Student Vulnerability and Agency in Networked, Digital Learning

Paul Prinsloo, University of South Africa, South Africa,
Sharon Slade, The Open University, United Kingdom

Abstract

The collection, analysis, and increased use of students' (digital) data promises to increase the effectiveness of student learning, but also potentially to increase student vulnerability. Given the asymmetrical power relationship between higher education institutions and students, they may have little insight or choice into data collected, how it is stored and used, and opportunities to verify or provide context for collected data.

In the context of increasing uses of online teaching and learning we face the dilemma that regulatory data privacy frameworks often lag technological developments and data uses. We should move beyond thinking in binary terms of permitting simple opt in or opt out, and begin to explore the possibilities of reciprocal care by institutions and students in the collection, analysis and use of their data.

This paper explores the promise and perils of learning analytics through the interpretive lens of *student vulnerability and agency*. An applied framework provides a basis for a student-centred approach to learning analytics which values student agency and recognises the fiduciary duty of higher education towards learning analytics as moral practice.

Abstract in German

Die Erfassung, Analyse und der zunehmende Gebrauch studentischer Daten versprechen zum einen eine höhere Effektivität im Bereich des studentischen Lernens, zum anderen könnten diese jedoch eine größere Vulnerabilität für Studenten zur Folge haben.

Angesichts der Tatsache, dass zwischen Hochschuleinrichtungen und Studenten ein unausgeglichenes Machtverhältnis besteht, scheint es, dass Studenten eine geringe Einsicht in erfasste Daten haben und nur wenig Einfluss darauf wie diese gespeichert und genutzt werden. Des Weiteren scheint es, dass sie keine Möglichkeit haben die gespeicherten Daten zu überprüfen oder diese in einen Kontext zu stellen.

Aufgrund des zunhemenden Gebrauchs von "Online Teaching and Learning", werden wir mit der Problematik konfrontiert, dass behördliche Datenschutzrichtlinien häufig der technischen Entwicklung, sowie der Datennutzung im Wege stehen. Wir sollten das Denken in binären Strukturen bezüglich der Zulassung von "Opt-ins oder Opt-outs" überwinden, und stattdessen beginnen die Möglichkeit gegenseitiger Nachsicht (von Hochschulinstituion und Studenten) bezüglich Datenerfassung, -auswertung und –nutzung wahrzunehmen.

Dieser Beitrag untersucht die Verheißung und Risiken von Bildungsanalytik wobei sich der Fokus auf die Vulnerabilität und Handlungsmacht von Studenten richtet.

Ein angewandtes Rahmenkonzept bietet die Grundlage für ein studenten-zentriertes Konzept der Bildungsanalytik, welches die Handlungsmacht von Studenten wertschaetzt. Zudem nimmt es die Verantwortung von Hochschulinstitutionen bezueglich der Bildungsanalytik als moralisches Handeln wahr.

Keywords: learning analytics, student data, agency, vulnerability

Introduction

> *"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).*

It is hard (if not almost impossible) to underestimate the extent to which our lives have become entangled in the technologies we use, generating an ever-increasing amount of data collected, analysed and used by a variety of users acting in unison and competition in an "elaborate lattice of information networking" (Solove, 2004; p.3). And so we are beginning to transform into "informational organisms (*inforgs*) mutually connected and embedded in an informational environment (the infosphere), which we share with other informational agents, both natural and artificial, that also process information logically and autonomously" (Floridi, 2014; p.94). As we connect and are connected in many often unintentional ways with increasingly uncertain outcomes, individual privacy is perhaps becoming 'the dearest of our possessions' (Floridi, 2014; p.101). In this hyperconnected world, there is no allowance for hermits, and our digital footprints have become the windows into our souls (Marx, 2016).

It is crucial that we remember, as Boam and Webb (2014) suggest above, that as we engage with individuals' data, we should remember that behind and embedded in the data are contexts and narratives, vulnerabilities and agency. Remembering this is increasingly important amidst the vast changes sweeping the higher education landscape, with the increasing need to use data to define and ensure the effectiveness of teaching and learning. Data and evidence-based management have become the mantra in higher education to ensure accountability and efficiency in an increasingly resource-constrained and competitive higher education landscape (Altbach et al., 2009; Prinsloo, 2016a). Learning analytics, as a research focus and educational practice, focuses on "students and their learning behaviours, gathering data from course management and student information systems in order to improve student success" (Oblinger, 2012; p.11). (Also see Prinsloo & Slade, 2014; Griffiths, Drachsler, Kickmeier-Rust, Hoel, & Greller, 2016; Sclater, Peasgood & Mullan, 2016).

