JOURNAL OF LEARNING ANALYTICS

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Student Vulnerability, Agency, and Learning Analytics: An Exploration

Paul Prinsloo
University of South Africa, South Africa
prinsp@unisa.ac.za

Sharon Slade
The Open University, UK
sharon.slade@open.ac.uk

ABSTRACT: In light of increasing concerns about surveillance, higher education institutions (HEIs) cannot afford a simple paternalistic approach to student data. Very few HEIs have regulatory frameworks in place and/or share information with students regarding the scope of data that may be collected, analyzed, used, and shared. It is clear from literature that basic opting in or out does not sufficiently address many of the complex issues in the nexus of privacy, consent, vulnerability, and agency. The notion of vulnerability (institutional and individual) allows an interesting and useful lens on the collection and use of student data. Though both institutional and individual vulnerability need to be considered, this paper focuses specifically on *student* vulnerability. In this conceptual article, we explore student vulnerability in the nexus between realizing the potential of learning analytics; the fiduciary duty of HEIs in the context of their asymmetrical information and power relations with students; and the complexities surrounding student agency in learning analytics. This article expands on an earlier framework developed by Prinsloo and Slade (2015). It aims to explore ways to decrease student vulnerability, increase their agency, and empower them *as participants* in learning analytics — moving them from quantified data objects to qualified and qualifying selves.

Keywords: Agency, ethics, informed consent, learning analytics, opt out, opting out, vulnerability

1 INTRODUCTION

"A new expository of power constantly tracks and pieces together our digital selves. It renders us legible to others, open, accessible, subject to everyone's idiosyncratic projects — whether governmental, commercial, personal, or intimate… And it does so with our full participation." (Harcourt, 2015, p. 15)

Amidst the current hype around big data (e.g., Boelstorff, 2013) presenting "a paradigm shift in the ways we understand and study our world" (Eynon, 2013, p. 237), there are a number of authors who flag concerns around the "neutrality" of data and algorithms (Boyd & Crawford, 2013; Crawford, 2013; Danaher, 2014; Gitelman, 2013; Marx, 2001; Marx & Muschert; 2007; Mayer-Schönberger & Cukier, 2013; Morozov, 2013; Pasquale, 2015), the possible negative impacts of discrimination (Henman, 2004), the increasing sharing of information by individuals (Solove, 2001, 2004, 2013), the quantified self (Boam & Webb, 2014; Carney, 2013; Lupton, 2014a), privacy (Lanier, 2013; Marwick, 2014; Solove, 2002, 2013;

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Tene & Polonetsky, 2012), and the governance of data (Slade & Prinsloo, 2013; Stiles, 2012; Totaro & Ninno, 2014). The collection, analysis, and sharing of data by a range of stakeholders such as government, commercial enterprises, and increasingly within education, foregrounds the issue of disclosure and the variety of options for users to opt in or out (if provided the opportunity) (Crawford & Schultz, 2013; Lane, Stodden, Bender, & Nissenbaum, 2015; Miyazaki & Fernandez, 2000; Ohm, 2010; Solove, 2013). The tensions inherent in the nexus between privacy, big data, and the public good raise a number of (yet) unanswered questions: "Privacy and big data are simply incompatible and the time has come to reconfigure choices that we made decades ago to enforce constraints" (Lane et al., 2015, p. xii).

In the context of higher education institutions (HEIs), student data (in a variety of formats) has always been used to inform policy, admission requirements, pedagogy, and resource allocation (Prinsloo & Slade, 2014; Prinsloo, Archer, Barnes, Chetty, & Van Zyl, 2015). More recently, the growth of online learning and the availability of digital student data (real-time and historical) have contributed to the emergence of learning analytics. However, the asymmetrical nature of the power relationship between students and their higher education institution (Swain, 2013; Watters, 2013) makes students more vulnerable. In their enthusiasm to adopt new practice, there is a danger that some HEIs forget that the primary aim of learning analytics is to better understand and support learning (Gašević & Siemens, 2015).

Within learning analytics, there is comparatively little discussion around issues of student data privacy and consent (Slade & Prinsloo, 2013) and student perceptions and agency regarding the harvesting and analysis of their data (Kruse & Pongsajapan, 2012). This is in somewhat stark contrast to the broader discourses and concerns surrounding the increasing surveillance by government and commercial entities (Bauman & Lyon, 2013; Carney, 2013).

Given the variety of emerging theoretical frameworks and practices in learning analytics in higher education, a critical engagement with the practices of disclosure and opting in or out of the collection, use, analysis, and sharing of personal and learning data seems paramount. In this paper, we aim to engage with the issue of student data privacy self-management from the perspective of *student vulnerability*. Against this background, and specifically in the context of issues informing disclosure, we adopt the notion of vulnerability as an interpretive lens to consider the control and choices available to users of digital networks (e.g., Mackenzie, Rogers, & Dodds, 2014).

In this *conceptual* paper, we first explore the notion of vulnerability as a heuristic lens to engage with issues surrounding privacy and student privacy, self-management, and agency.

2 VULNERABILITY AS AN INTERPRETIVE LENS

The Latin word "vulnus" means "wound" and to be vulnerable is "to be fragile, to be susceptible to wounding and to suffering; this susceptibility is an ontological condition of our humanity" (Mackenzie et al., 2014, p. 4). It is important to note that vulnerability refers not only to the exposure of individuals to

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

risk but also to experiences of vulnerability in institutions of higher learning (Fineman, 2008) and within broader society (see, for example, Baumann, 2007). While the focus of this article is specifically on *student* vulnerability in the context of learning analytics, it would be disingenuous to forget that HEIs also face potential risks in exploiting, or not exploiting, student data. These positions are inevitably intertwined in ways that lead to competing claims about the risks and ethical challenges in the uses of student data versus the complementary and potentially beneficial uses of that data. While it falls outside the scope of the article to explore the vulnerability of HEIs, we would like to briefly illustrate the interwoven and often mutually constitutive vulnerabilities of HEIs with the vulnerability experienced by students.

2.1 A Brief Introduction to the Notion of Vulnerability

Establishing vulnerability as a lens recognizes, as Fineman puts it, that "we are positioned differently within a web of economic and institutional relationships, [and] our vulnerabilities range in magnitude and potential at the individual level" (2008, p. 10). Fineman suggests that "privileges and advantages accumulate across systems and can combine to create effects that are more devastating or more beneficial than the weight of each separate part. Sometimes privileges conferred within certain systems can mediate or even cancel out disadvantages conferred in others" (2008, p. 15) resulting in individuals being perpetually caught up in dynamic and interacting "webs of advantages and disadvantages" (p. 16). This does not preclude the view that certain individuals and groups are "more than ordinarily vulnerable" (Sellman quoted by Mackenzie et al., 2014, p. 2; see also Fineman, 2008; Maringe & Singe, 2014). Vulnerability as ontology "stresses the ways that inequalities of power, dependency, capacity, or need render some agents vulnerable to harm or exploitation by others" (Mackenzie et al., 2014, p. 6).

The classification of students according to their vulnerability, risk, and need for support and *also* the potential for a return on investment forms the nexus of learning analytics and the practical need to allocate available resources to deliver that identified support. Prinsloo & Slade (2014) have considered the tension between seeing what *might* be done and knowing the limitations of what *can* be done and refer to this as educational triage. In classifying medical disorders in patients, Wardrope suggests that such classification may in itself be a "form of epistemic injustice that prevents people having the hermeneutical resources available to interpret and communicate significant areas of their experience" (2015, p. 314). That is, instead of helping, the classification of patients — and in the case of learning analytics, students — may resemble "iatrogenesis," whereby an action intended to help an individual has an unplanned detrimental effect.

Mackenzie et al. (2014) distinguish between two sources of vulnerability — inherent and situational. *Inherent* vulnerabilities are those intrinsic to the human condition and may depend on factors such as age, gender, race, and disability. In the context of learning analytics, adopting classification schemes increasingly relying on algorithms that focus on specific markers, such as logins, time-on-task, et cetera, but also combine these markers with age, gender, race, and/or disability, may inadvertently amplify the inherent vulnerability of some students.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Situational vulnerability results from a specific context, such as the personal, social, or economic status of an individual or group, and may be short-term, intermittent, or enduring. The scope, duration, and extent of the impact of situational vulnerabilities may in part depend on individuals' resilience. Examples of the linkages between situational vulnerability and learning analytics include changes to students' personal life-worlds due to (temporary) financial, family, or other changes, which may be exacerbated by learning analytics permanently classifying an individual in a particular risk category — disregarding the *situational* nature of the vulnerability.

