Privacy versus pedagogy – students' perceptions of using learning analytics in higher education

Tal Soffer, Anat Cohen
School of Education, Tel Aviv University

The rapid recent use of learning analytics (LA) in higher education, specifically during the COVID-19 pandemic, allows the monitoring of users' behavior while learning. Using LA may promote students' learning outcomes but also intrude into their privacy. This study aimed to explore students' behaviour and perceptions towards privacy and data protection when using LA for pedagogical needs, examine the privacy trade-off of students' willingness to share personal information in exchange for pedagogical benefits and understand the predicting variables for this privacy trade-off. A model was developed containing five groups of influencing variables (demographic data, perceptions, feelings, behaviour and awareness) on the privacy trade-off. A total of 1,014 students completed an online questionnaire. The results found that students do care about their privacy but are not aware of privacy and data protection regulations. They are willing to trade off privacy for pedagogical benefits, and they trust their academic institutions, but they want transparency. Age, a sense of security in the academic institution, behaviour, data misuse concern and institution management of students' personal information are the significant predictors for a privacy trade-off. It is important to engage students in the process as they are the main beneficiaries of LA and build trust between them and the institution.

Implications for practice or policy:

- Academic institution should actively provide information to raise privacy awareness.
- Academic institutions should engage students in the process of using LA to create a high degree of trust.
- Universities should endorse LA policy, fostering it for pedagogical purposes.
- Instructors may utilise LA to enrich student learning, respecting their willingness to share pedagogical data.
- Academic institutions should provide a high level of transparency in order to build students' trust in their institutions.

Keywords: privacy trade-off, privacy perception, higher education, online learning

Introduction

The use of learning analytics (LA) has increased rapidly during the last decade in higher education (Baek & Doleck, 2023). LA includes the measurement, collection, analysis and reporting of data about students. The data collected are used by academic institutions for pedagogical and administrative purposes (Romero & Ventura, 2020). Recently, during the COVID-19 pandemic, there was further use of these technologies for teaching and learning (Caspari-Sadeghi, 2023). This was because most universities were compelled to quickly transfer their teaching from traditional face-to-face courses to online courses in order to provide uninterrupted education. The accelerated use of technologies therefore further enabled academic institutions to collect data on students and their academic activities (Soffer & Cohen, 2019).

LA facilitates the adaptation and improvement of both student learning and lecturers' teaching practices (Khalil et al., 2024) providing pedagogical benefits to students. These include ongoing monitoring of their learning activities, providing feedback on their assignments and adjusting the learning contents to their needs (Gursoy et al., 2017; Schumacher & Ifenthaler, 2018). Despite the pedagogical benefits of LA for students, there is concern that students' privacy may be intruded (Drachsler & Greller, 2016), particularly as academic institutions often do not disclose their data collection processes (Fisher et al., 2014). Studies have indicated that students desire transparency and would like to be informed on the data collection processes, as well as the type of data that has been collected (Roberts et al., 2016). Nevertheless, students are interested in and hope to benefit from the information gathered in the learning management systems for their studies. They also express confidence in their academic institutions to protect their data and prevent its improper use (Fisher et al., 2014; Tsai et al., 2020). In summary, using LA technologies to collect students' data for learning and teaching purposes may promote students' learning outcomes but also intrude on students' privacy. Students are therefore positioned to analyse the costs and benefits related to this information trade – a process known as the privacy trade-off.

The privacy trade-off has also been studied in various fields using information and communication technology (ICT), such as social network services, e-commerce and e-shopping and mobile applications (Bol et al., 2018). However, studies regarding the privacy trade-off in higher education to better understand the type of personal data students are willing to share in exchange for pedagogical benefits is still limited. Those that exist emphasise the need for transparency, trust, and the raising of awareness regarding the type and purpose of data used by academic institutions.

This study aimed to (a) explore students' behaviour and perceptions towards privacy and data protection when using LA for pedagogical needs, (b) examine the privacy trade-off as represented in students' willingness to share personal information in exchange for receiving academic services (pedagogical and administrative) and (c) understand the predicting variables for the privacy trade-off. Consequently, the findings will significantly enhance our understanding of the dynamics between student willingness to trade off their privacy for pedagogical benefits and the development of university policies for the adoption of LA in higher education. This will assist in crafting more effective learning and teaching policies that align with both the educational aspirations of students and the strategic objectives of institutions.

Literature review

Privacy in the digital world

The core of LA is collecting and using data on students (Botnevik et al., 2020). In addition to administrative needs, these data allow for the tracking of students' learning activities, which helps to better understand their learning patterns and provide more personalised and adaptive learning experiences (Tsai et al., 2020). However, when dealing with the issue of collecting and analysing data on students, the challenges of privacy arise. In recent years, although ICT in general and big data and LA have rapidly made inroads into higher education, privacy and ethical issues have become core to the debate, due to their reliance on significant amounts of sensitive student data. Questions have been raised concerning students' rights, awareness and preferences regarding their privacy (Alzahrani et al., 2023).

