STUDENT VULNERABILITY AND AGENCY IN NETWORKED, DIGITAL LEARNING

Paul Prinsloo, University of South Africa, Sharon Slade, Open University

Abstract

The increasing collection, analysis, use and possible sharing of student digital data not only promise to increase the effectiveness of student learning and the effective allocation of institutional resources, but also increase student vulnerability. In the context of the asymmetrical power relationship between higher education institutions and students, students are often seen as data objects with now insight or choice regarding the type of data collected, how the data are stored and used, and opportunities to verify collected data or provide context.

Against the backdrop of Privacy 2.0 and the (in)effectiveness of regulatory frameworks to protect individual data privacy, as well as concerns that thinking in terms of the binary of either opting in or out, we need to critically investigate the collection, analysis and use of student digital data. This paper explores the promise and possible perils of learning analytics through the interpretive lens of student vulnerability. A framework is provided as basis for a student-centred approach to learning analytics where students' agency is valued and optimised within the context of a fiduciary duty of reciprocal care.

Introduction

Amidst vast changes sweeping the higher education landscape, there is an increasing need to use data to increase the effectiveness of teaching and learning, and subsequently, ensure accountability and efficiency in an increasingly resource-constrained and competitive higher education landscape (Altbach et al, 2009). Learning analytics as an emerging discipline and practice promises to contribute to more effective teaching, learning and resource allocation through the collection, analysis and use of student data (Prinsloo & Slade, 2014).

As teaching and learning move progressively online and digital, the amount of student data increases exponentially, opening opportunities for data-informed strategies and pedagogies. Though there is no doubt that the collection, analysis and use of student digital data do offer huge potential, there are also a number of risks and ethical challenges 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 (Slade & Prinsloo, 2013; Prinsloo & Slade, 2014).

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 in the light of the asymmetrical power relationship between student and institutions of higher learning, students' vulnerability may actually be exacerbated. As higher education institutions (HEIs) 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.

This paper explores student vulnerability and agency in the context of the phenomenon of Privacy 2.0.

Privacy 2.0

Central to an investigation of student vulnerability and agency in digital and networked learning is the notion of 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). Solove

(2006) and others therefore state that the notion of privacy is in disarray and increasingly fluid frustrating efforts to define it and to develop regulatory frameworks that safeguard it. 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). The asymmetrical power relationship is further embedded given that Terms and Conditions 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). Our definitions, as well as our legal and regulatory frameworks often struggle to keep up with technological developments and changing societal norms (Westin, 2003). HEIs have been caught un(der)prepared by, on the one hand, optimising the collection and analysis of student data, and on the other hand, protecting student privacy (Prinsloo & Slade, 2013).

Student vulnerability as lens

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 amidst 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) and institutions of higher learning (Altbach, Reisberg & Rumbley, 2009).

Though this paper specifically focuses on student vulnerability in the context of online and networked learning, we should also recognise that the higher education landscape is changing substantially, resulting in increasing resource constraints, competitiveness, and the need to optimise the collection and use of 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). This is of particular concern in the context of learning analytics.

A brief overview of some current approaches to addressing online vulnerability and agency

Xu (2011) 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 acting on them.

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) 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 (TOC), and the framing of the options.

Miyazaki and Fernandez (2000) provide a much needed, rich and nuanced presentation of 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 (1) never collecting data or identifying customers when they access a site; (2) customers opting in by explicitly agreeing to having their data collected, used and shared; (3) customers explicitly opting out; (4) the constant collection of data without consumers having a choice (but with their knowledge); and (5) 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 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.

Xu (2011), for example, 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. With regard to the latter, Acharya and Gorman (2013) provide a very helpful overview and review of tools such as Ghostery and BetterPrivacy, and a variety of encryption services.

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).

Towards a framework of student agency

Prinsloo & Slade (2015) suggest a framework to mitigate student vulnerability and optimise student agency. The framework includes (1) the duty of reciprocal care; (2) the contextual integrity of privacy and data; (3) the centrality of student agency and privacy self-management; (4) the need to rethink consent and employing nudges; (5) developing partial privacy self-management; (6) adjusting privacy's timing and focus; and (7) 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 & Slade (2015) therefore suggest that educational providers 'make their TOCs 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 approaches to education but if education is seen as moral practice (Slade & Prinsloo, 2013) and given the asymmetrical power relationship between students and institution, we need 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 & 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 used by Antón & Earp (2004) and Earp et al (2005) offers a useful starting point by providing a number of ways in which HEIs might optimise student participation whilst reducing the level and experiences of vulnerability and risk. The two central elements of the framework are 'privacy protection goal classification' and 'privacy vulnerability goal classification' (see Table 1 for an overview). For each element of the framework, it is crucial to fully consider 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, eg cookies, whether the data will be re-shared and with whom, etc.
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 informed regarding the extent and impact of aggregation as well as steps to prevent the re-identification or re-personalisation of aggregated 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.	**Information storage** – refers to what data is stored, the governance of data and access control.
Integrity/Security – students should be provided with the assurance that the data collected will be kept secure and not shared without prior consent.	**Information transfer** – students have a right to know what type of data will be shared with whom, and under which circumstances.
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 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.

	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 where possible, provide consent to the personalisation of services.
	Contact – How and for what purposes may students be contacted and by whom?