As teaching and learning move progressively online and digital, the volume of student data increases exponentially, opening opportunities for data-informed strategies and pedagogies. Sclater et al. (2016) suggest that "Implementing learning analytics is often one strand of a wider institutional strategy, although even a small scale pilot can generate increased awareness and discussion around issues such as retention. …Thus analytics can have beneficial effects beyond the immediate aims of the project, and can be part of a cultural change towards more evidence based-decision making" (p.22). Though there is no doubt that the collection, analysis and use of student digital data can offer huge potential, they bring associated risks and ethical challenges. Sclater et al. (2016) propose that the threats in the conceptualisation and implementation of learning analytics include "ethical and data privacy issues, 'over-analysis' and the lack of generalisability of the results, possibilities for misclassification of patterns, and contradictory findings" (p.16). There are additional concerns such as the belief that data is neutral; the role of algorithms and the algorithmic turn in higher education; the assumptions and epistemologies informing the collection and analysis and use of data; and the increasing possibilities for discriminating against already vulnerable and at-risk students (Drachsler & Greller, 2016; Griffiths et al., 2016; Slade & Prinsloo, 2013; Prinsloo & Slade, 2014).

Student vulnerability and agency should be reviewed in the broader context of the increasing pervasiveness of surveillance in institutions of learning (Knox, 2010; Prinsloo, 2016b; Tucker & Vance, 2016). Tucker and Vance (2016) for example point to tensions between surveillance resulting both in students feeling more secure and as a potential deterrent for bad behaviours, and the sense that "surveilled students may

feel they are in a less nurturing, comfortable learning environment" (p.8). These authors also warn that surveillance and the tracking of students may perpetuate historical and present injustices and biases.

This paper follows Prinsloo (2014) who proposes that "Learning analytics are a structuring device, not neutral, informed by current beliefs about what counts as knowledge and learning, coloured by assumptions about gender/ race/ class/ capital/ literacy and in service of and perpetuating existing or new power relations". Though the collection, analysis and use of student digital data aims to decrease students' vulnerability and risks of failing or dropping out, there is also the possibility that student vulnerability may actually be exacerbated in the light of the asymmetrical power relationship between student and institutions of higher learning. As higher education institutions (HEIs) move to optimise the potential of learning analytics, this paper proposes that institutions should adopt a student-centric approach to learning analytics, empowering students to make informed decisions about the type of data they share, the uses of that data and access to the data collected by higher education.

Privacy in Beta

Nissenbaum (2010) highlights definitions, assumptions and practices regarding personal privacy as challenged by advances in information technology that enable "pervasive surveillance, massive databases, and lightning-speed distribution of information across the globe" (p.1). National and institutional regulatory frameworks often struggle to keep up with technological developments and changing societal norms (Westin, 2003). Griffiths et al., (2016) point to the fact that the "technological environment in education is increasingly complex" with cloud-based and wearable technologies eroding the traditional "institutional silos of student information" (p.1). Learning analytics as a discourse, practice and emergent research focus is found in the nexus between various discourses and practices such as surveillance and privacy studies, information science, ethics and philosophy, as well as educational and learning theories, to mention but a few. For the purpose of this article, we explore student vulnerability and agency in the context of the broader discourses on privacy and surveillance studies (Drachsler & Greller, 2016; Griffiths et al., 2016; Slade & Prinsloo, 2013). Griffiths et al., (2016) state that learning analytics "inevitably partakes in the ethical ambiguity of the educational system as a whole", and "unplanned consequences of educational activities and interventions" (p.3). Learning analytics applications are furthermore "opportunistic, making use of the opportunities presented by bringing together data in ways which were not anticipated by those who decided to collect that

data in the first place" (p.3). As such learning analytics should account for how it protects and safeguards students' privacy.

Whilst privacy has traditionally been understood to encompass the "right to be left alone" as well as having sufficient control to restrict unauthorised access to personal information (Xu, 2011), Solove (2006) cites BeVier who suggests that "privacy is a chameleon-like word, used denotatively to designate a wide range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy" (p.479). In a recent study, Marx (2016) suggests that "Privacy, like the weather, is much discussed, little understood, and not easy to control" (p.27). Not only is the concept multidimensional and fluid, its contours are "often ill-defined, contested, and negotiated [and] dependent on context and culture" (Marx, 2016; p.27). Xu (2011) states that in the context of online social networks, conceptualisations of privacy "have been somewhat patchy" (p.1100). Contrary to the belief that the notion of privacy entails a "unitary concepts with a uniform value, which is unvarying across different situations" (Solove, 2006; p.480), we should see privacy as a "multifaceted concept" (Xu, 2011; p.1079) and pluralistic. Xu (2011) helpfully proposes that neither "privacy as control" nor "privacy as restricted access" (p.1080) are sufficient to encompass the complexities and layers inherent in privacy (Pasquale, 2012; 2015).

Blackall (2013) makes the interesting proposition that data is not about privacy in the first place, but rather about power, about determining who sees (collects, analyses and uses data); whether those who are the objects of data collection have access or input to the collection, analysis or uses. While there are ample examples of positive applications of "Data as power" (Blackall, 2013), there are equally, and possibly increasing concerns about the detrimental and potentially abusive effects of the use of data (e.g. O'Neil, 2016). Exactly because data *is* irrevocably linked to power, there is an increasing amount of pushback and activism surrounding uses of data, for example, from indigenous people's perspectives (Kukutai & Taylor, 2016) and discourses surrounding decolonisation (Prinsloo, 2016b).