Privacy is one of the most important values in democratic societies, which provides the individual the right to be independent. There is no single definition to privacy; it is related to philosophical, social, political,and legal discussions. The literature shows that the concept of privacy is not a universal one (Belanger & Crossler, 2011; Shukla et al., 2022). It changes over time and across cultures (Antón et al., 2010). The most famous definition of privacy, on which later ones have been based, was given by the American lawyers Warren and Brandeis (1890, p. 193): "the right to be let alone". With time, the definition of privacy has been expanded to include additional issues. For example, Westin (1967, p. 7) described privacy as "the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others". This definition includes the critical element of data security that in the age of information technologies dominates the discussion of privacy. It is also the freedom of an individual to choose which agents can access specific bits of their own information. Privacy is also about the right to know who collects this information, why the information is being collected and how it will be used (Jones et al., 2020; Vu et al., 2019).

In 2018, due to the rapid penetration of innovative technologies, the privacy regulations were extended by the European Parliament in the General Data Protection Regulation (European Parliament and Council Regulation, 2016). The aim was to provide a more comprehensive and extensive protection of online personal data and how to use it for purely legal purposes (Bharti & Aryal, 2023; Crutzen et al., 2019). Many institutions, including schools and universities, had to follow these regulations and invest resources in implementing them.

The concept of privacy consists of different aspects and can be described as an interest in different dimensions: privacy of the person, which pertains to the integrity of an individual's body; privacy of personal behaviour, which relates to all aspects of behaviour, particularly sensitive matters such as sexual preferences and habits, political activities and religious practices, in both private and public places; privacy of personal communications, which concerns an individual’s interest in being able to communicate, using various media without routine surveillance of their communications by others; and privacy of personal data, which involves control over who has access to an individual’s personal data (Kokolakis, 2017; Presthus & Sørum, 2018).

The impact of LA on privacy and data protection in higher education

Data collection become a core issue with the high usage of learning management systems (LMSs) into academic institutions. LMSs are used in most universities to support hybrid or online environments in teaching and learning. The students interact with the course content (e.g., assignments, reading files, videos lessons) as well as with collaborative tasks and discussions in forums and other communication channels (Cohen et al., 2022). LMSs capture the students’ activities, which were described by Norris (2011, p. 1) as "digital breadcrumbs". There are four types of information collected about learners: (a) personal characteristics, such as academic performance; (b) actions in the learning environment, such as accessing links and course materials; (c) learning and assessment measures, such as grades in courses; and (d) interactions with teachers and peers, such as activity in forums or social networks (Ifenthaler, 2015). The analysed data is available to the instructors, who can then intervene and provide feedback and recommendations to students to improve their learning. Studies have indicated that using LA through an LMS has assisted universities in helping students to improve their academic achievement and in reducing dropout rates (Campbell et al., 2007; Macfadyen & Dawson, 2010). For example, it was found that the frequency of access to the LMS, the monitoring of study materials, the identification of the pace of learning and assignment grades can predict the performance of students. Namely, this analysis allows students to receive feedback on their learning and encourages them to improve their academic achievements (Smith et al., 2012).

Despite the many advantages of using LA in higher education, there are important concerns regarding privacy and data protection (Falcao et al., 2019). Rubel and Jones (2016) found that there are four main issues that universities need to take into consideration when using sensitive data on students in order to protect them from inappropriate use: (a) monitor and control authorised staff that have access to the data; (b) provide a justification for collecting and storing the data; (c) explain how the data will benefit students and the academic institutions; and (d) be transparent in your activities so that students are aware of how their data is collected and used. Indeed, it is recommended to engage students in the process and allow them to have control over the collected data (Pardo & Siemens, 2014). Drachsler and Greller (2016) expanded these issues and added the following: ask for an informed consent letter from the students, anonymise the data as much as possible, implement technical procedures to ensure privacy and data protection and verify that external parties with access to the data are obliged to follow privacy regulations. Indeed, implementing data protection regulations in academic institutions should be considered as a service that will increase trust among students.

Students’ perceptions towards privacy and data protection

Students have the right to protect their privacy and know what data is being collected about them as part of their academic studies (Slade & Prinsloo, 2013). They are one of the main stakeholders in LA; thus, their voice in the decision process regarding the type of data collected and its purpose should be taken into consideration (Botnevik et al., 2020). Academic institutions are facing this delicate situation; they would like to improve learning by using LA while ensuring students’ privacy and data protection. Several studies have highlighted this issue and have explored students' privacy perceptions when using LA for academic needs (Lim et al., 2021; Pardo & Siemens, 2014). Such studies have found that most students are not aware of their privacy rights or have knowledge about their right to consent to data collection about them (Jones et al., 2020; Korir et al., 2022). They also are not aware of the process of data collection as well as the type of data collected in the LMS in their institution (Falcao et al., 2019). Furthermore, they express general fear of the use of their data (e.g., sharing personal photos, home address, personal phone number). However, when students are informed about the type and purpose of data collection, they react positively to the institutional use of their data to enhance learning (Korir et al., 2022) and express trust in their academic institution (Falcao et al., 2019; Korir et al., 2023). Indeed, research indicates that students expect transparency from their academic institutions and wish to be involved in the LA process. Nonetheless, these institutions do not always consider their students' opinions during the data collection process (Roberts et al., 2016; Tsai et al., 2020).

