Chapter 11

Eliciting students' preferences for the use of their data for learning analytics

A crowdsourcing approach

Maina Korir, Sharon Slade, Wayne Holmes and Bart Rienties

11.1 Introduction

Higher education institutions (HEIs) collect and use student data to improve operations and course delivery (Siemens, 2013), for research purposes (Griffiths, 2017), and to improve teaching and learning in a process referred to as learning analytics (Long & Siemens, 2011). Examples of such uses are illustrated in Chapter 8 (Rizvi, Rienties, Kizilcec, & Rogaten, 2022) and Chapter 14 (Nguyen, 2022). With the growing shift to blended and online learning in higher education, virtual learning environments (VLEs) facilitate the collection of data about whether and how students interact with learning resources. VLEs are designed to record a vast amount of information about students' behaviour, including number of clicks, time spent on the VLE, number of videos viewed, and number of forum posts (Rizvi, Rienties, Kizilcec, & Rogaten, 2022). This information may be used as a proxy for student engagement with a course, and to predict student success. Furthermore, the insights allow HEIs to improve educational practice in teaching and learning (Nguyen, 2022). Student support teams can identify students thought likely to drop out or fail the course (Foster & Siddle, 2020; Herodotou et al., 2017). These predictions can be made sufficiently early to allow tutors to intervene and support students to improve their performance and outcomes.

The institutional use of student data to facilitate various forms of student success has given rise to ethical and privacy concerns (Ferguson, 2012; Siemens, 2013; Slade & Prinsloo, 2013). Ethics in learning analytics may be understood as "the systematization of correct and incorrect behaviour in virtual spaces" (Pardo & Siemens, 2014, p. 439). Ethical considerations focus on issues such as morality, student identity, and the institutions' obligation to use student data (Slade & Prinsloo, 2013). Privacy in learning analytics may be understood as "the regulation of how personal digital information is being observed by the self or distributed to other observers" (Pardo & Siemens, 2014, p. 438). The value of privacy lies in its ability to promote relationships and autonomy, allowing people to limit what is known about them and to make decisions based on their values, without outside interference (Rubel & Jones, 2016).

Empirical research has consistently demonstrated that students are often unaware of the use of their data for learning analytics (Jones et al., 2020; Roberts, Howell,

DOI: 10.4324/9781003177098-13

Seaman, & Gibson, 2016), and the student data their institution collects (Sun, Mhaidli, Watel, Brooks, & Schaub, 2019). When informed about potential uses of their data, students express varied responses: such as indicating a lack of concern about the use of their data in cases where the recipient and data uses are made clear (Vu, Adkins, & Henderson, 2019), and accepting institutional use of their data to benefit their learning (Slade, Prinsloo, & Khalil, 2019). At the same time, students also express concern, for instance, about being surveilled or tracked (Slade & Prinsloo, 2014). Consequently, there seem to be inconsistent perceptions of students and privacy concern in learning analytics.

An area for further research, within the context of student privacy and learning analytics, is that of students' perceptions of the transactional nature of learning analytics (Ferguson, 2019; Wintrup, 2017). Students are asked (or are presumed) to consent to the use of their data for learning analytics so that data can be used for potentially beneficial purposes such as the provision of learning recommendations, or recommendations for remedial action and to improve student performance (Ho, 2017; Siemens, 2013). Use of student data in these ways has potential for privacy harms, that is, possible injury to students through the collection and use of their data (MacCarthy, 2014). This includes loss of autonomy (Rubel & Jones, 2016), profiling, and identification of the individual whose data is used (Solove, 2009). While there is insightful research on students' perspectives of the ethics and privacy of learning analytics, little is known about students' perceptions of this risk/benefit trade-off and their preferences for the use of their data. Chapter 11 offers additional insights in this context.

11.1.1 Empirical research on students and privacy in learning analytics

Findings from a number of studies converge on a common theme that students lack an awareness of learning analytics and about how their data is used for this purpose (Jones et al., 2020; Sun, Mhaidli, Watel, Brooks, & Schaub, 2019). In general, where they are informed about learning analytics, what data is used, and for what purpose, it might be argued that students appear positive about institutional use of their data to enhance their own and other students' learning. This is based on data collected using semi-structured interviews with 112 undergraduate students across eight universities in the USA (Jones et al., 2020). Other work, with a sample of students at a UK university, involving a survey (with 674 students) and focus group discussions (with 26 students) (Tsai, Whitelock-Wainwright, & Gašević, 2020) supports this perspective, as students in the focus groups indicated their support for institutional use of their data, but only for what they considered as legitimate purposes, namely, to comply with legal requirements, to improve educational services, and to improve the university's overall performance. It is noted that this positive perspective is conditional, thus, it is not clear whether negative perceptions of data use might arise in cases where there is insufficient institutional transparency surrounding use of student data.