While it is tempting to embrace a binary approach which views the collection, analysis and use of student data as either good or bad, it is clear that such an approach is overly simplistic. A further complicating factor is the impact of the asymmetrical power relationships on which most Terms and Conditions are based and which are typically "drafted by one party and offered to the other on a take-it-or-leave-it basis" (NYU, 2015; par.1). Solove (2004) therefore proposes that most "discussions of privacy merely scratch the surface" and that we need "a better understanding of the problems;

we must learn how they developed, how they are connected, what precisely they threaten, and how they can be solved" (p.6).

Marx (2016), for example, explores the tensions, value and conflicts in individual privacy and notes a number of contradictions such as the desire to seek privacy and a form of anonymity, whilst also to acknowledging that secrecy can "hide dastardly deeds and that visibility can bring accountability" (p.299). Indeed, too much transparency may inhibit creativity, experimentation and the taking of risks and disallow individuals from redeeming themselves from past errors of judgement (also see Mayer-Schönberger, 2009). There is also the sense that "many of us want to both see and be seen, even as we also want to look the other way and be left alone. We want to know, and we also want to be shielded from knowing" (Marx, 2016; p.299). We emphasise and value the right to have access to information, but yet, we also want to be assured that some information should not be available for public consumption. Individuals also want their individuality respected and enjoy personalised services – but in order to have our individuality respected and receive personalised services, we need to disclose ever increasing amounts of personal information resulting in an ever-increasing "risk of manipulation, misuse, and privacy violation" (Marx, 2016; p.300). These contradictions and tensions in our expectations and definitions of privacy reflect a misguided "either/or fallacy" (Marx, 2016; p.302) that prevents a proper understanding of the complexities and nuances pertaining to privacy in a networked and digitally pervasive world.

It falls outside the scope of this article to (dis)entangle the different views and theories on privacy (see for example Floridi, 2005, 2006, 2013, 2014; Floridi & Taddeo, 2016; Marx, 2016; Nissenbaum, 2010). It is sufficient to recognise that consensus around the definition, scope, contours and borders of the notion of privacy is fragile and fluid, and frustrates efforts to develop regulatory frameworks that safeguard individuals' right to privacy, protect individuals and enable them to make informed choices. Despite/amidst acknowledging the fragility and fluidity inherent in making sense of privacy, we embrace the suggestion by Floridi (2014) that privacy is "the dearest of our possessions" (p.101). Should we accept, as Floridi (2014) proposes, that human nature is informational so that the information and data that we generate are not distinct from who and what we are, but an integral part of us. As such our right to privacy is "a right to personal immunity from unknown, undesired, or unintentional changes in one's own identity as an informational entity, both *actively* and *passively*" (p.120). Our personal information and data and our identity as individuals "are co-referential, or two sides of the same coin. There is no difference because 'you are your information',

so anything done to your information, is done to you" (Floridi, 2014; p.120). Seeing personal information and privacy as constituting who you are, is vastly different from seeing personal information as a possession. Floridi (2014) proposes then that violations of informational personal are "now more fruitfully compared to kidnapping rather than trespassing" (p.120). Seeing informational privacy in ontological terms resolves the issue between public and private, personal spaces – "Trespassing makes no sense in a public space, but kidnapping is a crime independently of where it where it is committed" (Floridi, 2014; p.121).

Student Vulnerability and Agency as Lens

If then we proceed from the above stance of regarding student information privacy in ontological terms, rather than in terms of *ownership* and the binary between public and private, it provides us with a richer basis for exploring student vulnerability and agency.

As is clear from the many studies on privacy, data protection and surveillance, there are many possible lenses to choose from when mapping the complexities and nuances of the collection, analysis and use of personal data. Selecting student vulnerability and agency as lens offers one of many possible interpretations of the promises and dilemmas in the use of students' (digital) data. Combining both the notions of vulnerability and agency offers an interesting heuristic, acknowledging on the one hand that individuals not only willingly share data and personal information in what describes as "digital promiscuity" (Murphy, 2014), but also "do not understand the extent to which their activities generate data that is being collected, analysed, and put to use for varied governmental and business purposes" (Allen, 2016).

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). Despite and amid the asymmetrical power relationship between students and institutions of higher learning, Prinsloo and Slade (2015) state that it is important to note that vulnerability refers not only to the exposure to risk of individuals but also broader society – see, for example, Bauman (2007) as well as the increasing vulnerability of institutions of higher learning due to, inter alia, changing funding regimes and increasing competition (Altbach, Reisberg, & Rumbley, 2009). The increasing resource constraints, competitiveness, and the need to optimise the return-on-investment in the allocation of resources necessitate the need for higher education institutions to collect and use data, including student data, in order to plan more effectively (Prinsloo & Slade, 2014).