Privacy trade-off

The integration and use of ICT in higher education for learning purposes, alongside the challenges arising from the desire to protect user privacy, is at the core of the dilemma faced by organisations as well as individuals. What is the balance between using technology on the one hand and deriving benefits from it on the other hand, and the conditions under which users are willing to forfeit their privacy? This dilemma is known in the literature as the privacy calculus theory (Laufer & Wolfe, 1977). According to this theory, individuals disclose personal information based on a cost-benefit trade-off which considers the associations between the perception of privacy risks, the benefits of data use and the willingness to share personal information (Korir et al., 2022; Tang & Ning, 2023). The literature considers the privacy trade-off as a rational process of decision-making where users are carefully analysing the costs and benefits related to the information trade. The costs are typically viewed as a loss of privacy, whereas the benefits represent the added value or advantages individuals anticipate in return for sharing private information (Pentina et al., 2016).

The trade-off between privacy and the learning benefits in LA is significant. LA offers substantial benefits to students, particularly when personal data is utilised to tailor educational experiences. By providing personal data, students can receive personalised learning paths, targeted feedback and early interventions designed to meet their specific needs. For instance, detailed analysis of student interactions within digital environments can significantly enhance self-regulated learning strategies by providing real-time feedback and individualised support. Combining administrative data, such as demographics and test scores, with learning process data like keystrokes and response times, can offer profound insights into student behaviour and learning processes, allowing educators to address educational inequities more effectively (Osakwe et al., 2024; Slade et al., 2019). Ifenthaler and Schumacher (2016) found that students are willing to share their personal data and trade off privacy in exchange for receiving information that will improve their learning, specifically for personalised learning. Indeed, another recent study found that students positively reacted to personalised educational feedback enabled by LA (Lim et al., 2021). However, they are willing to share only data related to their studies and not data related to their behaviour, which traces their network activities.

Nonetheless, the use of personal data in LA raises privacy concerns. Students worry about surveillance, the purpose behind data collection and who has access to their information. Research indicates that students prefer to control their data and are particularly concerned about the privacy implications of detailed tracking. When personal data is not used, LA can still provide useful insights, but the level of personalisation and the ability to offer targeted interventions are significantly diminished. Aggregated and anonymised data can help identify broader trends and improve educational practices, yet interventions based on this generalised data may not be as effective as those tailored to individual needs. Thus, although non-personal data can contribute to overall improvements in educational strategies, the most significant benefits for students are realised when personal data is utilised responsibly and ethically (Regan & Jesse, 2019).

The privacy trade-off has been studied in various fields using ICT such as social network services, e-commerce and e-shopping and mobile applications. However, studies examining online learning in the field of higher education are still limited.

The research aims and questions

This study explored students' behaviour and perceptions towards privacy and data protection derived from using LA for pedagogical purposes. It investigated the privacy trade-off, in which students are willing to share their data for learning in return for pedagogical benefits. Therefore, the research questions (RQs) were:

- RQ1: What are the students' perceptions about their privacy and data protection when using LA at their academic institution?
- RQ2: To what extent are students willing to exchange their data for pedagogical needs?
- RQ3: What is the correlation between students' willingness to use their data in exchange for learning needs and their awareness, behaviour, perceptions and feelings towards privacy?
- RQ4: Which variables predict students' willingness to trade off their privacy for their pedagogical needs?

Methodology

Sample

The study sample consisted of 1,014 students (62.7% of whom were undergraduate students) from three higher education institutes in Israel. The student population was heterogeneous, coming from different disciplines: 37.3% are in science disciplines (engineering, exact and life sciences, and medicine), while 62.7% are in the social science and humanities faculties. The composition was 54% female, 45% male, and 1% other. The mean age was 29.56 years (*SD* = 10.56), including 66% aged between 20 and 30. An online questionnaire was distributed through social networks, in WhatsApp and Facebook students' groups, with an invitation to participate voluntarily and anonymously.

Procedure

The research was conducted quantitatively using an online questionnaire asking students about their privacy perceptions regarding the use of academic data through LA. The questionnaire was formulated based on the privacy calculus theory (Laufer & Wolfe, 1977), which is considered as one of most important and famous theoretical frameworks to be used. It focused on student awareness of privacy regulations, their privacy behaviour and the privacy trade-off for pedagogical needs. The questionnaire was voluntarily and anonymous. It was developed and validated during the study**.**

Notably, the development of the questionnaire items was conducted through a rigorous process that involved a literature review (e.g., Ahituv et al., 2014; Laufer & Wolfe, 1977; Schumacher & Ifenthaler, 2018), along with one-to-one in-depth interviews with seven independent experts in the fields of higher education, LA and privacy and data protection. Subsequently, consultation with the seven experts resulted in a list of potential items, which were then refined by the three project team members and experts to ascertain whether there was any pertinent content that may have been missed. Once the suggestions were incorporated, an online version of the questionnaire was tested for content validity using a pilot group of 31 heterogenous students from various degrees, disciplines, genders, ages and academic institutes. Based on the results, an updated version of the questionnaire was formulated and distributed through social media (Facebook and WhatsApp) during March 2020 to various students from different higher education institutions (*N* = 1,014). The questionnaire was accessible online for 1 month to students, who were invited to respond voluntarily. The Research Ethics Board of our university granted approval for this procedure.