One possible benefit of transparency about institutional use of student data is a reduction in privacy concerns as suggested by the work of Vu, Adkins, and Henderson (2019) who distributed a survey to 1,647 students at various HEIs in the USA. However, as previously stated, there are mixed results within the context of students' privacy concerns about data use for learning analytics. In contrast to the findings of Vu, Adkins, and Henderson (2019), students in the study by Ifenthaler and Schumacher (2016) were willing to share data related to their studies, but were less willing to share personal data or data trails collected from their use of a VLE. More specifically, of the 333 students who filled out the survey, 84% were willing to share course enrolment data, compared to 8% who agreed to share their medical data, and 9% who agreed to share their online user path for learning analytics purposes.

The role of students' acceptance of data use in exchange for learning-related benefits has been examined qualitatively in work by Tsai, Whitelock-Wainwright, and Gašević (2020) and quantitatively in work by Slade, Prinsloo, and Khalil (2019). In the latter case, the authors indicate that 74% of the 215 study participants stated that they were comfortable with the collection of their personal data in exchange for benefits such as personalised support. However, to the best of our knowledge, there is currently limited to no empirical research that has explored students' perspectives of the privacy risks inherent in the use of their data for learning analytics.

The privacy calculus theory and findings from related research (Dinev & Hart, 2006; Laufer & Wolfe, 1977), suggest that there is a relationship between both perception of privacy risks and benefits of data use, and willingness to share personal information. Specifically, where there is a high perception of privacy risk, users are less willing to transact with their personal information (Dinev & Hart, 2006), whereas users expecting to receive benefits are observed to share more data (Li, Rathindra, & Xu, 2010). Therefore, the following research questions were identified for Chapter 11:

1 To what extent does an awareness of the possible privacy risks and/or the benefits of data use for learning analytics influence students' data use preferences?
2 What do students indicate as the motivation for their data use preferences?

11.1.2 Methods

11.1.2.1 Setting and participants

Using the crowdsourcing platform Prolific, a sample was drawn from UK-based students. We sought to recruit an equal number of male and female participants. With respect to participants' ages, research findings have demonstrated that older adults express higher levels of privacy concern than younger adults (Black, Setterfield, & Warren, 2018). Therefore, we recruited participants aged between 18 and 25 years to enhance our evaluation of the influence of the interventions. A

total of 447 participants took part in the study. There were 216 male (48.3%) and 231 female (51.7%) participants. The mean age was 20.6 (SD = 1.86). Most of the participants (409–91.5%) were studying at university and the remainder were in further education (38–8.5%).

11.1.3 Study materials

All participants were shown a sample learning analytics dashboard (Figure 11.1), a data use preference prototype (Figure 11.2), and the privacy risks and/or benefits interventions (Figure 11.3). The latter was not provided to participants in the control group. The design of the sample learning analytics dashboard was based on the OU Analyse interface (Kuzilek, Hlosta, Herrmannova, Zdrahal, & Wolff, 2015) and was simplified to maintain participants' focus on the study aims.

The data use preference prototype showed participants two types of data that can be used for learning analytics, specifically data about the student and data about the students' activities on the online learning platform (Sclater, Peasgood, & Mullan, 2016).

The privacy risks intervention was developed using Solove's (2009) taxonomy of privacy harms. The first risk (1) is referred to at the beginning and end of the description. It relates to the information collection category of the taxonomy and the risk of surveillance. The second risk (2) falls under the information processing category of the taxonomy, and the risk of aggregation. The third risk (3) is also in the information processing category of the taxonomy, under the risk of identification. Additionally, the benefits intervention presented nudging, prediction, and recommendation of learning resources as benefits for students based on the use of their data.