Baker and Siemens (2014) point to the potential of learning analytics made possible due to increasing quantities of data, standardised formats of educational data, increased computational power and the availability of a range of analytical tools. As a result students are increasingly exposed and vulnerable as they study online and are confronted by the all-pervasive gaze of the institution. Prinsloo and Slade (2015) state that, 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 also be used inappropriately and unethically, further increasing the vulnerability of students. Like the notion of privacy, the notion of vulnerability is "undertheorised" (Mackenzie et al., 2014; p.2). Current theoretical thinking suggests that vulnerability is not only a key characteristic of human life, but a defining characteristic. This does not preclude the fact that certain individuals and groups are "more than ordinarily vulnerable" (Sellman quoted by Mackenzie et al., 2014; p.2) (Also see Fineman, 2008; Maringe & Singh, 2014; Trowler, 2014). In this paper we use the notion of vulnerability as *ontological* lens that "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). (Also see Floridi, 2014). This is of particular concern in the context of learning analytics.

Whilst highlighting student vulnerability, we should add the counter-balance of individuals' responsibility for self-care (e.g. Allen, 2016; Tene & Polonetsky, 2012a, 2012b). In acknowledging the asymmetries in the primary power relationships and the often limited and lagging protection offered by legislation and lengthy Terms and Conditions, individuals also have choices and responsibilities and an ethical duty to self-care and self-respect that "entail reservation and circumspection when it comes to sharing potentially sensitive information and the intimacies of identity and personality" (Allen, 2016).

A brief Overview of Some Current Approaches to Addressing Online Vulnerability and Agency

There are a number of approaches that combine to increase the protection of individuals' information and decrease vulnerability, as well as facilitating a more effective management of privacy. Xu (2011), for example, warns that most current approaches focus on individual agency but, given that individuals' information may be accessed due to ignorance of privacy and security of others, we should take a different approach when discussing individual agency. "Optimistic bias" impacts both on the steps which individuals take to control the disclosure and access to their personal

information and "the degree of ease with which [users'] online profiles and their personal information are visible and exposed to others" (p.1083). Though we would assume that individuals make rational decisions regarding the sharing and protection of their information, it is safer and possibly more realistic to speak about a "bounded rationality". That is, "individuals may genuinely want to protect their information privacy, but … may opt for immediate benefits of information disclosure, rather than carefully calculating long-term risks of information disclosure" (p.1088). Clearly there is a difference between acknowledging risks to personal privacy and embracing personal responsibility, self-care and self-respect (see Allen, 2016).

Traditionally the main strategy to protect privacy and provide individuals with choice is to provide a facility to opt in or out. A number of authors (e.g., Acharya & Gorman, 2013; Antón & Earp, 2004; Bellman et al., 2001; Earp et al., 2005; Pasquale, 2012; Prinsloo & Slade, 2015) however point to the failures of providing opting in or out as sufficient to protect against online vulnerability. For example, research done by Bellman et al (2001) points to a variety of aspects that might impact on individuals' decision to opt in or out, such as the default settings of the choice, the typeface and font size used, the length and technical complexity of the Terms and Conditions (TACs), and the framing of the options.

A more nuanced approach is proposed by Miyazaki and Fernandez (2000) who map a range of options regarding the collection, analysis, use and sharing of personal information in the context of e-commerce. Possibilities of disclosure range from (a) never collecting data or identifying customers when they access a site; (b) customers opting in by explicitly agreeing to having their data collected, used and shared; (c) customers explicitly opting out; (d) the constant collection of data without consumers having a choice (but with their knowledge); and (e) the collection, use and sharing of personal data without the user's knowledge. Prinsloo and Slade (2015) refer to the Organisation for Economic Cooperation and Development's (OECD) position that "prior affirmative consent in all cases would be impractical" and it can be assumed that should users be required to set up an account to use the services, they implicitly agree to the terms and conditions. Ohm (2015) notes that once data has been legitimately acquired, current legal frameworks do not dictate of the scope and constraints regarding the use of such data. There is therefore a need for a "new deal on data" (Greenwood et al., 2015; p.192). Though Greenwood et al. (2015) specifically refer to changes needed in the regulatory frameworks governing the collection, use and sharing of data, these frameworks are but one part of the bigger strategy to address individual digital vulnerability.

Another approach is offered by Xu (2011) who provides a very helpful framework with regard to privacy management distinguishing between *personal* control, *collective* control and *proxy* control.