(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).

'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).

References

1. ACHARYA, S., & GORMAN, S. (2013). Reclaiming information privacy online. *Colonial Academic Alliance Undergraduate Research Journa*l, 4(1), pp. 1-15. Retrieved from http://scholarworks.gsu.edu/caaurj/vol4/iss1/4
2. 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
3. ANTON, A.I., & EARP, J.B. (2004). A requirements taxonomy for reducing Web site privacy vulnerabilities. Requirements Eng, 9, pp. 169-185. Retrieved from http://link.springer.com/article/10.1007/s00766-003-0183-z
4. 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
5. BAUMAN, Z. (2007). *Liquid times. Living in an age of uncertainty.* Cambridge, UK: Polity Press.
6. BELLMAN, S., JOHNSON, E.J., & LOHSE, G.L. (2001). To opt-in or opt-out? It depends on the question. Retrieved from http://dl.acm.org/citation.cfm?id=359241
7. BOAM, E., & WEBB, J. (2014, May 2). The qualified self: going beyond quantification. [Web log post]. Retrieved from http://designmind.frogdesign.com/2014/05/qualified-self-going-beyond-quantification/
8. CARNEY, M. 2013. You are your data: the scary future of the quantified self movement. [Personal web log]. Retrieved from http://pando.com/2013/05/20/you-are-your-data-the-scary-future-of-the-quantified-self-movement/
9. DAVIES, J. 2013, March 13. The qualified self. [Web log post]. Retrieved from http://thesocietypages.org/cyborgology/2013/03/13/the-qualified-self/
10. EARP, J.B., ANTON, A.I., AIMAN-SMIT, L., 7 STUFFLEBEAM, W.H. (2005). Examining Internet privacy policies within the context of user privacy values. *IEEE Transactions on Engineering Management,* 52(2), pp. 227-237. Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.138.8232&rep=rep1&type=pdf
11. FINEMAN, M.A. (2008). The vulnerable subject: anchoring equality in the human condition. *The Yale JL & Feminism,* 1, pp. 1-23. Retrieved from http://heinonline.org/HOL/LandingPage?handle=hein.journals/yjfem20&div=4&id=&page=

12. GAŠEVIĆ, D., & SIEMENS, G. 2015. Let's not forget: learning analytics are about learning. *TechTrends*. Retrieved from http://link.springer.com/article/10.1007/s11528-014-0822-x
13. 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.
14. KRUSE, A., & PONGSAJAPAN, R. (2012). Student-centered learning analytics. Retrieved from https://cndls.georgetown.edu/m/documents/thoughtpaper-krusepongsajapan.pdf
15. LUPTON, D. (2014a, July 28). Beyond the quantified self: the reflexive monitoring self. [Web log post]. Retrieved from https://simplysociology.wordpress.com/2014/07/28/beyond-the-quantified-self-the-reflexive-monitoring-self/
16. 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
17. MACKENZIE, C., ROGERS, W., & DODDS, S. (EDS.). 2014. *Vulnerability. New essays in ethics and feminist philosophy*. Oxford University Press: Oxford.
18. 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), pp. 533-549.
19. MIYAZAKI, D., & FERENANDEZ, A. (2000). Internet privacy and security: an examination of online retailer disclosures. *Journal of Public Policy & Marketing,* 19(1), pp. 54-61.
20. NYU (New York University). (2015). Focusing on the fine print: Florencia Marotta-Wurgler's ground breaking research on consumer contracts. [Web log post]. Retrieved from http://www.law.nyu.edu/news/ideas/Marotta-Wurgler-standard-form-contracts-fine-print
21. 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.
22. PASQUALE, F. (2012). Privacy, antitrust, and power. *Geo. Mason L. Rev.*, *20*, pp. 1009-1024.
23. PASQUALE, F. (2015). *The black box society: the secret algorithms that control money and information.* London, UK: Harvard University Press
24. 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
25. PRINSLOO, P., & SLADE, S. (2013). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. Learning Analytics and Knowledge 2013 – Leuven, Belgium, 8-12 April. Retrieved from http://dl.acm.org/citation.cfm?id=2460344
26. 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
27. PRINSLOO, P., & SLADE, S. 2015. Student privacy self-management: implications for learning analytics. LAK15
28. SLADE, S., & PRINSLOO, P. (2013). Learning analytics: ethical issues and dilemmas. American Behavioural Scientist, 57(1) pp. 1509–1528. Retrieved from http://abs.sagepub.com/content/early/2013/03/03/0002764213479366.abstract
29. SOLOVE, D.J. (2004). *The digital person. Technology and privacy in the information age.* New York, NY: New York University Press.
30. SOLOVE, D.J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review,* 154(3), pp. 477-564.
31. TROWLER, V. 2014. May the subaltern speak? Researching the invisible 'other' in higher education. *European Journal of Higher Education, 4*(1), pp. 42-54. DOI: 10.1080/21568235.2013.851614
32. WESTIN, A.F. (2003). Social and political dimensions of privacy. Journal of Social Issues, 59(2), pp. 431-453.
33. XU, H. (2011). Reframing Privacy 2.0 in Online Social Network. *U. Pa. J. Const. L.*, *14*, pp. 1077-1102.