The questionnaire

The questionnaire consisted of 85 items on a Likert scale (1 = *not at all* to 5 = *to a very large extent*) assessing students' perceptions and awareness of privacy protection as well as their willingness to trade off their privacy for pedagogical benefits. The questionnaire was composed of five parts: (a) demographic data; (b) technology usage (α = 0.824); (c) privacy awareness on the Internet (α = 0.713); (d) privacy perception (α = 0.666); (e) privacy trade-off for pedagogical needs (α = 0.940).

(1) The first part collected the demographic data, such as academic affiliation, learning discipline, age, and gender.

(2) The second part dealt with the main uses of ICT and consisted of 29 items in order to understand the students' behaviour. Most of the items (except for four) used Likert scales; participants were required to rate the degree of use of the technologies, over a sequence of five categories: 1 = *not at all*, 2 = *to a small extent*, 3 = *to a moderate extent*, 4 = *to a large extent* and 5 = *to a very large extent*. Additionally, students were asked about the use of technologies for general and academic needs, the length of time they spent on the Internet and the social networks they use.

(3) The third part of the questionnaire comprised 21 items focusing on students' feelings, experiences, perceptions and awareness regarding privacy. Students' feelings were examined through students' sense of concern working online and their need for protection and security using a 1–5 Likert scale (1 = *disagree*, 5 = *agree to a very large extent*) and yes/no questions for experiences of privacy abuse. Their online behaviour, including password sharing, use of protection software and personal data sharing on the Internet and academic platforms, were explored. Binary questions (yes/no) and a binary variable (1 = *no*, 2 = *yes*) were used for behaviours such as profile publication on social networks. The degree of privacy awareness was examined through the students' familiarity with privacy protection regulations (European Parliament and Council Regulation, 2016) and behaviours indicating awareness of the need to preserve their privacy, such as reading privacy policies. This familiarity and awareness were measured on a 1–5 Likert scale, where 1 = *not at all* and 5 = *to a very large extent*, particularly through two items that assessed the frequency of reading privacy policies of Internet sites they visited.

(4) The fourth part examined students' privacy perceptions through seven statements relating to student trust, the degree of security in the Internet space and academic online systems, the desire for transparency and their attitudes towards the protection and treatment of academic institutions in their systems. These items used 1–5 Likert scales where 1 = *not at all* and 5 = *to a very large extent*.

(5) The fifth part dealt with students' willingness to share personal information for addressing academic needs. It examined the degree of students' willingness to share information with academic stakeholders, the use of information for academic benefits and services and sharing information for receiving pedagogical information. This section consisted of 28 items on a 1–5 Likert scale that checked their readiness where 1 = *not at all* and 5 = *to a very large extent*.

Data analysis

The students' responses to the questionnaire were analysed based on the main dimensions of the privacy calculus theory (Laufer & Wolfe, 1977) using SPSS version 23. Additionally, exploratory factor analysis (using the principal component analysis method) with a varimax rotation and standardised values (*z* scores) was used to simplify the variables and form clusters with shared significance, thereby reducing the number of variables related to students' perceptions (about their privacy and willingness to trade-off their privacy for pedagogical benefits) into groups of factors (Table 1). Four new variables were created: feelings, behaviour patterns, awareness and attitudes towards privacy. To answer RQ1 and RQ2, descriptive statistics were performed regarding privacy perceptions, awareness and data protection, as well as correlation tests to find relationships between privacy awareness (familiarity with privacy regulations and behaviour) and their perceptions of privacy and data protection by their academic institution (transparency, data protection, trust and security). A Pearson test was conducted to explore the relationships between privacy perceptions and privacy trade-off variables to answer RQ3. Notably, the correlation analysis was used to identify basic relationships between variables, serving as a foundation for the subsequent, more comprehensive multiple regression analysis. For RQ4, a regression analysis was conducted to identify the variables that predict students' willingness to use their data for their academic needs (Figure 1).