- *Personal* or individual privacy management involves both behavioural self-protection and technological self-protection. (Also see Acharya & Gorman, 2013).
- *Collective* privacy management refers to a group accepting the responsibility for co-responsibility of privacy and addressing risk. Though individuals may make informed decisions regarding what they share on which platforms, it may not be the case that others sharing that information will take the same amount of care – e.g., the practice of *tagging* and *untagging*. Sharing practices on Facebook, for example, highlight the "complexities of collective privacy management, the tensions of content ownership, and the effects that one user uploading and tagging a picture of another can have on the latter's relationships with friends, family, employers, etc." (Xu, 2011; p.1093). (See Xu (2011) for a discussion on privacy-enhancing technologies for collective privacy control).
- *Proxy* privacy control refers to the practice of individuals and groups who align themselves to "a powerful force in order to gain control through powerful others" in recognition that individuals and groups often lack skills or knowledge in protecting information privacy (Xu & Teo in Xu, 2011; p.1095). Proxy privacy management includes, but is not limited to, industry self-regulation and government regulation. An interesting development in proxy privacy management is the development of accreditation authorities such as TRUSTe, BBBonline and Webtrust who will verify an organisation's privacy management TOC and their adherence to it (Antón & Earp, 2004).

A more recent example of a framework that maps the complexities and nuances is proposed by Marx (2016; pp.303-304) and is framed by four questions:

- What is the ratio of what a technology is capable of to how extensively it is applied? (*surveillance slack ratio*)
- What is the ratio of what is known about a person to the absolute amount of personal information potentially available? (*personal information penetration ratio*)

- What is the ratio of what individuals wish to keep to themselves to how able they are to do this, given the technology, laws, and policies? (*achieved privacy ratio*)
- What is the ratio of what superordinates know about subordinates to what subordinates know about superordinates? (*reciprocity-equity-ratio*)

As is clear then, there are several ways to approach the dilemmas and tensions in providing optimum and appropriate protection of individuals that also include empowerment to ask more informed questions. (Also see Allen (2016) and Tene & Polonetsky (2012a, 2012b)).

Towards a Framework for the Protection of Student Vulnerability and Enabling Student Agency

In the process of maturing as an established (and accepted) educational practice and research focus, concerns about the ethical and privacy considerations in learning analytics have moved from the margins toward becoming a central focus in learning analytics studies (Prinsloo & Slade, 2016). Despite huge advances in charting different approaches to map and safeguard student privacy (see e.g. Drachsler & Greller, 2016; Griffiths et al., 2016; Prinsloo & Slade, 2016) – there are still concerns and a lag in implementing more ethical approaches. Perhaps as a result of the fluidness and fragility of privacy (as pointed out above) and contesting agendas pertaining to the collection, analysis and use of student data, Griffiths et al., (2016) (still) ask "Is privacy a show-stopper for learning analytics?" (p.1).

While we acknowledge the vast advances in theorising and mapping more ethical approaches to the collection, analysis and use of student data, we would like to see the main value contribution of this article as highlighting student vulnerability and agency. For example, in an earlier work (Prinsloo & Slade, 2015) we suggest a framework to mitigate student vulnerability and optimise student agency. The framework includes (a) the duty of reciprocal care; (b) the contextual integrity of privacy and data; (c) the centrality of student agency and privacy self-management; (d) the need to rethink consent and employing nudges; (e) developing partial privacy self-management; (f) adjusting privacy's timing and focus; and (g) moving toward substance over neutrality and moving from quantified selves to qualified selves.

Though HEIs have the right to collect, analyse, use and share data within the scope of their mandate, learning analytics should also be located within the ambit of the fiduciary duty of the providers. Though the balance of power lies with the providing

institution, students are not mere data objects but can (and should) participate in the collection, analysis and the verification of data. Prinsloo and Slade (2015) therefore suggest that educational providers make their TACs "as accessible and understandable as possible" making clear "what data is collected, for what purposes, and with whom the data may be shared (and under what conditions)". 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". From a procedural perspective, this might necessitate the appointment of a neutral ombudsperson to address concerns and issues flowing from the contract between institution and students. The fact that the collection of student data takes place within an asymmetrical power relationship does not exempt students from a responsibility to ensure that their data is correct and current. As already acknowledged, since data and algorithms are not neutral but are embedded in ontological and epistemological positions and assumptions, it is crucial that the contextual integrity of data and especially historical data is recorded, open for scrutiny and preserved. As historical data are increasingly aggregated and re-used in contexts and for purposes different from the original context and purpose in which the data was collected, it is necessary to prevent contextual integrity collapse.

There are many perspectives of education but if it is seen as "moral practice" (Slade & Prinsloo, 2013) and given the imbalanced inherent power relationships, we should aim to critically explore the range of student control over what data will be analysed, for what purposes, and how students will have access to verify, correct or supply additional information. If students are rightly seen as agents and active collaborators in the harvesting, analysis and use of their data, 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 (Kruse & Ponsajapan, 2012). As Prinsloo and Slade (2015) state, "it is no longer acceptable to assume as default a position where students must accept that registration equates to forfeit of control over their data".