With a variety of stakeholders (e.g., faculty, administrators, and student support staff) having access to student data, how does the institution ensure that decisions based on this data have, for example, sufficient time-specific context? On the other hand, what is the potential of learning analytics to actually reveal these situational vulnerabilities and so trigger appropriate institutional responses to support students? What are the boundaries between using learning analytics to identify and address vulnerabilities without being patronizing and disregarding the (relative) autonomy of students?

Mackenzie et al. (2014, p. 8) further suggest two different states of vulnerability — dispositional and occurrent. The dispositional–occurrent distinction refers to states of potential as opposed to actual. In the context of learning analytics, this reflects the response to information that notes the existing situation (a student has not submitted a required assignment) and a prediction (based on other student behaviours like this, we might predict the likelihood of a student submitting their assignment). Mackenzie et al. (2014) suggest that there is a moral obligation to support those identified as occurrently vulnerable and to reduce the risks of dispositional vulnerabilities becoming occurrent. Their view is that the overriding responsibility in response to identifying vulnerability is to restore autonomy to the individual. In the context of learning analytics, this potentially translates into giving students the information needed to make informed and supported choices rather than taking a more paternalistic perspective and making decisions on their behalf.

2.2 Institutional Vulnerability

The nature and pace of change in (inter)national public higher education is (possibly) unprecedented (Altbach, Reisberg, & Rumbley, 2009; Carr, 2012; Christensen, 2008). Not only is the public higher education sector faced with changes in student profiles, funding regimes, a dramatic increase in privatization and internationalization, and greater demand for empirical research, but it is also faced with the emergence of new providers and the increasing convergence of various forms of higher education (Altbach et al., 2009; Watters, 2012). According to Watters (2012), there is increasing evidence of the "unbundling" of higher education, with curriculum development, course delivery, teaching, student support, assessment, and accreditation being designed and often delivered by different providers. This fragmentation of the different elements of higher education is not necessarily negative, but it does challenge many assumptions and beliefs about knowledge production and knowledge dissemination, questions the traditional roles of faculty, interrogates intellectual property regimes, and challenges

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

organizational structures and funding hierarchies. It is no longer business as usual for higher education. The obsolescence of some curricula, assessment strategies, faculty expertise and roles, and traditional forms of higher education is becoming a new reality. Amidst funding cuts and increasing competition (Altbach et al., 2009), funding follows performance rather than precedes it, necessitating the need for evidence of the effectiveness of teaching and learning (Howard, McLaughlin, & Knight, 2012; Schildkamp, Lay, & Earl, 2013).

In this context, HEIs are increasingly vulnerable and must optimize their use of data, in particular student data (Baker & Siemens, 2014; Gašević & Siemens, 2015; Prinsloo & Slade, 2015). Though student and learning data can be used for many purposes (Gašević & Siemens, 2015), HEIs have a fiduciary duty to ensure that they harvest, analyze, and use it with a view to improving students' chances of success (Prinsloo & Slade, 2014). Ironically, the collection, analysis, and use of student data have the potential, in some cases, to increase, rather than decrease the vulnerability of students (a point to which we will return later).

2.3 Vulnerabilities in an Era of Pervasive Surveillance

As technology continues to advance and we make greater use of mobile devices, there is evidence of a parallel increase in the collection, analysis, and use of individuals' digital data (Bauman & Lyon, 2013; Gangadharan, 2012; Mayer-Schönberger, 2009; Mayer-Schönberger & Cukier, 2013; Solove, 2004). Many authors suggest that as this activity proliferates (often without the knowledge of individuals), the potential for harm and discrimination increases (Gangadharan, 2012; Henman, 2004; Lazar, 2015; Lyon, 2015; O'Connell, 2016).

Since vulnerability in the digital context depends on our understanding of the notion of privacy, it is useful to briefly explore the four categories of privacy problems proposed by Solove (2006). Table 1 (below) uses Solove's taxonomy of privacy to illustrate the potential for increasing individuals' vulnerability.

Table 1: Solove's privacy taxonomy (2006) and individual vulnerability.

TAXONOMY CATEGORY	ELEMENT	IMPLICATIONS FOR VULNERABILITY
Information collection	Surveillance	Solove makes clear that surveillance (whether covert or transparent) should not be assumed to be automatically harmful and that some social control can be beneficial. However, the potential for harm, misuse, wrongful downstream use, lack of transparency, etc., suggests that the "attentive gaze" (2006, p. 499) of many unknown institutions and entities inherently results in increased vulnerability.
	Interrogation	"Interrogation is the pressuring of individuals [whether indirectly or through coercion] to divulge information" (Solove, 2006, p. 477). Interestingly, in the light of what Payne (2014) calls "digital promiscuity," we also need to point to the ways in which individuals freely provide personal information (albeit

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

TAXONOMY CATEGORY	ELEMENT	IMPLICATIONS FOR VULNERABILITY
		specific to a particular context). The scope and role of the coercive and nudging nature of online platforms that encourage information sharing (see, for example, Marx & Muschert, 2007; Raynes-Goldie, 2010) adds another dimension to the link between interrogation and vulnerability.
Information processing	Aggregation	While there are examples of the benefits of aggregation, the compiling of digital profiles from a range of disparate sources and databases also exponentially increases the potential for misinterpretation, misuse, erosion of contextual integrity of data, and resulting discrimination (Henman, 2004; O'Connell, 2016). Individuals share pieces of information on disparate platforms and when these different pieces of information are combined, the "whole becomes greater than the parts" (Solove, 2006, p. 507).
	Identification	Identification is linked to aggregation (above) and connects aggregated profiles to a specific individual or group of individuals. This may also allow potential benefits, such as ensuring accountability, etc.
	Insecurity	Examples of insecurity (lack of security) include issues around identity theft and distortion (whereby an individual's record can become polluted). Some may focus on disclosure (the actual leakage of information) as the underlying issue, but insecurity comes from being placed in a weakened state, of having increased vulnerability to a range of future harms.
	Secondary use	Where information is used for purposes other than for the original purpose for which the information was shared.
	Exclusion	In the context of vulnerability, exclusion refers to a lack of transparency around personal information stored and an inability to amend that information.
Information dissemination	Breach of confidentiality	Vulnerability resulting from a breach of confidentiality refers to the violation of trust.
	Disclosure	Individuals make decisions (however arbitrarily) on what information to share under what circumstances and with some consideration of context. To disclose information out of these contexts and without specific knowledge and permission to do so increases the scope and impact of the vulnerability experienced by the individual. For example, we might share our personal or political views as part of a private conversation, but might prefer not to have those attributed to us in a public forum. The potential for disclosure thus increases vulnerability.
	Exposure	Solove states that "Unlike disclosure, exposure rarely reveals any significantly new information that can be used in the assessment of a person's character or personality" (2006, p. 477). Though it reveals nothing out-of-the-ordinary, it reveals situations where we are vulnerable, weak, and indisputably human. In an age of "digital promiscuity" (Payne, 2014) it is clear that individuals can expose themselves on social media platforms or mobile technologies. Excluding the original act of self-exposure, the potential sharing and re-use of these acts exponentially increase vulnerability.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

TAXONOMY CATEGORY	ELEMENT	IMPLICATIONS FOR VULNERABILITY
	Increased accessibility	With the increased scope and reach of the "elaborate lattice of information networking" (Solove, 2004, p. 3), it has become much easier to access public-domain information. Solove (2006) suggests that the issue at stake is not the breach of confidentiality, but the increased ease in accessing information that is already available. While there are also benefits to increased accessibility — for example, access to scholarly works and profiles, and profiling for specific jobs — it is fair to say that there is also possible harm to individuals.
	Blackmail	"The harm is not in the actual disclosure of information, but in the control exercised by the one who makes the threat over the data subject" (Solove, 2006, p. 543).
	Appropriation	This refers to the appropriation of someone else's identity, personality, or intellectual labour, presenting it as one's own.
	Distortion	"Distortion is the manipulation of the way a person is perceived and judged by others, and involves the victim being inaccurately exposed to the public" (Solove, 2006, p. 550). The result of both distortion and disclosure is embarrassment, stigma, and reputational harm.
Invasion Interestingly, Solove (2006) notes that invasion does not always involve information	Intrusion	Similar to surveillance in many ways, intrusion takes this a step further so that the individual becomes aware of and affected by the presence or activities of others. It might be argued that the maintenance of a digital profile in an online community actively invites the gaze of others (Dennis, 2008; Solove, 2004; Weber, 2015) in the context of sousveilance and the "participatory panopticon" (Dennis, 2008, p. 347). However, we might easily recognize the vulnerability associated with an unsought or offensive response to a publicly available action or post, for example.
	Decisional interference	This refers to institutional interference in personal decision-making, such as paternal jurisdiction on the upbringing of children. Decisional interference compromises individuals' autonomy to make decisions and take responsibility for those decisions. Within the higher education context, it might then relate to the restriction of options available to the student based on their available data.