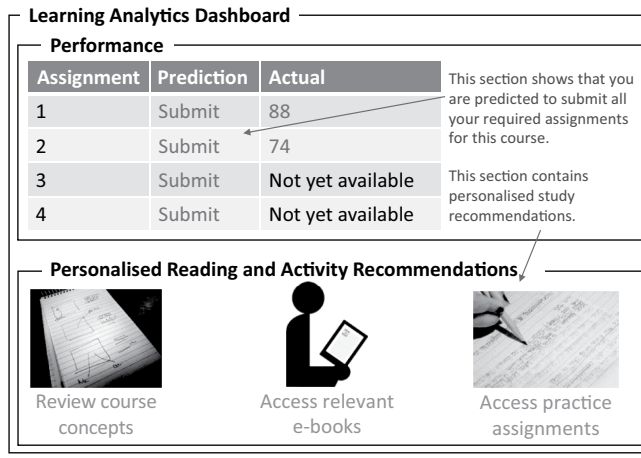

Figure 11.1 The sample learning analytics dashboard.

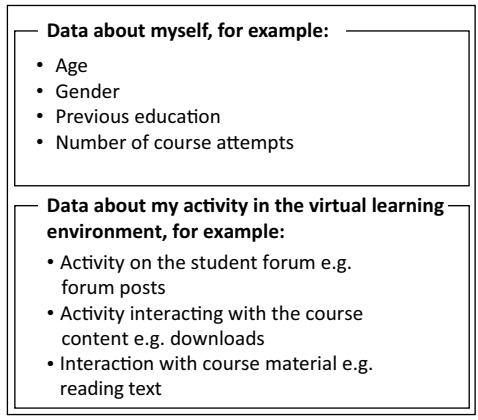

Figure 11.2 Examples of student data used for learning analytics.

Possible privacy risks of data use

We will monitor what you and other students are doing on the online learning platform [1]. Data that you and other students have provided to separate information systems at your learning institution (for example during registration) will be combined to form a digital profile [2]. The digital profile can be linked to the individual student [3], and this information will be used to make decisions about you and other students, such as predicting your performance and giving you study recommendations [1].

Possible benefits of data use

We can offer you personalised support to help you complete the course, including nudging to submit assignments or follow up from the student support team. We can also provide you with personalised recommendations of learning materials that can improve your understanding of the course material.

Figure 11.3 Descriptions of the privacy risks and benefits.

11.1.4 Study measures

Three measures of data use preferences, concern over data use, and concern over privacy risks were created. It was necessary to create these three measures as there was limited research on students' data use preferences in the learning analytics context, and therefore there were few opportunities to identify questions from related research as recommended in best practice for questionnaire design (Bryman, 2016; Groves et al., 2009).

Four other study measures were obtained from published research. The scale perceived usefulness of learning analytics was adapted from Arbaugh (2000) who developed it with 114 students in a study on student satisfaction with MBA courses. The sharing data scale was developed with over 300 students in Germany (Ifenthaler & Schumacher, 2016). The scale perception of benefit from data use for learning analytics was adapted from Naeini et al. (2017) who used it with 1,014 participants in a study on privacy preferences in the Internet of Things. Finally, the Internet

Users Information Privacy Concern (IUIPC) scale (Malhotra, Kim, & Agarwal, 2004) was developed in two studies with over 700 participants and has been used extensively to measure users' privacy concerns. The scales used in the study were modified to include a "not applicable" option following recommendations by Aldridge and Levine (2001) and Krosnick (2018) to allow participants to respond even if a question did not apply to them. Additionally, attention check questions were used to ensure that spurious data could be detected in the data cleaning phase (Egelman, Chi, & Dow, 2014).

11.1.5 Study design and procedures

A between-subjects design was used where each participant was randomly assigned to one of four groups: the risks group, the benefits group, the risks and benefits groups, and the control group. After providing consent to take part in the study, participants indicated their data use preference (pre-test), choosing between preferring to share no data, only data about themselves, only data about their activities on the learning platform, or both data about themselves and their activities on the learning platform. They were given brief background information on learning analytics and then viewed the sample learning analytics dashboard. In the experimental condition participants were shown the intervention, and afterwards they indicated their level of concern for the stated privacy risks and their perception of the benefits. Participants were then asked to assess the usefulness of the learning analytics dashboard features and indicate whether they were concerned about the use of their data. They again provided their data use preferences (post-test) and indicated their general privacy concern, before providing demographic information at the end of the study.