The framework proposed by Antón and Earp (2004) and Earp et al. (2005) offers another useful approach to safeguarding student privacy and enabling student agency. The framework maps 12 categories against which organisations can check that stated and actual policies are internally consistent and reflect customer preferences. The two central elements of the framework are "privacy protection goal classification" (desired protection of user privacy rights) and "privacy vulnerability goal classification"

(potential for invasions of privacy). Table 1 provides a useful application of the framework to a higher education and learning analytics context. For each element of the framework, we emphasise the importance of fully considering the reciprocal aspects of care and responsibility in order to address various nuances of vulnerability, but also to mitigate against any potential impact on student vulnerability which might result from the asymmetrical power relationship.

Table 1: Privacy policy taxonomy: Privacy protection and vulnerability goals, adapted from Earp et al. (2005)

Privacy protection goal classification	Privacy vulnerability goal classification
Notice/Awareness – informing students regarding the type of data collected, timing of collection, protection and storage, sharing of data.	Information monitoring – students should be informed regarding not only the scope and use of data collected, but also methods of collection, e.g. cookies, whether the data will be re-shared and with whom, etc. However, we suggest that students should be more than informed data objects – they should also be permitted to actively participate in a range of activities that may impact on their studies in biased or detrimental ways. For example, determining the purposes and scope of data collection, as well as safeguards and strategies to ensure the verification of information and provide context for any findings/analyses.
Choice/Consent – the range of available options goes beyond the simple binary of opting in or out. Institutions must explore various possibilities to enlarge students' participation and awareness.	Information aggregation – historical data is increasingly combined with recent or current data to provide more complete user digital profiles. Students should be better informed regarding the extent and impact of aggregation as well as steps taken to prevent the re-identification or re-personalisation of aggregated data. There is ample evidence regarding ways in which historical data potentially skews institutional perceptions of student potential and risk. Data such pre-higher education experience and performance, home addresses, income classifications, etc., may adversely affect students' choice and their risk profiles. Students ought then to be involved in making sense of the validity and impact of these variables and be clearer regarding how the institution's assumptions and beliefs about these variables impact on students' choices and access to

resources.
If "data is power" (Blackall, 2013), it is especially important that HEIs acknowledge those inherent vulnerabilities which flow from student data.

Access/Participation – though the collection of most student data takes place behind institutional firewalls, HEIs should investigate the various layers of access and/or participation with various levels of exposure and collection of data. Though Earp et al (2005) only flag the possibility of opting in or out, we suggest that students should also be provided access to data to ensure its accuracy and, where necessary, provide additional information to ensure contextual integrity.

Integrity/Security – students should be provided with the assurance that the data collected will be kept secure and not shared without prior consent.

Enforcement/Redress – not only should students be held responsible for ensuring the accuracy of information, but they should be held accountable where fellow-student information is shared outside the institution's regulatory/policy environment.

Information storage – refers to what data is stored, the governance of data and access control. As Blackall (2013) suggests, consideration should be given to who collects, analyses and makes use of student data, as well as allowing data objects to engage with their data and subsequent analyses, and participate in the sense making of data. Considering student data as an integral part of the ontology of students (Floridi, 2014) raises the responsibility of need for effective and appropriate safeguards.

Information transfer – students have a right to know what type of data will be shared with whom, and under which circumstances. (See Floridi, 2014; Knox, 2010).

Information collection – students need to be informed regarding the scope, type, use, methods and timing of data collection – whether by targeted collection through, e.g., surveys, or by collecting browser information, IP addresses, etc. (See Knox, 2010).

Information personalisation – the mere personalisation of a user's experience when accessing a web site (e.g., 'Welcome back Paul') points to the nature of data collected and used. Students should be informed and provide consent to the personalisation of services where possible. We need to take account of context and make space for student narrative as an integral part of the collection, analysis and use of student data (Boam & Webb, 2014)/

Contact – For what purposes may students be contacted, how and by whom? We need to consider student data in terms of not only preventing "trespassing" but in terms of "kidnapping" (Floridi, 2014)

(In)conclusions

In line with a student centred approach to learning analytics (Kruse & Pongsajapan, 2012), the renewed emphasis that learning analytics is about "learning" (Gašević & Siemens, 2015) and embracing the agency of students will allow students and HEIs to move from seeing students as data objects or students seeing themselves as quantified selves but rather as qualified selves (Davies, 2013; Lupton, 2014a, 2014b). Through the quantification practices in higher education, students' vulnerability is increased when they see themselves, their potential and their futures, as presented in the number of clicks, logins, time-on-task. We are more than our data (Carney, 2013). "Where the quantified self gives us the raw numbers, the qualified self completes our understanding of those numbers" (Carney, 2013; par.8). Our students are therefore much more than just conglomerates of quantifiable data and it is important that we take into account "the contexts in which numbers are created" (Lupton, 2014b; p.6).

In this article we accept student informational privacy as "ontological" (Floridi, 2014) which strengthens the need to explore student vulnerability and agency. Protecting student information and privacy in ontological terms means that our frameworks and strategies must go beyond protecting their information and data from being stolen and misused, and rather protect student data as an integral part of who they are. We should remember that student data are much more than what can be quantified. In our collection, analysis and use of student data we should recognise student identity, context and narratives as embedded in the data we collect, analyse and use. Only when we combine student identity, context and narrative (as proposed by Boam & Webb, 2014; Floridi, 2014), can we deepen our understanding of student vulnerability and agency.