Table 1 illustrates the many ways in which the notion of vulnerability is closely linked to different problems connected to understanding and regulating privacy. The taxonomy makes clearer many of the nuances in privacy and helps us to better understand how each element of privacy has the potential for harm and benefit, which in turn either ameliorates or exacerbates vulnerability.

2.4 Student Vulnerability

Within the context of the increasing quantities of data, standardized formats of educational data, increased computational power, and availability of a range of analytical tools (Baker & Siemens, 2014),

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

students are increasingly exposed as they study online and are confronted by the all-pervasive gaze of their institution (Knox, 2010). Though the intention of collecting and using student data arguably falls within the scope of the fiduciary duty of higher education, it is increasingly possible that student data *may* be also used inappropriately and unethically, further increasing the vulnerability of students (Prinsloo & Slade, 2015). Research on student success and retention using the lens of student vulnerability is rare and the notion of vulnerability is mostly implied in issues such as under-preparedness, risk, deficiency models, and so forth (Maringe & Sing, 2014; Subotzky & Prinsloo, 2011).

The notion of vulnerability is generally "under-theorised" (Mackenzie et al., 2014, p. 2) and "raises new issues, poses different questions, and opens up new avenues for critical exploration" (Fineman, 2008, p. 9). Current theoretical thinking includes the notion that vulnerability is not only a key characteristic, but also a defining characteristic of *all* human life. Recognizing the scope and impact of vulnerability furthermore goes beyond anti-discrimination and strategies to ensure equal opportunities for all. Vulnerability as heuristic lens suggests that equal opportunities and the emphasis on equality do not address "institutional arrangements that privilege some and disadvantage others. It does not provide a framework for challenging existing allocations of resources and power" (Fineman, 2008, p. 3). It is precisely the impact of these "institutional arrangements that privilege some and disadvantage others" that illustrate the need and provide the rationale for exploring student vulnerability as lens.

While learning analytics attempts to address the vulnerability of the institution and of students through the identification of potential pitfalls and risks in students' learning journeys, there is a danger that such identification may render some students even more vulnerable (Prinsloo & Slade, 2014). Whilst interventions aim "to enable or restore, wherever possible and to the greatest extent possible, the autonomy of the affected persons or groups" (Mackenzie et al., 2014, p. 9), they may also become *pathogenic* such that "a response intended to ameliorate vulnerability has the paradoxical effect of exacerbating existing vulnerabilities or generating new ones" (Mackenzie et al., 2014, p. 9).

Within the context of the complexities surrounding institutional and student vulnerability, it is helpful to go beyond a simple "rights" or "privacy" perspective and explore the notion and scope of learner agency through vulnerability as lens. Such an approach resembles a "discursive–disclosive" (Stoddart, 2012) approach. While a rights-based approach sets out procedural guarantees establishing rules and access to satisfaction if these rules are breached, there are increasing concerns about its effectiveness in an environment where legislation and regulatory frameworks almost permanently lag behind new breaches of privacy and technological developments (Westin, 2003). A discursive–disclosive approach situates surveillance in the context of what is being done, by whom, and for what purpose and then investigates alternative approaches to satisfy the need that initially resulted in surveillance (Prinsloo & Slade, 2014).

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

3 VULNERABILITY, DISCLOSURE, AND INDIVIDUAL PRIVACY MANAGEMENT

3.1 Individual Agency and Disclosure: A Complex Combination

In the discourses surrounding privacy, the collection, analysis, and use of personal information and disclosure, it is clear that our definitions and regulatory frameworks barely scratch the surface of the complexities resulting from linkages between personal understandings of privacy, perceptions of trust, and risk, agency, and context (Haggerty & Ericson, 2006; Kerr & Barrigar, 2012; Lyon, 2006; Solove, 2004). There is ample evidence in literature of a growing interest in the threats to individual privacy as well as expressed concern that current Terms and Conditions (TACs) don't disclose the full extent to which personal information is collected, analyzed, and (often) shared. Authors also now recognize that many individuals don't engage with these TACs — because of their length, or the technical and legal nature of the language used.

Alongside this are increasing concerns about the ways in which individuals are inadvertently increasing their own vulnerabilities through the inconsiderate sharing of information, which Payne (2014) terms "digital promiscuity." We therefore need to understand individual vulnerability not only in respect to increasingly ubiquitous surveillance, but also to their own comprehension of risk, their perceptions of trust in particular contexts, and their agency (Miltgen & Smith, 2015). It is crucial, then, that we begin to recognize that "privacy self-management and consent is a fluid and changing notion worth exploring. It is important that legal and regulatory frameworks differ between geopolitical and institutional contexts" (Prinsloo & Slade, 2015, p. 84).

It is clear that privacy self-management goes beyond the traditional binary of simply opting in or opting out. We need to consider a "palette of 'privacy solutions'" (Gurses, 2015) which potentially allows individuals to make more informed choices (Brian, 2015; Lane et al., 2015). Recent studies such as the report on "Public perceptions of privacy and security in the post-Snowden era" (Pew Research Center, 2014) indicate a general decrease in public confidence over control of personal information. The report suggests that an overwhelming majority feels that it would be very difficult to remove biased, inaccurate, or embarrassing personal information and they express concern regarding the access that commercial third parties might have to personal online data. Interestingly, though most also feel that government should do more to regulate access to digital personal information, *over half also indicated that they were prepared to trade off personal data for benefits*. Though there is an increased awareness among individuals regarding the collection and use of their personal information, Brian states that "consumers are largely unaware of the consequences of the seemingly mundane things that they share everyday through their online activities" (2015, p. 7).

3.2 Trading (Perceived) Privacy for (Perceived) Benefits

Since the late 1990s, studies have indicated that commercial websites are typically slow to share

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

information on the collection, analysis, and use of personal data and often don't have comprehensive or easily understandable privacy policies (Miyazaki & Fernandez, 2000). The conceptual framework developed by Miyazaki and Fernandez (2000) suggests the need for a richer and more nuanced understanding of the collection, analysis, use, and sharing of personal information in the context of e-commerce. Possibilities of disclosure (Figure 1) range from never collecting data nor identifying customers when they access a site; customers opting in by explicitly agreeing to having their data collected, used, and shared; customers explicitly opting out; the constant collection of data without consumers having a choice (but with their knowledge); to the collection, use, and sharing of personal data without the user's knowledge (Miyazaki & Fernandez, 2000).