11.2 Results

11.2.1 The influence of risks and benefits awareness on participants' data use preferences

In terms of RQ1, the descriptive statistics for participants' data use preferences in terms of the mean and standard deviation are shown in Table 11.1. There was a decrease in the mean values (post-test) for the control group and the risks group, and an increase in the mean values for the benefits group. At the same time, the mean values for the risks and benefits group remained unchanged. In other words, the results suggest that the awareness intervention might have had an influence on participants' data use preferences in the risks, and in the benefits group, but made no difference in the risks and benefits group. It might be that any increase in participants' data use preferences (thereby indicating a willingness to share more data) resulting from the benefits intervention was tempered by the risks intervention.

There was a slight decrease comparing the overall post-test and pre-test mean scores (pre-test mean = 3.03, SD = 0.90; post-test mean = 3.00, SD = 0.94). A paired samples t-test revealed that these differences were not statistically significant

Table 11.1 Descriptive statistics of students' pre-test and post-test data use preferences by experimental group

	Data use preference pre-test		*Data use preference post-test*		
Condition	*Mean*	*Std. Deviation*	*Mean*	*Std. Deviation*	*N*
Control	3.09	0.976	2.97	0.98	128
Risks	2.93	0.906	2.89	0.934	104
Benefits	3.04	0.858	3.07	0.906	104
Risks and benefits	3.05	0.824	3.05	0.923	111

($p > .340$). A one-way ANOVA revealed no significant differences among the means of the four groups on pre-test data use preferences ($F(3, 443) = 0.637$, $p > .590$), and post-test data use preferences ($F(3, 443) = 0.786$, $p > .501$). Finally, using McNemar's test, as the variables were at the nominal measurement level, we determined that there was no statistically significant difference in participants' data use preferences pre- and post-intervention ($p > -.140$).

11.2.2 Motivation for participants' data use preferences

11.2.2.1 Theme 1: Support for institutional use of student data

Two main themes were identified from participants' open responses in order to address RQ2. The first theme indicated participants' support for institutional use of student data (49% of codes, $n = 238$), and participants gave several reasons for their data use preferences (80% of codes, $n = 190$ (out of 238 codes)), for example, that the data shared was sufficient or appropriate for the stated purposes (19% of codes, $n = 37$ (out of 190 codes)). Their perception of the data being sufficient took on several forms, for example, they shared what was most relevant (38% of codes, $n = 14$ (out of 190 codes)), was less invasive (19% of codes, $n = 7$ (out of 190 codes)), felt comfortable or safe for them to share (19% of codes, $n = 7$ (out of 190 codes)), or what they thought showed their engagement (11% of codes, $n = 4$ (out of 190 codes)). As participant 161 stated:

> Because that is directly related to my learning and doesn't take into consideration other factors which may not assess academic performance.
>
> (P161, risks group, Female, willing to share data about activities, no change in data use preference)

This code suggests that the way student data will be used is a useful information point in transparency initiatives as students might relate to one or more of the stated purposes, thereby agreeing to the use of their data, as seen in (Slade & Prinsloo, 2014).

Participants additionally expressed several expectations of what the learning institution should do with their data (9% of codes, $n = 21$ (out of 238 codes)). For example, they expressed an expectation for purpose limitation (33% of codes, $n = 7$ (out of 21 codes), that is, that only academic data would be used for academic purposes:

> I do not think it is appropriate to use data about a student's private life and background to make a judgement on their academic performance. It is not fair to do so, as it could lead to discrimination and unfair bias. A student's academic performance and private life should be separate and it is not the place of the university to be able to access that data or use it to judge a person's abilities. Their abilities should be judged solely on their present engagement with the course and their previous academic record.
>
> (P269, control group, Female, willing to share data about activities, no change in data use preference)

Here we see the role that context plays in students' expectations of institutional data use. In contextual integrity (Nissenbaum, 2004), there are generally expectations around what information about a person can and cannot be revealed in a given context.

Finally, participants were observed to make trade-offs in data use for benefits even while supporting the use of student data (4% of codes, $n = 9$ (out of 238 codes)). For instance, participants indicated that they had shared just enough to protect privacy (44% of codes, $n = 4$ (out of 9 codes)), that they sought the best balance between privacy and services for students (22% of codes, $n = 2$ (out of 9 codes)), they were getting something back for their information (11% of codes, $n = 1$ (out of 9 codes)), and that the benefits outweighed the privacy risks (11% of codes, $n = 1$ (out of 9 codes)).