References

1. Acharya, S., & Gorman, S. (2013). Reclaiming information privacy online. *Colonial Academic Alliance Undergraduate Research Journal, 4*(1), 1-15. Retrieved from http://scholarworks.gsu.edu/caaurj/vol4/iss1/4

2. Allen, A. L. (2016, December 9). Protecting one's own privacy in a Big Data economy. [Blog post] Harvard Law Review Forum. Retrieved from http://harvardlawreview.org/2016/12/protecting-ones-own-privacy-in-a-big-data-economy/

3. Altbach, P. G., Reisberg, L., & Rumbley, L. E. (2009). *Trends in global higher education: tracking an academic revolution.* A report prepared for the UNESCO World Conference on Higher Education. Paris. UNESCO. Retrieved from http://atepie.cep.edu.rs/public/Altbach,_Reisberg,_Rumbley_Tracking_an_Academic_Revolution,_UNESCO_2009.pdf

4. Antón, A. I., & Earp, J. B. (2004). A requirements taxonomy for reducing Web site privacy vulnerabilities. *Requirements Engineering, 9*(3), 169-185. Retrieved from http://link.springer.com/article/10.1007/s00766-003-0183-z

5. Baker, S.J. D., & Siemens, G. (2014). *Educational data mining and learning analytics. Cambridge Handbook of the Learning Sciences.* Retrieved from http://www.columbia.edu/~rsb2162/BakerSiemensHandbook2013.pdf

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

7. 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. Retrieved from http://dl.acm.org/citation.cfm?id=359241

8. Blackall, L. (2013, October 1). Data and power. Presentation given to the University Analytics Forum in Melbourne. Retrieved from https://www.youtube.com/watch?v=TgPsrPRa1t8

9. Boam, E., & Webb, J. (2014, May 2). The qualified self: going beyond quantification. [Blog post] Design Mind – Collection No. 5., Insights Sensing. Retrieved from http://designmind.frogdesign.com/2014/05/qualified-self-going-beyond-quantification/

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

11. Davies, J. (2013, March 13). The qualified self. [Blog post] The Society Pages – Cyborgology. Retrieved from http://thesocietypages.org/cyborgology/2013/03/13/the-qualified-self/

12. Drachsler, H., & Greller, W. (2016). *Privacy and learning analytics – it's a DELICATE issue.* Retrieved from http://dspace.ou.nl/bitstream/1820/6381/1/Privacy%20a%20DELICATE%20issue%20%28Drachsler%20%26%20Greller%29%20-%20submitted.pdf

13. Earp, J. B., Antón, A. I., Aiman-Smith, L., Stufflebeam, W. H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management, 52*(2), 227-237. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.8232&rep=rep1&type=pdf

14. Fineman, M. A. (2008). The vulnerable subject: anchoring equality in the human condition. *The Yale Journal of Law & Feminism, 1*, 1-23. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/yjfem20&div=4&id=&page=

15. Floridi, L. (2005). The ontological interpretation of informational privacy. Ethics and Information *Technology, 7*(4), 185-200.

16. Floridi, L. (2006). Four challenges for a theory of informational privacy. *Ethics and Information technology, 8*(3), 109-119.

17. Floridi, L. (2013). *The ethics of information.* Oxford, UK: Oxford University Press.

18. Floridi, l. (2014). *The fourth revolution.* Oxford, UK: Oxford University Press.

19. Floridi, L., & Taddeo, M. (2016). What is data ethics? *Philosophical Transactions A, 374*(2083), 1-5. doi : 10.1098/rsta.2016.0360. Retrieved from http://rsta.royalsocietypublishing.org/content/roypta/374/2083/20160360.full.pdf

20. Gašević, D., & Siemens, G. (2015). Let's not forget: learning analytics are about learning. *TechTrends, 95*(1), 64-71. Retrieved from http://link.springer.com/article/10.1007/s11528-014-0822-x

21. Griffiths, D., Drachsler, H., Kickmeier-Rust, M., Hoel, T., & Greller, W. (2016). *Is privacy a show-stopper for learning analytics? A review of current issues and solutions. Learning Analytics Review 6. LACE.* Retrieved from http://www.laceproject.eu/learning-analytics-review/is-privacy-a-show-stopper/

22. 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, NY: Cambridge University Press.

23. Knox, D. (2010). *Spies in the house of learning. A typology of surveillance in online learning environments.* Paper presented at Edge, Memorial University of Newfoundland, Canada, 12-15 October.