Table 1
The variables included in the study from the factor analysis

Variable	Variable name	Description	Operalisation
Independent variables			
	Demographics	Age	Continuous number
		Gender	Male, female and other
		Education	Undergraduate, graduate, PhD and vocational diploma
		Discipline	All disciplines as reflected in nine faculties
	Privacy and data protection perceptions	Data protection	Binary – yes/no
	Anxiety	Concern from data misuse	Binary – yes/no
		Privacy abused	1–5 scale
		Sense of security on the Internet and the institution sites	1–5 scale
	Behaviour	Type of data shared	Select list from 14 types of data
		Sharing passwords	Binary – yes/no
		Use of protection software	Select list from 7 options + not use
		Publishing a personal profile on the Internet	1–5 scale
	Awareness	Familiarity with privacy laws and regulations (European Parliament and Council Regulation, 2016)	1–5 scale
		Reading of privacy policies	1–5 scale
	Feelings	Privacy violation by using the Internet	1–5 scale
		Transparency from the institution	1–5 scale
		Trust in the institution	1–5 scale
		Personal information management by the academic institution	1–5 scale
		Data monitoring	1–5 scale
Dependent variable	Students' privacy trade-off – willingness to share data with the institution in return for pedagogical benefits	The degree of willingness that the institution will use students' data	1–5 scale

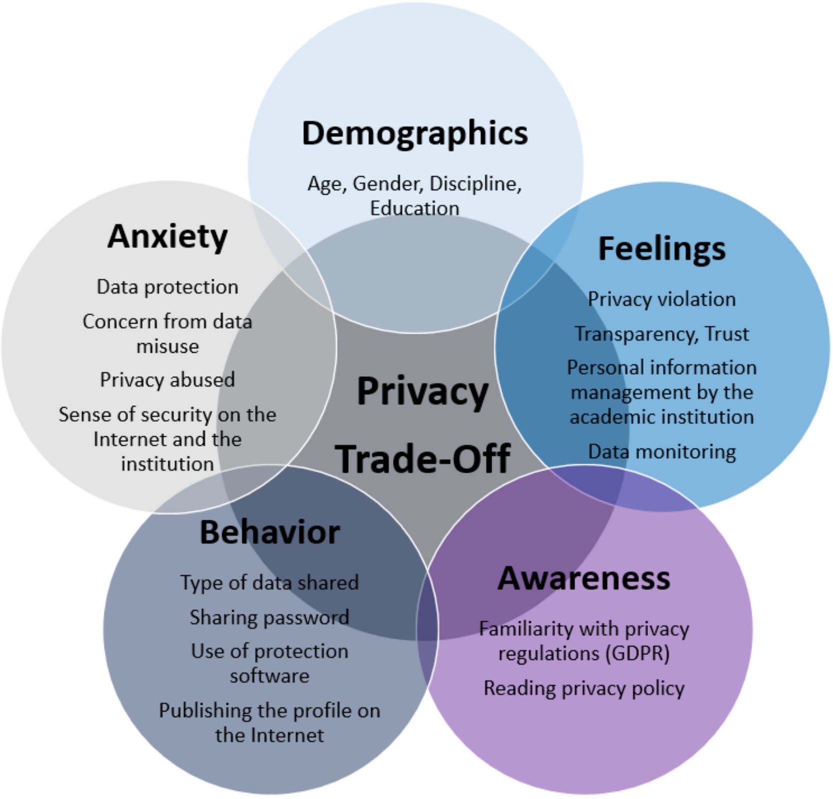
Demographics
Age, Gender, Discipline, Education
Anxiety
Data protection
Concern from data misuse
Privacy abused
Sense of security on the Internet and the institution
Feelings
Privacy violation
Transparency, Trust
Personal information management by the academic institution
Data monitoring
Privacy Trade-Off
Behavior
Type of data shared
Sharing password
Use of protection software
Publishing the profile on the Internet
Awareness
Familiarity with privacy regulations (GDPR)
Reading privacy policy

Figure 1. The research model showing the variables that predict students' privacy trade-off for pedagogical benefits

Results

Students' perceptions about privacy and data protection of LA at their academic institution (RQ1)

Four main themes were explored with regard to students’ perceptions towards privacy and data protection: (a) the degree of students’ privacy awareness, including familiarity with privacy regulations; (b) students’ privacy and data protection perceptions of their academic institution, including the level of transparency from their academic institution; (c) the degree of trust in the academic institution; and (d) the degree of security in data protection.

The results indicate that most of the participating students do not read and are unaware of the privacy regulations in general (69%) and the privacy consent of the academic institutions in particular (77%). Students’ awareness of privacy and data protection was examined through three main variables: the degree of the academic institution’s control over data transfer, the degree of willingness to provide the academic institution with access to personal information about the students; and the degree of willingness to collect and analyse this data. It was found that most students (73.9%) feel that their academic institution should control data transfer to increase security and data protection. Moreover, most students (62.5%) feel that their privacy will not be intruded upon due to data collection and analysis by their academic institution. Additionally, an analysis was conducted on the students' perceptions of allowing the academic institutions full access to their academic data. The results show dual perceptions, where 51.2% of the students do not think that the academic institutions should have full access to their data, while 44.5% of the students perceived that the academic institutions could have full access to their data.