11.2.2.2 Theme 2: Hesitation about institutional use of student data

The second theme highlighted participants' hesitation about institutional use of student data (51% of codes, $n = 247$). Participants provided various reasons why they hesitated to share (all) their data. These reasons clarified why they chose to share some data, that is data about themselves or data about their activities (43% of codes, $n = 104$ (out of 247 codes)). One reason that participants agreed on was that personal details were either not needed or should not be shared (42% of codes, $n = 44$ (out of 104 codes)). A preference for privacy (23% of codes, $n = 24$ (out of 104 codes)) was another reason why participants hesitated to share their data, as participant 64 stated:

> I tend to avoid giving away personal information as I like to be private. Information about what I do on my university's learning platform is ok though.
>
> (P64, risks group, Male, willing to share data about activities, no change in data use preference)

As explained previously, the context influenced the participant's data use preference, helping him make an exception because it was the university's learning platform.

Furthermore, participants raised ethical and privacy considerations (35% of codes, $n = 87$ (out of 247 codes)). Their responses captured their concern about (potential) bias, discrimination, or prejudice (21% of codes, $n = 18$ (out of 87 codes)).

> I feel the knowledge of certain things such as my gender may be used to discriminate.
>
> (P412, risks group, Female, not willing to share data, change to prefer to share no data)

The example above demonstrates that transparency initiatives may cause students, where they can control whether their data is used, to prefer not to share any data. As this participant was in the risks group, the change in their data use preference was unsurprising. Transparency initiatives in learning institutions should seek to balance information about privacy risks alongside information about benefits, thereby enabling students to make informed decisions about the use of their data.

Additionally, participants raised concerns that institutional use of student data as described in the study could negatively impact students (18% of codes, $n = 16$ (out of 87 codes)), for instance, that students would be pressured to behave in a certain way:

> With more information, I could determine that the personal information used would be almost a breach of my privacy, and even giving away data about my use of the learning platform is somewhat private to me, as I would like to privately access learning materials without feeling pressure (for example if I downloaded some materials a little late in the course, or past a deadline).
>
> (P425, control group, Male, willing to share data about activities, change to prefer to share no data)

Finally, other concerns were raised including that the data use was privacy invasive (8% of codes, $n = 7$ (out of 87 codes)), and that the data could only give a partial picture of the student (8% of codes, $n = 7$ (out of 87 codes)).

There was some tension observed between understanding the need for data use and discomfort with data use (12% of codes, $n = 29$ (out of 247 codes)) where participants appeared in two minds about the use of data. Participants were seen to express an understanding, for instance, that institutional data use was needed, alongside seemingly contradictory views, such as expressing corresponding concerns about discrimination, or a sense that the data use was privacy invasive:

> I don't mind giving basic information about myself since that would be fairly easy to get anyway, but I do not like to have everything about me being

> tracked even it could have some minor benefits to helping me improve my performance.
>
> (P424, Risks and benefits group, Female, willing to share data about self, no change in data use preference)

Finally, participants expressed a desire for boundaries or separation in data use across their personal lives and their lives as students (8% of codes, $n = 19$ (out of 247 codes)). They were keen to keep academic and private life separate or their online activity separate from student life:

> At first I thought it might be a good idea to share some data, but I believe that the suggested options of the data shared/what will be done with it oversteps its boundaries and could have negative effects on performance and mental health. I believe that if the only outcome of the data collection was to improve learning by providing support, then I'd be alright with sharing some of the suggested data.
>
> (P326, control group, Female, willing to share data about self and activities, change to prefer to share no data)

11.3 Discussion and moving forwards

In Chapter 11 participants were presented with privacy risks and/or benefits interventions to examine whether and how these would influence their data use preferences. While we observed slight changes to participants' data use preferences, these changes were not statistically significant (RQ1). Therefore, we analysed participants' open responses to better understand motivations for their data use preferences (RQ2).

We identified nuances in participants' responses as they expressed support for institutional use of student data for learning analytics alongside hesitation to support institutional use of student data. While one would expect either full support for use of student data or complete refusal to support the same, participants' responses suggested a middle ground where this apparent tension between support and hesitation co-existed.