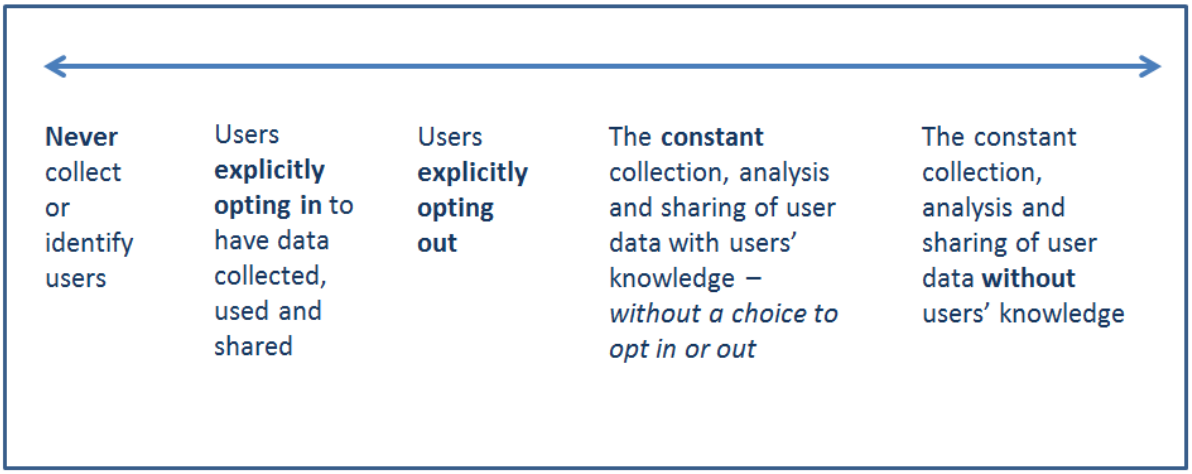

Figure 1: A framework for mapping the collection, use, and sharing of personal information (Miyazaki & Fernandez, 2000).

While Figure 1 illustrates the various options available from the perspective of the service provider, it also demonstrates that thinking in terms of a binary of privacy positions is limiting. We suggest an extended framework that allows us to consider the issues from the perspective of the *users* of these services (Figure 2).

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

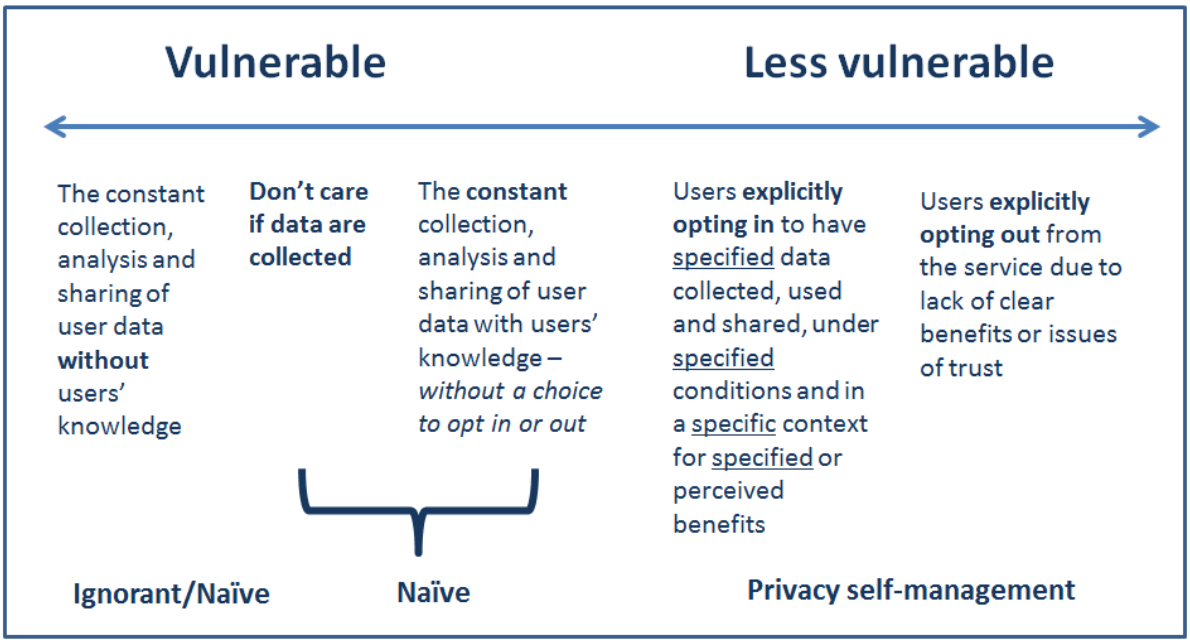

Figure 2: A framework for mapping user vulnerability and privacy self-management.

Since the collection, analysis, and use of personal digital information have become endemic, it is hard to believe that any users remain unconcerned — either because they believe that it does not affect them or that they don't have anything to hide (Solove, 2007). Our proposed framework, shown as Figure 2, suggests that the first three scenarios result in users becoming highly vulnerable. In this space, individuals are most likely to share personal and even sensitive information carelessly, resulting in "digital promiscuity" (Payne, 2014). We might also include as naïve those users who *know* that their data[1] are being collected and possibly shared as a compulsory part of the conditions of using a service, but consider their participation or use of that service as having enough (perceived or real) benefits not to terminate their use. We propose that this presents a paradox of privacy self-management. In such cases, it is often clear that a user's ability to continue using a service or platform is contingent upon the acceptance of cookies, for example, *as a given.* It is (perhaps briefly) communicated by the service provider that refusal will either deny further access or seriously downgrade the effectiveness or quality of the service. In many cases, where there is a perceived (or real) urgency to continue, an apparent lack of alternatives, or simply sufficient apathy to discourage the user from seeking alternatives, the user will effectively opt in. Ignorance may not be claimed here, and it is true that there will be some services for which there simply *are* no ready alternatives or providers in which the user has sufficient trust — but the informed agreement to continue still renders the user vulnerable.

To the right of the spectrum we find not only increased awareness but also increased agency where users make choices regarding what information is shared, under what conditions, in what contexts, and for what

[1] In following Kitchen (2014), we have used "data" as plural unless part of a quotation.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182.
http://dx.doi.org/10.18608/jla.2016.31.10

benefits. As Prinsloo and Slade (2015) indicate, the matter of consent is complex. Individuals may adapt decisions regarding how much information they are prepared to share (and for what purpose) depending on the context. Prinsloo and Slade (2015) suggest that these individuals will typically decide to opt in or out on a case-by-case basis, considering the context of each opportunity. When the default option of information sharing is to opt in rather than to opt out, Bellman, Johnson, and Lohse (2001) found that individuals take greater care. Other aspects influencing opting in or out include the ways in which the option is displayed; for example, where the notice is placed on the screen, the length of supporting documents or notices, and even the font size. Other research suggests that "many organisations will have the sophistication and motivation to find ways to generate high opt-in rates" (Solove, 2013, p. 1898). Despite the challenges and the contestations regarding the effectiveness of opting in/out regimes, Solove states that "Providing people with notice, access, and the ability to control their data is key to facilitating some autonomy in a world where decisions are increasingly being made about them with the use of personal data, automated processes, and clandestine rationales, and where people have minimal abilities to do anything about such decisions" (2013, p. 1899).

We suggest that it is simply impossible for individuals to comprehend, at the time of opting in or out, the scope of data that might be collected, analyzed, and used and the implications of the different layers of collection and use by a range of third parties. "Even if every entity provided people with an easy and clear way to manage their privacy, there are simply too many entities that collect, use, and disclose people's data for the rational person to handle" (Solove, 2013, p. 1888). The sheer scale of the collection of data, and the different approaches to providing information on how data will be collected per site, makes it almost impossible for individuals to assume full responsibility for their opt in/opt out decisions. Individuals can have no idea how the data collected may be re-identified and aggregated in future or whether this matters. While data may seem innocuous in one context, aggregation results in disembodying data from its original context, increasing possibilities for misuse and misinterpretation. "There are too many unknowns with regard to how data may be combined at a certain future point in time, when the original context in which the data were captured is no longer known" (Prinsloo & Slade, 2015, p. 86). As new uses for historical data are found, the quality and fit of the historical data within new contexts may be severely compromised.

Levels of risk-averseness may also vary, with some sharing willingly to their own possible detriment, while others attempt to navigate site terms and conditions, only to give up due to their length, legalese, and complexity. There are many examples of the ways in which changing social norms regarding the scope and nature of personal data shared can result in changes in how we see and/or participate in surveillance, self-surveillance, or the "quantified self" phenomenon, or sousveillance (Prinsloo & Slade, 2015; also see Lupton, 2012).