Regarding the academic institutions, most students (64.4%) perceived the need for transparency as high and very high degree (4–5 on the Likert scale), about the data collected on them, including how it is used and for what purposes. Moreover, 42.3% of the students perceived that their data is protected by the academic institution to a very high degree (4–5 on the Likert scale). Additionally, 53.4% of the students trust that their academic institution will use their data in an appropriate manner (e.g., for pedagogical purposes). Notably, regarding the students' sense of security on the Internet, most of them (50.5%) indicated that they did not feel secure regarding their data protection. Figure 2 presents the averages and the standard deviation of the above perceptions.

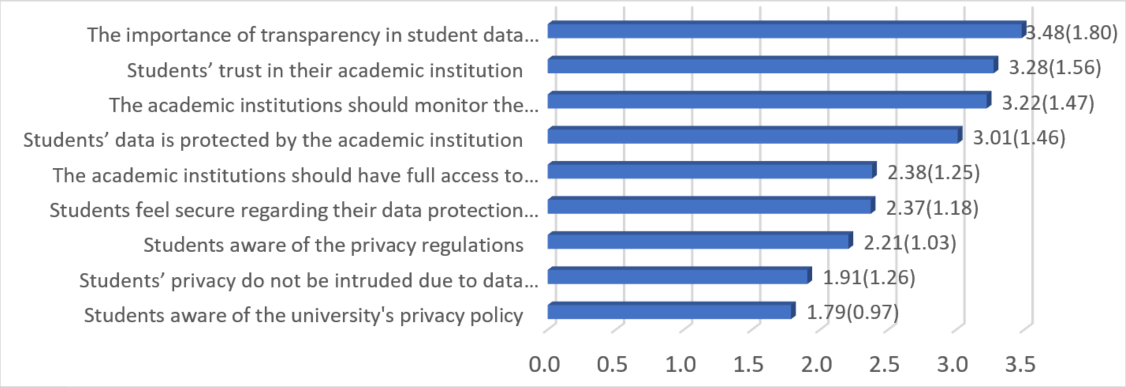

Figure 2. Student perceptions about privacy and data protection of LA at their academic institution (*N* = 952)

Interestingly, no significant correlations were found between privacy awareness (familiarity with privacy regulations and behaviour) and their privacy and data protection perceptions of their academic institution (transparency, data protection, trust and security).

Students' willingness to exchange their data for pedagogical needs (RQ2)

The results show (Figure 3) that most students (68.3%) are willing to share their data with their academic institutions for pedagogical purposes, including feedback on assignments (*M* = 3.68, *SD* = 1.25), recommendations for improving learning and passing the course, such as preferred content and topics (*M* = 3.46, *SD* = 1.32), ranks for the course content (*M* = 3.41, *SD* = 1.33) and for additional learning materials (*M* = 3.40, *SD* = 1.31). Notably, the students were willing to a very low degree to share their data, such as for suggestions of other students' names with whom to learn (*M* = 2.19, *SD* = 1.27).

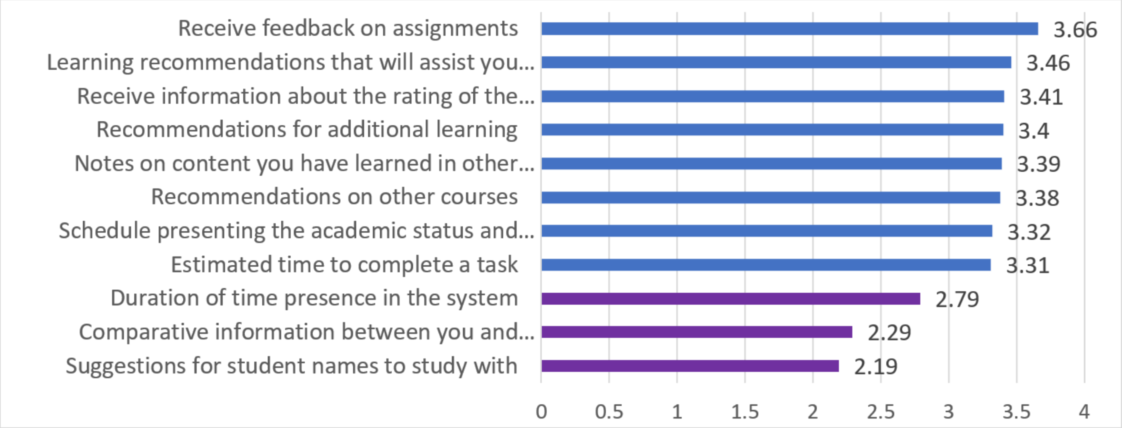

Figure 3. Students' degree of willingness to share their personal data in order to receive pedagogical information (*N* = 952)

When exploring the authorised stakeholders who could have access to the students' data, it was found that most of the students recognised to a low degree (1.82 < *M* < 2.87) the importance of sharing their data with various academic institution stakeholders. As presented in Figure 4, the highest scores were given to teaching instructors (*M* = 2.87, *SD* = 1.32) and teaching assistants (*M* = 2.72, *SD* = 1.39), as well as researchers (*M* = 2.52, *SD* = 1.29), although the lowest scores were given to administration stakeholders such as librarians (*M* = 1.82, *SD* = 1.09), the students' registration department (*M* = 2.12, *SD* = 1.21), university management (*M* = 2.13, *SD* = 1.2), and the academic secretary (*M* = 2.36, *SD* = 1.23).