Participants' responses indicated that they made trade-offs to arrive at what was an acceptable use of student data for them. This suggests a hidden negotiation process that students go through. Learning institutions can provide supporting structures such as inviting and publicly responding to students' questions on institutional data use to make these tensions and negotiations visible. There are also different student preferences to consider and support. While some students might want to choose what data is used, others may find this effort a step too far. However, this apparent apathy should not be construed as students lacking an interest in or having no concerns over the privacy of their data (Hargittai & Marwick, 2016).

Throughout Chapter 11 we noted that participants had contrasting views on what data was appropriate to share and why. For example, one student shared data about themselves saying that was less invasive, while another student shared data

about their activities on the online learning platform for the same reason. This suggests a need to enhance students' data literacy. For instance, they may not know that their personal data has less prominence in the statistical models over time and data about their activities on the learning platform becomes more important (Kuzilek, Hlosta, Herrmannova, Zdrahal, & Wolff, 2015). Additionally, it may be unclear whether sharing different data modifies the digital profiles created about students, how the resulting digital profile influences the benefits available to students, and the corresponding privacy harms. In this way, students can make more informed decisions about the use of their data which should be an aim of learning institutions' transparency initiatives.

11.3.1 Implications for practice

We recommend greater transparency from learning institutions about institutional uses of student data. This would require that the relevant content is made accessible and understandable for students, identifying what and how specific data is used for learning analytics purposes. This level of detail in learning institutions' transparency initiatives will be received positively by some students. Teachers can also support institutional efforts for transparency around data use by making students aware of when and how their course data is used for learning analytics. Furthermore, institutions should examine ways to empower students with respect to the use of their data by allowing them to indicate whether they want to participate in learning analytics, and which data items they would be willing to have used for the same. Whatever students choose, ethical practice places a burden on the learning institution to ensure that the benefits truly outweigh any harms.

References

Aldridge, A., & Levine, K. (2001). *Surveying the social world: Principles and practice in survey research*. Milton Keynes: The Open University Press.

Arbaugh, J. B. (2000). Virtual classroom characteristics and student satisfaction with internet-based MBA courses. *Journal of Management Education*, *24*, 32–54.

Black, C., Setterfield, L., & Warren, R. (2018). *Online data privacy from attitudes to action: An evidence review*. Edinburgh: Carnegie UK Trust.

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford: Oxford University Press.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*, 61–80.

Egelman, S., Chi, E. H., & Dow, S. (2014). Crowdsourcing in HCI research. In J. Olson & W. Kellogg (Eds.), *Ways of knowing in HCI* (pp. 267–289). New York, NY: Springer. https://doi.org/10.1007/978-1-4939-0378-8_11

Ferguson, R. (2012). Learning analytics: Drivers, developments and challenges. *International Journal of Technology Enhanced Learning*, *4*, 304–317.

Ferguson, R. (2019). Ethical challenges for learning analytics. *Journal of Learning Analytics*, *6*, 25–30.

Foster, E., & Siddle, R. (2020). The effectiveness of learning analytics for identifying at-risk students in higher education. *Assessment & Evaluation in Higher Education*, *45*, 842–854. doi:10.1080/02602938.2019.1682118

Griffiths, D. (2017). An ethical waiver for learning analytics? In É. Lavoué, H. Drachsler, K. Verbert, J. Broisin, & Pérez-Sanagustín (Eds.), *Data driven approaches in digital education: 12th European conference on technology enhanced learning, EC-TEL 2017, proceedings* (pp. 557–560). Cham: Springer International Publishing. doi:10.1007/978-3-319-66610-5_62

Groves, R. M., Jr., F. J. Couper, M. P. Lepkowski, J. M. Singer, E., & Tourangeau, R. (2009). *Survey methodology* (2nd ed.). Hoboken, NJ: John Wiley & Sons.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication*, *10*, 3737–3757.

Herodotou, C., Rienties, B., Boroowa, A., Zdrahal, Z., Hlosta, M., & Naydenova, G. (2017). Implementing predictive learning analytics on a large scale: The teacher's perspective. In *Proceedings of the seventh international learning analytics & knowledge conference* (pp. 267–271). New York: Association for Computing Machinery. doi:10.1145/3027385.3027397

Ho, A. (2017). *Advancing educational research and student privacy in the 'big data' era*. Washington, DC: National Academy of Education.

Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development*, *64*, 923–938.

Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *Journal of the Association for Information Science and Technology*, *71*, 1044–1059. https://doi.org/10.1002/asi.24358.