While the notion of informed consent plays a vital role in the discourses surrounding privacy and privacy self-management, Prinsloo and Slade (2015) identified the following problems regarding the notion of informed consent: 1) the problem of scale; 2) the re-identification and the problem of aggregation; 3) the

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182.
http://dx.doi.org/10.18608/jla.2016.31.10

quality, accountability, and purpose of data; 4) the drawbacks in setting limitations for use; 5) the impact of the increasing openness and sharing of data; and 6) the problematics and understandings of user agency.[2]

Indeed, the Organisation for Economic Cooperation and Development (OECD) noted in 2012 that "*prior* affirmative consent in all cases would be impractical" (in Brian, 2015, p. 170; emphasis added). There is also a suggestion that should users need to set up an account in order to use a service, they are accepting an ongoing relationship with the provider and so implicitly agreeing to the terms and conditions. The act of signing up provides the opportunity to assess and accept subsequent tracking and to manage what is shared going forward more knowingly. It is, however, not clear that many users consciously enter into such a relationship. Adding to the importance and need to understand privacy from the perspective of individual vulnerability is an understanding that once data have been legitimately acquired, current legal frameworks do not dictate of the scope and constraints regarding the use of such data (Ohm, 2015). Greenwood, Stopczynski, Sweat, Hardjono, and Pentland therefore moot the need for a "new deal on data" (2015, p. 192).

In the context of the collection, analysis, and use of student data by HEIs, anecdotal evidence suggests that most students are either unaware of the fact that HEIs collect, analyze, and use their digital data, or they don't care. Reasons explaining the naivety or ignorance of students include the inherent trust that students may have in their institution not only to store their personal information, but also to use the information to their benefit (Prinsloo, Slade, & Van Zyl, In Press). All HEIs collect, analyze, store, and share student information for regulatory, national statistic, and funding purposes. Most (if not all) of this data are at an *aggregated* level. Of particular concern in the context of student vulnerability are the collection, analysis, and use of *learning* data combined with demographic and personal funding data to inform and decide on student progress, or to form the basis for a decision when a student is transferring to another institution. Further concerns include the fact that the assumptions and beliefs informing algorithmic decision-making are hidden and, most probably, never open for review (Willis, Slade, & Prinsloo, In press).

There are, however, also the potential benefits for students when they understand the implications of the data collected by institutions and how, in light of the beneficiary duty of HEIs, the analysis and use of the information may benefit them (an issue to which we will return later).

Balancing concerns that the collection, analysis, and use of data can exacerbate injustice and increase or amplify existing inequalities against the potential benefits of the collection, analyzing and using that data remains difficult and complex. Engaging with the dangers but also with the potential, using student vulnerability as a heuristic lens, necessitates a discursive–disclosive approach that opens up a space to critically engage with questions such as who benefits, what can the individual control, what is the role of data in (often unequal) power-relations, and what are the dynamics of resistance-compliance (see, for

[2] For a full discussion on the limitations of informed consent, see Prinsloo & Slade, 2015.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

example, Stoddart, 2012). Given all that, and the fact that users often do not read and/or engage with TACs, it is crucial to at least consider the ways in which TACs and institutional transparency function (or should function) in educational contexts.

4 TERMS AND CONDITIONS IN AN EDUCATIONAL CONTEXT

In an analysis of the TACs of three providers of massive open online courses (MOOCs) namely Coursera, EdX, and FutureLearn, Prinsloo and Slade (2015) found several troubling gaps in both the providers' fiduciary duty to students and their consideration for the inherent privacy issues and resulting student vulnerability. The TACs of these three providers were analyzed focusing on the following elements: 1) length; 2) types of data collected; 3) methods of data collection; 4) conditions for sharing data collected; 5) uses of data; 6) user access to, responsibility, and control of data; and 7) institutional duty of care.

This study found that the length, font size, and number of headings used in these TACs would, in all probability, discourage engagement, so that users would accept the TACs without reading them. All three providers stated clearly that all information provided by users would be collected and used. One MOOC provider explicitly stated that they may request information from third parties such as credit reference agencies. Interestingly, while all three providers acknowledged that they used cookies to collect data, only one (FutureLearn) provided a list of cookies with clear descriptions of their function. All three providers made it clear that disabling the cookies would disrupt the service, potentially to the extent that it would be rendered unusable. Regarding the collected data, all three stated that it would be used to increase the efficiency of the platform and the structure of the learning experience. One provider (EdX) alerted users that student posts are owned by EdX in perpetuity and could be used for whatever purposes EdX decides. There was no indication whether that use would include a depersonalization of the data. Interestingly, and of some concern, was the encouragement by FutureLearn for users to reveal personal details such as gender, location, and history in order to deepen the personal element in the learning.

None of the providers gave the option to opt out — indeed, users were alerted to the inability of their MOOC provider to ensure and guarantee that information shared would not be used by fellow users or made public because of security breaches. Only one, FutureLearn, provided an opportunity (for a small fee) for users to request access to the data held by the company (in line with national data protection requirements).

In exploring learner agency in the context of user vulnerability, it seems that TACs do not, on their own, address and ameliorate student vulnerability. This does not negate the potential of TACs to become part of the "palette of 'privacy solutions'" (Gurses, 2015), but we need a broader, more agile, more nuanced approach to address student vulnerability in learning analytics. The Open University's (2014) "Policy on ethical use of student data for learning analytics" is a recent example of a higher education institution providing a regulatory framework to guide the ethical implementation of learning analytics. There is also room for the development of a Code of Ethical Practice for data analysts in the higher education context — an issue explored by Willis, Slade, and Prinsloo (in press).

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Using the framework suggested by Prinsloo and Slade (2015), the next section attempts to explore the (im)possibilities of creating spaces for students to be not only more aware, but also to make more informed and conscious decisions about what they share and for what purposes. As a framework, it is clear that the different elements are not absolute, separate entities, but that the potential linkages between these elements may address the obvious, potential limitations of the separate elements and the framework as a whole.

5 A FRAMEWORK FOR LEARNER AGENCY

5.1 The Duty of *Reciprocal* Care

It is increasingly clear that the boundaries between public and private spaces continue to evolve and blur so that a complete separation of public and private is no longer feasible. As the Internet of Things (IoT) evolves, linking and tracing linkages between personal devices across the traditional divides of public and private, it is clear that we need a "new deal" of privacy and personal data (Greenwood et al., 2015). In the context of higher education, we simply can no longer ignore the implications of our fiduciary duty pertaining to the collection, analysis, and use of student data. Higher education institutions, by virtue of the service they offer, have almost complete power to collect, analyze, use, and share student data within their service mandates and national and international legal frameworks. There is no question that the balance in the power relationship is *with the provider.*

We contend that this increases the responsibility of that *provider* to ensure transparency, security, and reasonable care. While acknowledging the limitations of TACs, we propose that HEIs should formulate their TACs in a language and format that make clear "what data is collected, for what purposes, and with whom the data may be shared (and under what conditions)" (Prinsloo & Slade, 2015, p. 89). It is also suggested that, where feasible, institutions make data sets available to students "to verify or correct conclusions drawn where necessary, as well as provide context, if appropriate" (p. 89). This does not mean, necessarily, that students will be able to make complete sense of their data, as this may be complicated by practicalities of size and format. Perhaps more useful would be the ability to share the rationale of decisions which that impact students' current or future learning opportunities and the data on which assumptions are made *at the time* such decisions are made. While reflecting this information back to students is likely to remain complex, it has the potential to create greater transparency and accountability.

Although the collection of student data typically takes place within an *asymmetrical* power relationship, this does not exempt students from a responsibility to ensure that they also take responsibility for both the accuracy and completion of the data and information they share, but the extent to which they (publicly) share personal details. HEIs cannot easily ensure that the personal information students share in discussion forums will remain private and secure. There is ample evidence that once information is posted, even if later deleted, it may be shared (e.g., via a screenshot) on platforms outside of the

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

institutional learning management system (LMS).

It is clear that though HEIs can and should do everything possible to decrease the potential of harm and vulnerability of students, they do not and cannot carry the full or sole responsibility for securing student data. From a procedural perspective, the provision of greater access and recourse to revisions might necessitate the appointment of a neutral ombudsperson to address concerns and issues flowing from the contract between institution and students.

5.2 The Contextual Integrity of Privacy and Data

Users decide to share or not share information given a particular context and, as research shows, opting in, or sharing information in one context, does not imply that the information provided can be used in a different circumstance. Privacy is relational and using information outside of the original context implies different sets of relationships and linkages, not originally foreseen (Nissenbaum, 2010, 2011). For example, analyzing and combining student information from blog posts and discussion forums with other information such as library access and demographic data means that the potential for a resulting loss of contextual integrity of data (Nissenbaum, 2010) becomes an increasing concern.