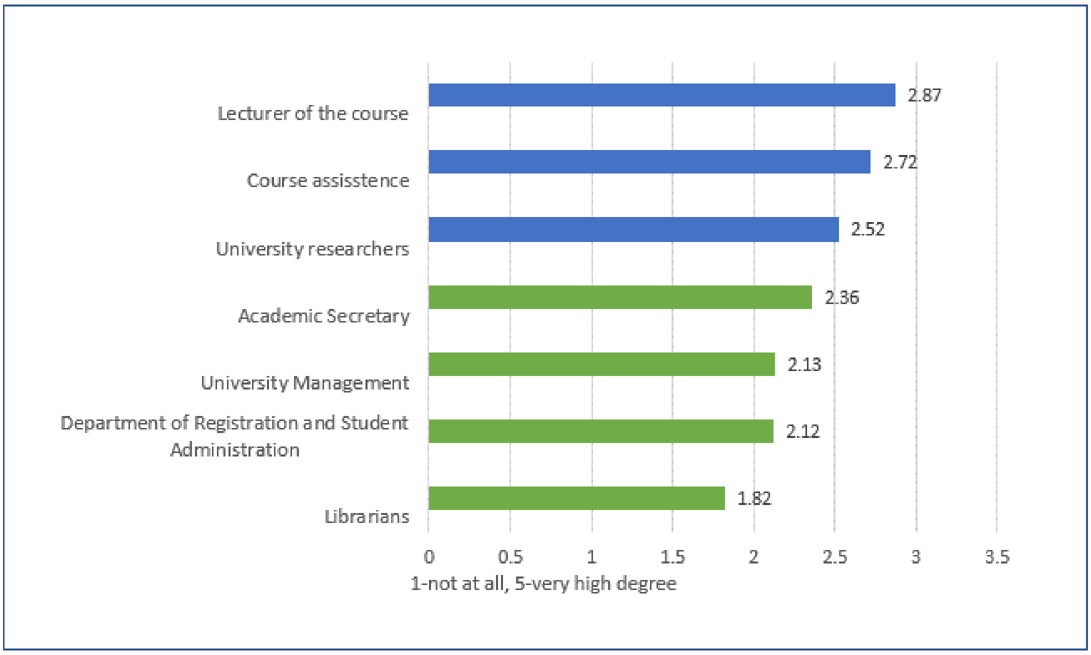

Figure 4. The degree of importance to which students think various stakeholders in the academic institution should have to access their data (*N* = 948)

The correlation between students' willingness to use their data in exchange for learning needs and their awareness, behaviour, perceptions and feelings towards privacy (RQ3)

Pearson tests (Table 2) reveal positive moderated significant correlations between students' willingness to share their data for pedagogical purposes and their sense of security (*r* = 0.33, *p* < 0.01) and their personal information management by the academic institution (*r* = 0.371, *p* < 0.01). Thus, the more students are confident about the protection of their information online and the role of the academic institution in supervising their data, the more they are likely to consent to its use. Interestingly, a negative weak significant correlation was found between age and student willingness to share data for pedagogical purposes (*r* = -0.168, *p* < 0.01*)*. Another negative weak significant correlation was found between students' behaviour to share their data on the Internet and their willingness to share data for pedagogical purposes (*r* = -0.121, *p* < 0.01).

Table 2
Pearson correlation between students' willingness to share data for pedagogical purposes and age, awareness, behaviour, perceptions and feelings towards privacy (N = 999)

Variable	Willingness to share data
Age	-.168**
Anxiety – Sense of security	.330**
Anxiety – Privacy abused	-0.041
Behaviour – Types of data shared	-.121**
Behaviour – Use of protection software	-0.042
Privacy awareness – Familiarity with privacy law and regulations (European Parliament and Council Regulation, 2016)	-0.027
Awareness – Reading privacy policy	-.088**
Anxiety – Concern from data misuse	.-102**
Feelings – Personal information management by the academic institution	.371**

**p* < 0.05. ***p* < 0.01.

The variables that predict students' willingness to trade-off their privacy for their pedagogical needs (RQ4)

A multiple regression was conducted in order to explore the variables which predict the students' willingness to trade off privacy for pedagogical needs. Five independent groups of variables were included in the regression: demographics, feelings, behaviour, awareness and perceptions towards privacy. As presented in Table 3, in the regression model, five significant variables were found: the students' age – from the demographic group (*B* = -0.19, *SE* = 0.004, *p*<0.01); sense of security – from the feeling group (*B* = 0.297, *SE* = 0.047, *p*<0.01); type of data shared – from the behaviour group (*B* = -0.200, *SE* = 0.044, *p*<0.01); privacy concerns from data misuse – from the perception group (*B* = 0.127, *SE* = 0.047, *p*<0.01) and personal information management by the academic institution – from the privacy perception group (*B* = 0.427, *SE* = 0.048, p<0.01). The regression model is significant and predicts the students' privacy trade-off, explaining 25% of the variance (adjusted R^2 = 0.254, *p*<0.01, *F*(9,712) = 29.93).

