented campus groups, who are more likely to be subjected to normative system of judgement (Stewart, 2017) through anti-Black box technologies have no enumerated policy concerns to resist against. Students must do the work of naming and claiming their concerns in order to resist institutional expression of informatic power.

Implications for Organizational Practice and Policy

Our analysis suggests that organizations should revise their data governance and use policies to represent data systems as they are. From a duty of care and with data justice in mind, students should be centered in the development of data privacy policies and practices. Institutions must make data extraction and use visible, ensure that students are able to control how they engage with technology, and work towards systems, policies, and networks that operate from a starting point of non-discrimination (Slade & Prinsloo, 2015; Taylor, 2017).

In their recent global guide on ethical use of LA data, Slade and Tait (2019) coalesce the core principles established over 10 years of LA research on various emerging codes of practice, foregrounding the importance of transparency, student agency, and inclusion. This guide acts as a useful tool for institutions and institutional stakeholders seeking to improve equitable LA use and to address issues of legitimate interest and representation. This work is achievable, as collaborative Data Governance councils currently exist, like those developed at Vanderbilt University and the University of Michigan. Through collaborative governance, institutions need to draw clear boundaries around what constitutes legitimate interest and

who is a legitimate actor. Just systems move toward inclusion by providing data producers (i.e., students) the opportunity to understand and to have control over their level of engagement with data systems and to opt out of systems of judgement like predictive analytical tools. Head, Fister, and MacMillan (2020) with Project Information Literacy provide useful guidance in this area, demonstrating why and how information literacy is increasingly an essential skill for democratic citizenship.

Just data systems also reflect and prevent the disproportionate potential for harm from administrative violence that systems of judgement present for minoritized Students of Color, Queer, Trans*, non-binary, and gender non-confirming students (among many others, i.e. Spade, 2015). Instead of policies that minimize the complexities of students and their data by reducing them to student data subjects, policies should explicitly acknowledge inequality and enumerate the ways in which institutions work to prevent harm from algorithmic decision-making. Institutional actors must work to learn about how algorithmic bias and digital redlining can create the potential for harm by engaging with current research and supporting investigation of their data structures and solutions.

Conclusion

Institutions could (and should) acknowledge the material role that data and data collection, analysis (specifically algorithmic decision-making), and use play in the governance of student life. Doing so requires institutions to acknowledge the informatic power imbalance between institutional data users and student data subjects. Unquestioned data systems and their outputs allow anti-Black box technologies that reside on historical policies of anti-Blackness and white supremacy to persist. We build campus life, in part, through institutional databases and the tools of judgement that they service- this is a new form of institutional world-making (e.g. Benjamin, 2019). As Dixon-Román (2016) argued, “if software have become the engines of society and algorithms do the ‘thinking’

(Manovich, 2013; Parisi, 2013), then data have become the information for algorithmic cognition” (p 7). The longer that institutions try to mask their thinking, especially their biases, from students the greater the potential for harm.

References

- Allan, E. J. (2008). *Policy discourses, gender, and education: Constructing women's status*. New York, NY: Routledge.
- Allan, E.J. (2018, April). *Power, discourse, & institutional policy: discourse analysis in higher education research*. Symposium conducted at the AERA 2018 Annual Meeting in New York, NY.
- Allan, E. J., Iverson, S., & Ropers-Huilman, R. (Eds.). (2010). *Reconstructing policy in higher education: Feminist poststructural perspectives*. New York, NY: Routledge.
- Anagnostopoulos, D., Rutledge, S. A., & Jacobsen, R. (2013). *The Infrastructure of Accountability: Data Use and the Transformation of American Education*. Harvard University Press.
- Bacchi, C. L. (1999). *Women, policy and politics: The construction of policy problems*. Sage.
- Benjamin, R. (2019). *Race after technology: Abolitionist tools for the new Jim Code*. John Wiley & Sons.
- Blackmore, J. (1999). Troubling women feminism, leadership and educational change.
- Blue, A (2018). Researchers look at digital traces to help students. UANews. Retrieved from <https://uanews.arizona.edu/story/researcher-looks-digital-traces-help-students>. on November 11, 2019.
- Bok, D. C. (1990). *Universities and the future of America*. Durham, NC: Duke University Press.
- Bowman, N. A., Jarratt, L., Polgreen, L. A., Kruckeberg, T., & Segre, A. M. (2019). Early identification of students' social networks: Predicting college retention and graduation via campus dining. *Journal of College Student Development*, 60(5), 617-622.
- Cohen, J. E. (2018). The biopolitical public domain: the legal construction of the surveillance economy. *Philosophy & Technology*, 31(2), 213-233.
- Dixon-Román, E. (2016). Algo-ritmo: More-than-human performative acts and the racializing assemblages of algorithmic architectures. *Cultural Studies? Critical Methodologies*, 16(5), 482-490.