As historical data are increasingly aggregated and re-used for purposes different from the original context in which it was collected, it is necessary to be aware of and act to prevent contextual integrity collapse. The danger of contextual integrity collapse increases when algorithms collect data, often from a range of institutional repositories (Prinsloo et al., 2015).

5.3 Student Agency and Privacy Self-Management

In this section, we locate the possibilities and constraints of student agency and privacy self-management having accepted the informational asymmetry (Brunton & Nissenbaum, 2015) in the relationship between students and HEIs. Given this informational asymmetry, individual agency becomes more complex as users are unable to foresee how information shared now has the potential to become more damaging in future, often when combined with other sources such as medical and/or financial records. In such situations, opting out becomes a mere "fantasy" (Brunton & Nissenbaum, 2015, p. 53). The current and future costs of opting out or *not* opting in cannot possibly be foreseen at the moment of choice (see Figure 2 and the following discussion). Brunton and Nissenbaum state that the scope and potential of individual agency in the "context of unavoidable relationships between people and institutions with large informational and power asymmetries" (2015, p. 56) is very difficult to map and plan for, but that we should nonetheless attempt to broaden "*the spectrum* of responses to oppression and coercion" (p. 57; emphasis in the original).[3]

[3] See Brunton and Nissenbaum, 2015, for a discussion of various strategies to resist and obfuscate the collection, analysis and use of data and the ethical dimensions of these responses and strategies.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

If we see education as moral practice (Slade & Prinsloo, 2013), we cannot negate the scope of care in the fiduciary duty of the institution towards students especially in the light of the informational and power asymmetries. "The social contract and fiduciary duty of care provides a crucial basis for thinking critically about the range of student control over what data will be analyzed, for what purposes, and how students will have access to verify, correct or supply additional information" (Prinsloo & Slade, 2015, p. 89). This duty of care should, however, not be construed to mean that the responsibility for privacy and care only resides with the institution. If students are rightly seen as agents and active collaborators in the harvesting, analysis, and use of their data (see Kruse & Pongsajapan, 2012), HEIs must find ways to engage students not only in policy formulation but also in assuming responsibility for verifying information and analyses and in contributing information that can result in a better, mutual understanding of students' learning journeys.

We acknowledge that there are a number of challenges, many of which are, at face value insurmountable, such as balancing the fiduciary duty of care with acknowledging students' agency and autonomy to make their own decisions. How do we increase students' self-awareness regarding the potential hazards of sharing personal information and context (in order for us to offer better and more appropriate support) and, at the same time, acknowledge the difficulties in preventing future misuse of that information by others, both within and outside of the original context? How do we balance the need to know our students better with the responsibility that comes with knowing them better? (Prinsloo, 2015).

Most HEIs currently apply as default the position whereby the act of registration equates forfeiture of student control over their data. Although HEIs have a right to collect, analyze, and use aggregated student data responsibly, students should also be aware of the circumstances under which their personal information may be used to tailor both their curriculum and their access to resources and support (see Figure 2). We might also work to create more substance over neutrality and acknowledge the limitations of the quantification of students and their learning and move towards thicker, qualitative descriptions of students and their learning.

5.4 Rethinking Consent and Employing Nudges

In following Solove, we acknowledge that "consent is far more nuanced, and privacy law needs a new approach that accounts for the nuances without getting too complex to be workable" (2013, p. 1901). We therefore suggest that nudges (as used in the health and energy sectors) be explored as alternatives to the default opt out strategies generally practiced within higher education (see Rubel & Jones, 2014; Selinger, 2015). As the Pew Research Center (2014) report indicates, users of online services are often willing to share data in return for services or discounts. If students are more actively engaged and informed regarding the benefits of sharing their data as well as the protocols employed to safeguard access to it, they may more willingly participate in sharing data that decreases both their own and their institution's vulnerability. There is, however, the warning issued by Solove (2006) (Table 1) that we need to consider the scope and implications of coercion when nudging individuals to share information.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

5.5 Developing Partial Privacy Self-Management

As it is virtually impossible for users to engage with the TACs of every service they use, Solove (2013) raises the possibility of a blanket opt in for a range of services or providers. Though this potentially raises a number of other issues, HEIs might at least make clearer what data are harvested and used for what purposes on which of its sites and provide students with the opportunity to provide blanket approval. Additional sites or services may then have different protocols and/or TACs for which students could be made aware and provided with separate opportunities to opt in (see Figure 2).

5.6 Adjusting Privacy's Timing and Focus

With the increasing use and re-use of historical data, it is clear that student data can be used for many years after the student has left the institution. HEIs therefore need to make clear which student data may be stored and used "downstream," for what purposes, and under what conditions. While the storage of data is governed by national and institutional legislation and policy, Solove (2013) suggests that "users may be provided different options such as outright restrictions, partial consent depending on the scope, context and timing, and permission to harvest and use data with an option to later revoke consent or change the scope of consent depending on the context or circumstances" (also see Prinsloo & Slade, 2015).

5.7 Moving Toward Substance over Neutrality

In following Solove (2013), Prinsloo and Slade suggest that despite concerns about the effectiveness of regulation and legislation, we cannot altogether negate the role of substantive rules and hard boundaries "that block particularly troublesome practices as well as softer default rules that can be bargained around" (2015, p. 90; also see Solove, 2013). There seems to be a move towards regulation that considers, inter alia, the need for explicit consent to the processing of information and the recognition of the right of subjects to be forgotten or to have personal digital data removed. There are, however, a number of authors who express concern that in the context of big data and individuals freely sharing information, regulation and legislation will always be behind (Carney, 2013; Crawford & Shultz, 2013).

5.8 Moving from Quantified Selves to Qualified Selves

In line with the main tenets of a student-centred approach to learning analytics (Kruse & Pongsajapan, 2012), the renewed emphasis that learning analytics is about *learning* (Gašević & Siemens, 2015), and of students as agents rather than data objects or passive recipients of services (Slade & Prinsloo, 2013; Subotzky & Prinsloo, 2011), the above framework allows us to contemplate the significance and impact of the notion of students not as quantified selves but as qualified selves (e.g., Davies, 2013; Lupton, 2014a, 2014b).

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Carney (2013) suggests that the quantification of the self through tracking processes (whether as participant and provider of the data, or as data object) can result in the belief that we are our data. The digital data provided about us and by us may then be seen to provide a complete picture of who we have been, who we are, and (most probably) who we will be. Though the use of data to quantify an individual's credit worthiness or health status (to mention but two examples) is not necessarily bad per se, we should be aware of any implicit assumption that the collected data provide a complete picture. As many authors (e.g., Mayer-Schönberger, 2009; Mayer-Schönberger & Cukier, 2013; Solove, 2013) have warned, the increasing use, re-identification, and combination of various sets of decontextualized data raise a range of serious concerns.

While learning analytics can and should play an important role in students' self-awareness, self-knowledge, self-efficacy, and healthy loci of controls, a lack of specific context can result in limited or even faulty assumptions. In the current collection and use of student data, students often have no insight into the data collected by their HEI and so there is no possibility that data can be verified or any context provided. Considering the asymmetrical relationship of students and their institutions, students potentially then become quantified selves based on, for example, the number of log-ins, clicks, downloads, or time-on-task. It is important to allow opportunities for context-rich information so that institutions and students may better understand the complexities and interdependencies in the nexus between students, institutions, and the impacts of socioeconomic, technological, environmental, political, and legal contexts. "Where the quantified self gives us the raw numbers, the qualified self completes our understanding of those numbers" (Boam & Webb, 2014, par. 8). Our students are therefore much more than just conglomerates of quantifiable data so it is important that we take into account "the contexts in which numbers are created" (Lupton, 2014b, p. 6).