24. Kruse, A., & Pongsajapan, R. (2012). *Student-centered learning analytics.* CNDLS Thought Papers. Retrieved from https://cndls.georgetown.edu/m/documents/thoughtpaper-krusepongsajapan.pdf

25. Kukutai, T., & Taylor, J. (Eds.) (2016). *Indigenous data sovereignty. Toward an agenda.* Research Monograph no. 38. Australian National University Press. Retrieved from https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty

26. Lupton, D. (2014a, July 28). Beyond the quantified self: the reflexive monitoring self. [Blog post] This Sociological Life. Retrieved from https://simplysociology.wordpress.com/2014/07/28/beyond-the-quantified-self-the-reflexive-monitoring-self/

27. Lupton, D. (2014b). *You are your data: self-tracking practices and concepts of data.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2534211

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

29. 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.

30. Marx, G.T. (2016). *Windows into the soul. Surveillance and society in an age of high technology.* Chicago: University of Chicago Press.

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

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

33. Murphy, K. (2014, October 4). We want privacy, but can't stop sharing. [Blog post] The New York Times. Retrieved from http://www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html?partner=rss&emc=rss&smid=tw-nytopinion

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

35. NYU – New York University (2015, January 30). Focusing on the fine print: Florencia Marotta-Wurgler's ground breaking research on consumer contracts. [Blog post] NYU LAW. Retrieved from http://www.law.nyu.edu/news/ideas/Marotta-Wurgler-standard-form-contracts-fine-print

36. Oblinger, D. G. (2012). Let's talk analytics. *EDUCAUSE Review, July/August*, 10-13.

37. 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, NY: Cambridge University Press.

38. O'Neil, C. (2016). *Weapons of math destruction. How big data increases inequality and threatens democracy.* Great Britain: Allen Lane.

39. Pasquale, F. (2012). Privacy, antitrust, and power. *George Mason Law Review, 20*(4), 1009-1024.

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

41. Prinsloo, P. (2014). *A brave new world: Student surveillance in higher education.* Paper presented at SAAIR, Pretoria, South Africa, 16-18 September. Retrieved from http://www.slideshare.net/prinsp/a-brave-new-world-student-surveillance-in-higher-education

42. Prinsloo, P. (2016a). Evidence-based decision making as séance: implications for learning and student support. In J. Botha & N. Muller (Eds.), *Institutional Research in support of evidence-based decision-making in Higher Education in Southern Africa* (pp. 331-353). Stellenbosch, South Africa: SUN Media.

43. Prinsloo, P. (2016b, November 14). Decolonising the collection, analyses and use of student data: A tentative exploration/proposal. [Blog post] opendistanceteachingandlearning. Retrieved from https://opendistanceteachingandlearning.wordpress.com/2016/11/14/decolonising-the-collection-analyses-and-use-of-student-data-a-tentative-explorationproposal/

44. Prinsloo, P., & Slade, S. (2013). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. *Proceedings of the Third International Conference on Learning Analytics and Knowledge – Leuven, Belgium, 8-12 April*, 240-244. Retrieved from http://dl.acm.org/citation.cfm?id=2460344

45. 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), pp. 306-331. Retrieved from http://www.irrodl.org/index.php/irrodl/article/view/1881

46. Prinsloo, P., & Slade, S. (2015). Student privacy self-management: implications for learning analytics. *Proceedings of the Fifth International Conference on Learning Analytics and Knowledge, LAK15*, 83-92. Retrieved from http://dl.acm.org/citation.cfm?doid=2723576.2723585

47. Prinsloo, P., & Slade, S. (2016). Here be dragons: Mapping student responsibility in learning analytics. In M. Anderson & C. Gavan (Eds.), *Developing Effective Educational Experiences through Learning Analytics* (pp. 174-192). Hershey, Pennsylvania: ICI-Global.

48. Sclater, N., Peasgood, A., & Mullan, J. (2016). *Learning analytics in higher education.* JISC. Retrieved from https://www.jisc.ac.uk/sites/default/files/learning-analytics-in-he-v3.pdf

49. Slade, S., & Prinsloo, P. (2013). Learning analytics: ethical issues and dilemmas. *American Behavioural Scientist, 57*(1), 1509–1528. Retrieved from http://abs.sagepub.com/content/early/2013/03/03/0002764213479366.abstract

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

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

52. Tene, O., & Polonetsky, J. (2012a). Privacy in the age of big data: a time for big decisions. *Stanford Law Review Online, 64.* Retrieved from https://www.stanfordlawreview.org/online/privacy-paradox-privacy-and-big-data/

53. Tene, O., & Polonetsky, J. (2012b). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 239-273. Retrieved from http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1191&context=njtip

54. Trowler, V. (2014). May the subaltern speak? Researching the invisible 'other' in higher education. *European Journal of Higher Education, 4*(1), 42-54. doi: 10.1080/21568235.2013.851614

55. Tucker, J. W. & Vance, A. (2016). *School Surveillance: The consequences for equity and privacy.* National Association of State Boards of Education. Retrieved from http://www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf

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

57. Xu, H. (2011). Reframing Privacy 2.0 in Online Social Network. *Journal of Constitutional Law, 14*(4), 1077-1102. Retrieved from http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1058&context=jcl