Krosnick, J. A. (2018). Questionnaire Design. In D. L. Vannette, & J. A. Krosnick (Eds.), *The Palgrave handbook of survey research* (pp. 439–455). Cham: Springer International Publishing. doi:10.1007/978-3-319-54395-6_53

Kuzilek, J., Hlosta, M., Herrmannova, D., Zdrahal, Z., & Wolff, A. (2015). OU analyse: Analysing at-risk students at The Open University. *Learning Analytics Review*, LAK15-1, 1–16.

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues*, *33*, 22–42. doi:10.1111/j.1540-4560.1977.tb01880.x

Li, H., Rathindra, S., & Xu, H. (2010). Understanding situational online information disclosure as a privacy calculus. *The Journal of Computer Information Systems*, *51*, 62–71.

Li, W., Sun, K., Schaub, F., et al. (2021). Disparities in students' propensity to consent to learning analytics. *International Journal of Artificial Intelligence in Education*. https://doi.org/10.1007/s40593-021-00254-2

Long, P., & Siemens, G. (2011). Penetrating the fog: Analytics in learning and education. *Educause Review*, *46*, 30–40.

MacCarthy, M. (2014). Student privacy: Harm and context. *International Review of Information Ethics*, *21*, 11–24.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*, 336–355.

Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., & Sadeh, N. (2017). Privacy expectations and preferences in an IoT World. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 399–412). USENIX Association. Retrieved from https://www.usenix.org/conference/soups2017/technical-sessions/presentation/naeini

Nguyen, Q., Rienties, B., & Whitelock, D. (2022). Informing learning design in online education using learning analytics of student engagement. In B. Rienties, R. Hampel, E. Scanlon, & D. Whitelock (Eds.), *Open World Learning: Research, innovation and the challenges of high-quality education* (pp. 189–207). London: Routledge.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 119–158.

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, *45*, 438–450.

Rizvi, S., Rienties, B., Kizilcec, R. F., & Rogaten, J. (2022). Culturally adaptive learning design: a mixed-method study of cross-cultural learning design preferences in MOOCs. In B. Rienties, R. Hampel, E. Scanlon, & D. Whitelock (Eds.), *Open World Learning: Research, innovation and the challenges of high-quality education* (pp. 103–116). London: Routledge.

Roberts, L. D., Howell, J. A., Seaman, K., & Gibson, D. C. (2016). Student attitudes toward learning analytics in higher education: "The fitbit version of the learning world". *Frontiers in Psychology*, 7, 1959. doi: 10.3389/fpsyg.2016.01959.

Rubel, A., & Jones, K. M. (2016). Student privacy in learning analytics: An information ethics Perspective. *The Information Society*, *32*, 143–159.

Sclater, N., Peasgood, A., & Mullan, J. (2016). *Learning analytics in higher education: A review of UK and international practice*. London: JISC.

Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist*, *57*, 1380–1400.

Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist*, *57*, 1510–1529.

Slade, S., & Prinsloo, P. (2014). Student perspectives on the use of their data: Between intrusion, surveillance and care. In *Challenges for research into open & distance learning: Doing things better? Doing better things* Eden Conference (pp. 291–300).

Slade, S., Prinsloo, P., & Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. In *Proceedings of the 9th international conference on learning analytics & knowledge* (pp. 235–244). ACM. doi:10.1145/3303772.3303796

Solove, D. (2009). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Sun, K., Mhaidli, A. H., Watel, S., Brooks, C. A., & Schaub, F. (2019). It's my data! Tensions among stakeholders of a learning analytics dashboard. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (pp. 594:1–594:14). ACM. doi:10.1145/3290605.3300824

Tsai, Y.-S., Whitelock-Wainwright, A., & Gašević, D. (2020). The privacy paradox and its implications for learning analytics. In *Proceedings of the tenth international conference on learning analytics & knowledge* (pp. 230–239). Frankfurt, Germany. https://doi.org/10.1145/3375462.3375536

Vu, P., Adkins, M., & Henderson, S. (2019). Aware, but don't really care: Students' perspective on privacy and data collection in online courses. *Journal of Open Flexible and Distance Learning*, *23*, 42–51.

Wintrup, J. (2017). Higher education's panopticon? Learning analytics, ethics and student engagement. *Higher Education Policy*, *30*, 87–103. doi:10.1057/s41307-016-0030-8