Lupton warns that in order to optimize our understanding of data (especially self-tracking data) it is important to appreciate that the meanings of self-tracked data are often hard to determine; "that personal data can be disempowering as well as empowering; the conditions in which data are gathered can influence their validity; [and] the contexts in which data are generated are vital to understanding their meaning" (2014b, p. 7). Lupton (2014b) also raises concerns about the secure storing and governance of data and notes that data can be used to discriminate against individuals.[4]

Boam and Webb (2014) suggest that "Just as stories yield data, data yield stories. And just as it is difficult to quantify our lives without data, we cannot qualify them without context or narrative. When we bring the two sides together, we achieve deeper self-knowledge" (Boam & Webb, 2014, par. 21). Diversifying our data collection methods, contexts, and timing and allowing individual students to participate in reiterative and collaborative processes of sense-making challenges many of the assumptions and practices of current TACs in higher education.

[4] See Prinsloo and Slade (2014) for an exploration of educational triage in higher education.

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

6 CONCLUSION

If big data herald "a paradigm shift in the ways we understand and study our world" (Eynon, 2013, p. 237), the increasing potential and practice of collecting, analyzing, and using student data allows us the opportunity to explore some of the current paradigms surrounding that data. In the context of the fiduciary duty of HEIs and the asymmetrical power and information relationship, higher education cannot afford a simple paternalistic approach to the use of student data. Such an approach should not be considered appropriate given the complexities within the nexus of privacy, consent, vulnerability, and agency.

Individual choice to allow for or disregard individual agency regarding the collection, use, and sharing of one's digital data (Miyazaki & Fernandez, 2000) depends on a range of factors including context (clarity of) information provided in TACs and the risk-averseness or vulnerability-awareness of the individual (Figure 2).

The notion of vulnerability allows an interesting and useful lens on student data. Though both institutional and individual vulnerability needs to be considered, we have focused specifically on student vulnerability. This article expands on an earlier framework developed by Prinsloo and Slade (2015) and explores ways to decrease student vulnerability, increase their agency, and empower them as *participants* in learning analytics to move from quantified data objects to qualified and qualifying selves.

REFERENCES

Altbach, P. G., Reisberg, L., & Rumbley, L. E. (2009). *Trends in global higher education: Tracking an academic revolution*. A report prepared for the UNESCO 2009 World Conference on Higher Education. France: UNESCO. Retrieved from http://www.uis.unesco.org/Library/Documents/trends-global-higher-education-2009-world-conference-en.pdf

Baker, R. S. J. d., & Siemens, G. (2014). Educational data mining and learning analytics. In K. Sawyer (Ed.), *The Cambridge Handbook of the Learning Sciences (2nd ed.)* (pp.253—275*).* UK: Cambridge University Press.

Bauman, Z. (2007). *Liquid times: Living in an age of uncertainty.* Cambridge, UK: Polity Press.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance.* Cambridge, UK: Polity Press.

Bellman, S., Johnson, E. J., & Lohse, G. L. (2001). To opt-in or opt-out? It depends on the question. *Communications of the ACM, 44*(2), 25–27. http://dx.doi.org/10.1145/359205.359241

Boam, E., & Webb, J. (2014, 2 May). The qualified self: Going beyond quantification. [Web log post] Retrieved from http://designmind.frogdesign.com/2014/05/qualifiedself-going-beyond-quantification/

Boelstorff, T. (2013). Making big data, in theory. *First Monday, 18*(10). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/view/4869

boyd, d., & Crawford, K. (2013). Six provocations for big data. Paper presented at Oxford Internet

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Institute's "A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society" on September 21, 2011. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1926431

Brian, S. (2015). The unexamined life in the era of big data: Toward a UDAAP for data. *University of Dayton Law Review, 40*, 181–199. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2533068

Brunton, F., & Nissenbaum, H. (2015). *Obfuscation. A user's guide for privacy and protest.* Cambridge, MA: The MIT Press.

Carney, M. (2013, May 20). You are your data: The scary future of the quantified self movement. [Web log post]. Retrieved from http://pando.com/2013/05/20/you-are-your-data-thescary-future-of-the-quantified-self-movement/

Carr, N. (2012, 27 September). The crisis in higher education. *MIT Technology Review.* Retrieved from http://www.technologyreview.com/featuredstory/429376/the-crisis-in-higher-education/

Crawford, K. (2013, 1 April). The hidden biases in big data. *Harvard Business Review*. Retrieved from http://blogs.hbr.org/cs/2013/04/the_hidden_biases_in_big_data.html

Crawford, K., & Schultz, J. (2013). Big data and due process: Towards a framework to redress predictive privacy harms. *Boston College Law Review, 55(1)*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2325784

Christensen, C. (2008). Disruptive innovation and catalytic change in higher education. In *Forum Futures 2008 (A compilation of summaries presented at the Forum's 2007 Aspen Symposium)* (pp.43—46). Retrieved from EDUCAUSE library website https://net.educause.edu/forum/ff08.asp

Danaher, J. (2014, 7 January). Rule by algorithm? Big data and the threat of algocracy. [Web log post] Retrieved from http://ieet.org/index.php/IEET/more/danaher20140107

Davies, J. (2013, 13 March). The qualified self. [Web log post]. http://thesocietypages.org/cyborgology/2013/03/13/thequalified-self/

Dennis, K. (2008). Viewpoint: Keeping a close watch — the rise of self-surveillance and the threat of digital exposure. *The Sociological Review*, *56*(3), 347–357. http://dx.doi.org/10.1111/j.1467-954X.2008.00793.x

Eynon, R. (2013). The rise of big data: What does it mean for education, technology, and media research? *Learning, Media and Technology, 38*(3), 237–240. http://dx.doi.org/10.1080/17439884.2013.771783

Fineman, M. A. (2008). The vulnerable subject: Anchoring equality in the human condition. *Yale Journal of Law & Feminism*, *20*(1), 8–40.

Gangadharan, S. P. (2012). Digital inclusion and data profiling. *First Monday*, *17*(5). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/3821

Gašević, D., & Siemens, G. (2015). Let's not forget: Learning analytics are about learning. *TechTrends, 59*(1), 64–71. http://dx.doi.org/10.1007/s11528-014-0822-x

Gitelman, L. (Ed.). (2013). "Raw data" is an oxymoron. London: MIT Press.

Greenwood, D., Stopczynski, A., Sweat, B., Hardjono, T., & Pentland, A. (2015). The new deal on data: A framework for institutional controls. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good* (pp. 192–210). New York: Cambridge University Press.

Gurses, S. (2015). Privacy and security: Can you engineer privacy? *Communications of the ACM, 57*(8), 20–23. http://dx.doi.org/10.1145/2633029

Haggerty, K. D., & Ericson, R. V. (Eds.) (2006). *The new politics of surveillance and visibility*. Toronto, ON: University of Toronto Press.

Harcourt, B. E. (2015). *Exposed: Desire and disobedience in the digital age.* Cambridge, MA: Harvard

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

University Press.

Henman, P. (2004). Targeted!: Population segmentation, electronic surveillance and governing the unemployed in Australia. *International Sociology, 19*, 173–191. http://dx.doi.org/10.1177/0268580904042899

Howard, R. D., McLaughlin, G. W., & Knight, W. E. (Eds.). (2012 *infrastructures*). *The handbook of institutional research.* San Francisco, CA: John Wiley & Sons.

Kerr, I., & Barrigar, J. (2012). Privacy, identity and anonymity. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *Routledge handbook of surveillance studies* (pp. 386–394). Abingdon, UK: Routledge.

Kitchen, R. (2014). *The data revolution: Big data, open data, data and their consequences.* London: SAGE.

Knox, D. (2010). *Spies in the house of learning: A typology of surveillance in online learning environments.* Paper presented at the International Conference on Teaching and Teacher Education (Edge2010), Memorial University of Newfoundland, St. Johns, NL, Canada. Retrieved from http://www.mun.ca/edge2010/wp-content/uploads/Knox-Dan-Spies-In-the-House.pdf

Kruse, A., and Pongsajapan, R. (2012). Student-centered learning analytics. Retrieved from https://cndls.georgetown.edu/m/documents/thoughtpaper-krusepongsajapan.pdf

Lane, J., Stodden, V., Bender, S., & Nissenbaum, H. (Eds.). (2015). *Privacy, big data, and the public good*. New York: Cambridge University Press.

Lanier, J. (2013, 1 November). How should we think about privacy? Making sense of one of the thorniest issues of the digital age. *Scientific American, 309*(5), 64–71.