- EDUCAUSE. (2019, January 29). *Improving data management and governance in higher education*. Retrieved from: <https://www.educause.edu/guides/improving-data-management-and-governance-in-higher-education>
- Eubanks, V. (2018). *Automating inequality: How high-tech tools profile, police, and punish the poor*. St. Martin's Press.
- Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 CFR Part 99 (1974).
- Ferguson, R. A. (2018). *One-dimensional Queer*. John Wiley & Sons.
- Fisher, D., Metcalfe, A. S., & Field, C. (2016). The structural force exerted by marketization on higher education systems, research universities and academic researchers. In *Routledge handbook of the sociology of higher education* (pp. 63-73). Routledge.
- Gilliard, C., & Culik, H. (2016). Digital redlining, access, and privacy. *Common Sense Education*. Retrieved from <https://www.common sense.org/education/articles/digital-redlining-access-and-privacy>. on November 11, 2019.
- Glesne, C. (2006). *Becoming qualitative researchers: An introduction* Boston.
- Hall, S. (2017). Political Commitment. In S. Davison, D. Featherstone, M. Rustin, and B. Schwarz (Eds.), *Selected Political Writings: The Great Moving Right Show and Other Essays* (pp. 85–106). Durham, NC: Duke University Press.
- Harvey, D. (2007). *A brief history of neoliberalism*. Oxford University Press, USA.
- Hora, M. T., Bouwma-Gearhart, J., & Park, H. J. (2017). Data driven decision-making in the era of accountability: Fostering faculty data cultures for learning. *The Review of Higher Education*, 40(3), 391-426.
- Igo, S. E. (2018). *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press.
- Johnson, J. A. (2014). From open data to information justice. *Ethics and Information Technology*, 16(4), 263-274.

- Johnson, J. A. (2018). *Toward Information Justice*. Springer.
- Kezar, A., & Eckel, P. D. (2004). Meeting today's governance challenges: A synthesis of the literature and examination of a future agenda for scholarship. *The Journal of Higher Education, 75*(4), 371-399.
- Klein, C. and Brown, M. (April 2019). Student Privacy in the Age of Big Data. *NACUBO Business Officer Magazine*. Washington, D.C.: National Association of College and University Business Officers
- Knight, W. (2019). The Apple card didn't 'see' gender- and that's the problem. *Wired Online*. Retrieved from <https://www.wired.com/story/the-apple-card-didnt-see-genderand-thats-the-problem/> on November 23 2019.
- Manovich, L. (2013). *Software takes command* (Vol. 5). A&C Black.
- Martínez-Alemán, A. M. (2015). Critical discourse analysis in higher education policy research. in Martínez-Alemán, A. M., Pusser, B., & Bensimon, E. M. (Eds.). (2015). *Critical approaches to the study of higher education: A practical introduction*. JHU Press. 7-43.
- McCulloch, G. (2004). *Documentary research: In education, history and the social sciences*. New York, NY: Routledge.
- Miles, M. B., Huberman, A. M., Huberman, M. A., & Huberman, M. (1994). *Qualitative data analysis: An expanded sourcebook*. Sage.
- Mills, S. (1997). *Discourse*. London, UK: Routledge.
- Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. nyu Press.
- Parisi, L. (2013). *Contagious architecture: computation, aesthetics, and space*. MIT Press.
- Parks, C. (2017). Beyond compliance: Students and FERPA in the age of big data. *Journal of Intellectual Freedom and Privacy, 2*(2), 23.

- Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*, 1(3), 261-283.
- Patton, L. D. (2016). Disrupting postsecondary prose: Toward a critical race theory of higher education. *Urban Education*, 51(3), 315-342.
- Picciano, A. G. (2012). The Evolution of Big Data and Learning Analytics in American Higher Education. *Online Learning*, 16(3). <https://doi.org/10.24059/olj.v16i3.267>
- Prinsloo, P., & Slade, S. (2013, April). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. In *Proceedings of the third international conference on learning analytics and knowledge* (pp. 240-244). ACM.
- Prinsloo, P., & Slade, S. (2015, March). Student privacy self-management: implications for learning analytics. In *Proceedings of the fifth international conference on LA and knowledge* (pp. 83-92). ACM.
- Prinsloo, P., & Slade, S. (2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, 3(1), 159-182.
- Prinsloo, P., & Slade, S. (2017). Big data, higher education and learning analytics: Beyond justice, towards an ethics of care. In *Big data and learning analytics in higher education* (pp. 109-124). Springer, Cham.
- Head, A.J., Fister, B., MacMillan, M. (2020, January 15). Information literacy in the age of algorithms. *Project Information Literacy*. Retrieved from: <https://www.projectinfolit.org/>
- Pusser, B. (2015). A critical approach to power in higher education. in Martínez-Alemán, A. M., Pusser, B., & Bensimon, E. M. (Eds.). (2015). *Critical approaches to the study of higher education: A practical introduction*. JHU Press. 7-43.
- Ruppert, E., Isin, E., & Bigo, D. (2017). Data politics. *Big Data & Society*, 4(2), 2053951717717749.
- Saldaña, J. (2015). *The coding manual for qualitative researchers*. Sage.

- Scott, J. C. (1998). *Seeing like a state: How certain schemes to improve the human condition have failed*. Yale University Press.
- Selwyn, N. (2015). Data entry: towards the critical study of digital data and education. *Learning, Media and Technology*, 40(1), 64-82.
- Selwyn, N. (2019). What's the Problem with Learning Analytics?. *Journal of Learning Analytics*, 6(3), 11-19.
- Slade, S., & Prinsloo, P. (2013). Learning analytics ethical issues and dilemmas. *American Behavioral Scientist*, 57(10), 1510-1529.
- Slade, S., & Tait, A. (2019, March). *Global guidelines: Ethics in learning analytics*. Oslo, Norway: International Council for Open and Distance Education.
- Slaughter, S. A., & Rhoades, G. (2004). *Academic capitalism and the new economy: Markets, state, and higher education*. Baltimore, MD: Johns Hopkins University Press.
- Stewart, D. L. (2017). Producing 'docile bodies': disciplining citizen-subjects. *International Journal of Qualitative Studies in Education*, 30(10), 1042-1046.
- Society for Learning Analytics Research [SOLAR]. (2018). *About SOLAR* [webpage]. Retrieved from <https://solaresearch.org/about/>
- Souto-Otero, M., & Beneito-Montagut, R. (2016). From governing through data to governmentality through data: Artefacts, strategies and the digital turn. *European Educational Research Journal*, 15(1), 14–33. <https://doi.org/10.1177/1474904115617768>
- Spade, D. (2015). *Normal life: Administrative violence, critical trans politics, and the limits of law*. Duke University Press.
- Steiner, C. M., Kickmeier-Rust, M. D., & Albert, D. (2016). LEA in private: a privacy and data protection framework for a learning analytics toolbox. *Journal of Learning Analytics*, 3(1), 66-90.

- Strauss, A., & Corbin, J. M. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA: Sage Publications.
- Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*, 4(2). <https://doi.org/10.1177/2053951717736335>
- Williamson, B. (2016). Digital education governance: An introduction. *European Educational Research Journal*, 15(1), 3–13. <https://doi.org/10.1177/1474904115616630>
- Williamson, B. (2018). The hidden architecture of higher education: building a big data infrastructure for the ‘smarter university’. *International Journal of Educational Technology in Higher Education*, 15(1), 12.
- Wishon, G. D., & Rome, J. (2012). Enabling a data-driven university. *EDUCAUSE Review Online*.
- Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), 75-89.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.