Lazar, N. (2015). The big picture: Big data and privacy. *CHANCE*, *28*(1), 39–42. http://dx.doi.org/10.1080/09332480.2015.1016848

Lupton, D. (2012, 4 November). The quantified self-movement: Some sociological perspectives. [Web log post]. Retrieved from http://simplysociology.wordpress.com/2012/11/04/thequantitative-self-movement-some-sociological-perspectives/

Lupton, D. (2014a, 28 July). Beyond the quantified self: The reflexive monitoring self. [Web log post]. https://simplysociology.wordpress.com/2014/07/28/beyondthe-quantified-self-the-reflexive-monitoring-self/

Lupton, D. (2014b). You are your data: Self-tracking practices and concepts of data. In S. Selke (Ed.), *Lifelogging: Theoretical approaches and case studies about self-tracking* (provisional title). Berlin: Springer.

Lyon, D. (Ed.). (2006). *Theorising surveillance: The panopticon and beyond*. Cullumpton, UK: Willan Publishing.

Lyon, D. (2015). The Snowden stakes: Challenges for understanding surveillance today. *Surveillance & Society*, *13*(2), 139–152.

Mackenzie, C., Rogers, W., & Dodds, S. (Eds.). (2014). *Vulnerability: New essays in ethics and feminist philosophy*. Oxford, UK: Oxford University Press.

Maringe, F., & Sing, N. (2014). Theorising research with vulnerable people in higher education: Ethical and methodological challenges. *South African Journal of Higher Education, 28*(2), 533–549.

Marwick, A. E. (2014, 9 January). How your data are being deeply mined. *The New York Review of Books*. Retrieved from http://www.nybooks.com/articles/archives/2014/jan/09/how-your-data-are-being-deeply-mined/

Marx, G. T. (2001). Murky conceptual waters: The public and the private. *Ethics and Information Technology, 3*, 157–169. http://dx.doi.org/10.1023/A:1012456832336

Marx, G. T., & Muschert, G. W. (2007). Personal information, borders, and the new surveillance studies. *Annual Review of Law and Social Science.* http://dx.doi.org/10.1146/annurev.lawsocsci.3.081806.112824

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

Mayer-Schönberger, V. (2009). *Delete: The virtue of forgetting in the digital age.* Princeton, NJ: Princeton University Press.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think.* New York: Houghton Mifflin Harcourt Publishing.

Miltgen, C. L., & Smith, H. J. (2015). Exploring information privacy regulation, risks, trust, and behavior. *Information & Management*, *52*(6), 741–759. http://dx.doi.org/10.1016/j.im.2015.06.006

Miyazaki, D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*(1), 54–61.

Morozov, E. (2013). *To save everything, click here.* London: Penguin Books.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford, CA: Stanford Law Books.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48.

O'Connell, A. (2016). My entire life is online: Informed consent, big data, and decolonial knowledge. *Intersectionalities: A Global Journal of Social Work Analysis, Research, Polity, and Practice*, *5*(1), 68–93.

Ohm, P. (2010). Broken promises of privacy: Responding to the surprising failure of anonymisation. *UCLA Law Review, 57*, 1701–1777.

Ohm, P. (2015). Changing the rules: General principles for data use and analysis. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), *Privacy, big data, and the public good* (pp. 96–111). New York: Cambridge University Press.

Open University (2014). *Policy on ethical use of student data for learning analytics.* Retrieved from http://www.open.ac.uk/students/charter/essential-documents/ethical-use-student-data-learning-analytics-policy

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information.* London: Harvard University Press.

Payne, R. (2014). Frictionless sharing and digital promiscuity. *Communication and Critical/Cultural Studies*, *11*(2), 85–102. http://dx.doi.org/10.1080/14791420.2013.873942

Pew Research Center (2014, 12 November). *Public perceptions of privacy and security in the post-Snowden era*. Retrieved from http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/

Prinsloo, P. (2015). *The ethics of (not) knowing our students.* Presentation at the Ethics Roundtable, 3 September, University of South Africa, Pretoria. Retrieved at http://www.slideshare.net/prinsp/the-ethics-of-not-knowing-our-students-52373670

Prinsloo, P., Archer, L., Barnes, G., Chetty, Y., & Van Zyl, D. (2015). (Big)ger data as better data in open distance learning. *International Review of Research in Open and Distance Learning (IRRODL), 16*(1).Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/1948/3203

Prinsloo, P., & Slade, S. (2014). Educational triage in higher online education: Walking a moral tightrope. *International Review of Research in Open Distance Learning (IRRODL)*, *14*(4): 306–331. http://www.irrodl.org/index.php/irrodl/article/view/1881

Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. *Proceedings of the 5th International Conference on Learning Analytics and Knowledge (LAK '15),* 83–92. http://dx.doi.org/10.1145/2723576.2723585

Prinsloo, P., Slade, S., & Van Zyl, D. (in press). Students' privacy calculus: Negotiating boundaries of trust, disclosure and benefit [Draft manuscript].

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, *15*(1). Retrieved from http://firstmonday.org/ojs/index.php/fm/article/viewArticle/2775

(2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182. http://dx.doi.org/10.18608/jla.2016.31.10

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

Schildkamp, K., Lay, M. K., & Earl, L. (Eds.). (2013). *Data-based decision making in education: Challenges and opportunities.* London: Springer.

Selinger, E. (2015). Neo-liberal reform and the big data university. *Foundations of Science*, 1–4. http://dx.doi.org/10.1007/s10699-015-9446-7

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist*, *57*(10), 1510–1529. http://dx.doi.org/10.1177/0002764213479366

Solove, D. J. (2001). Privacy and power: Computer databases and metaphors for information privacy. *Stanford Law Review, 53*(6), 1393–1462.

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155.

Solove, D. J. (2004). *The digital person: Technology and privacy in the information age.* New York: New York University Press.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–564.

Solove, D. J. (2007). "I've got nothing to hide" and other misunderstandings of privacy. *San Diego Law Review*, *44*, 745–772.

Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *126 Harvard Law Review* 1880.

Stiles, R. J. (2012). Understanding and managing the risks of analytics in higher education: A guide. *EDUCAUSE*. Retrieved from https://net.educause.edu/ir/library/pdf/EPUB1201.pdf

Stoddart, E. (2012). A surveillance of care: Evaluating surveillance ethically. In K. Ball, K. D. Haggerty, & D. Lyon (Eds.), *The Routledge handbook of surveillance studies* (pp. 369–376). Abingdon, UK: Routledge.

Subotzky, G., & Prinsloo, P. (2011). Turning the tide: A socio-critical model and framework for improving student success in open distance learning at the University of South Africa. *Distance Education*, *32*(2), 177–193. http://dx.doi.org/10.1080/01587919.2011.584846

Swain, H. (2013, 5 August). Are universities collecting too much information on staff and students? *The Guardian.* Retrieved from http://www.theguardian.com/education/2013/aug/05/electronic-data-trail-huddersfield-loughborough-university

Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 239,* 1–36.

Totaro, P., & Ninno, D. (2014). The concept of algorithm as an interpretive key of modern rationality. *Theory Culture Society, 31*, 29–49. http://dx.doi.org/10.1177/0263276413510051

Wardrope, A. (2015). Medicalization and epistemic injustice. *Medicine, Health Care and Philosophy*, *18*(3), 341–352. http://dx.doi.org/10.1007/s11019-014-9608-3

Watters, A. (2012, 5 September). Unbundling and unmooring: Technology and the higher ed tsunami. *EDUCAUSE Review.* Retrieved from http://www.educause.edu/ero/article/unbundling-and-unmooring-technology-and-higher-ed-tsunami

Watters, A. (2013, 13 October). Student data is the new oil: MOOCs, metaphor, and money. [Web log post]. Retrieved from http://www.hackeducation.com/2013/10/17/studentdata-is-the-new-oil

Weber, R. H. (2015). The digital future: A challenge for privacy? *Computer Law & Security Review*, *31*(2), 234–242. http://dx.doi.org/10.1016/j.clsr.2015.01.003

Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of Social Issues*, *59*(2), 431–453.

Willis, J. E., Slade, S., & Prinsloo, P. (In press). Ethical oversight of student data in learning analytics: A typology derived from a cross-continental, cross-institutional perspective. Submitted to the Special issue of *Educational Technology Research and Development*