Table 3
Multiple regression for predicting students' willingness to trade off their privacy for their pedagogical needs (N = 721)

Variable	*B*	*SE B*	β
Age	-0.019	0.004	**-0.154****
Anxiety – Sense of security	0.297	0.047	**0.221****
Anxiety – Privacy abused	0.013	0.048	0.009
Behaviour – Type of data shared	-0.200	0.044	**-0.148****
Behaviour – Use of protection software	-0.067	0.044	-0.049
Privacy awareness – Familiarity with privacy law and regulations (European Parliament and Council Regulation, 2016)	-0.001	0.044	-0.001
Privacy awareness – Reading privacy policy	-0.067	0.045	-0.050
Anxiety – Concern from data misuse	0.127	0.047	**0.094****
Feelings – Personal information management by the academic institution	0.427	0.048	**0.313****

**p* < 0.05. ***p* < 0.01.

Discussion

The rapid adoption of LA in higher education (Korir et al., 2023), especially during the COVID-19 pandemic, has highlighted privacy and data protection concerns. Although LA enhances student learning, it can also compromise their privacy. Notably, LA can operate without revealing personal information, although this limits the data to broad group insights, useful only for refining teaching strategies and providing comparative performance overviews. Conversely, using identifiable details with LA allows for customised learning experiences, tailored guidance on content and adaptive learning styles, enhancing engagement and reducing dropout risks. This dilemma is central to the debate over the privacy trade-off. Therefore, this study explored students’ perceptions towards privacy and data protection (awareness, behaviour, feelings, anxiety), as well as their willingness to trade privacy for pedagogical benefits that can enhance their academic success.

Students' perceptions about privacy and data protection of LA

Studies have shown that most citizens are not aware of privacy and data protection regulations (Markovic et al., 2019; Presthus & Sørum, 2018; Reis et al., 2018). Our study, which focused on students in higher education, strengthens and elaborates on previous findings by showing that most students, like other citizens, are not aware of privacy and data protection regulations. Moreover, as was revealed from RQ1, students are less aware or do not read at all the privacy consent information of their academic institutions. Notably, understanding the level of students’ privacy awareness is significant due to the major impact it has on their privacy behaviour (Jones et al., 2020; Korir et al., 2023).

As reflected in RQ1, the students in this study perceive that their data is protected by their academic institutions but expressed their desire for data transparency in terms of collecting, analysing and using the data (0Korir et al., 2023; Slade et al., 2019; Sun et al., 2018). Additionally, it was found that students perceived a high sense of security regarding their privacy and data protection in their academic institution (Fisher et al., 2014). They also believe that their data is treated properly, specifically for pedagogical purposes (Vu et al., 2019). It should be noted that a high level of perceived transparency among students is important for building their trust in their academic institutions (Drachsler & Greller, 2016; Slade et al., 2019). Therefore, academic institutions should take these findings into account when developing and implementing privacy and data protection policies. For example, they should actively provide information to raise privacy awareness by incorporating targeted educational programs and workshops about privacy and data protection regulations, as well as engage students in the process of using LA to create a high degree of trust (e.g., clarifying the type of data that is collected, its purpose and how it is used). This approach will ensure that students are not only informed but also educated on how to safeguard their personal information, aligning with the critical gaps identified in our findings regarding students' lack of knowledge in this area.

Students’ willingness to exchange their data for pedagogical needs

The results of this study (RQ2) validate and support the claim that students are willing to share their data in exchange for pedagogical benefits (Ifenthaler & Schumacher, 2016; Slade et al., 2019), such as receiving online feedback, dedicated learning materials and personal support during their studies according to their needs. Specifically, this study reveals the variations in students’ perceptions regarding the specific stakeholders with whom they are willing to share their data for pedagogical needs. The results emphasise that students prefer to share their data with their instructors, teaching assistants and researchers (Jones et al., 2020) more than with management and administrative staff (e.g., academic secretary, registrations and librarians). In concordance, students are willing to share their pedagogical data (e.g., feedback on assignments, recommendations that assist them in passing courses) more than their personal data (e.g., duration of time spent in the online academic system, comparative information between them and their peers and names of other students with whom they are suited to study).

An interesting aspect of this research was the examination of the relationship between the role of academic institutions in privacy and data protection and student perceptions thereof. The findings for RQ3 indicate a positive correlation between students' confidence in the protection of their personal information and the supervisory role of the academic institution over their data, and their likelihood to consent to the use of such data. The rationale behind employing LA for pedagogical purposes is multifaceted, aiming to personalise learning experiences, optimise educational pathways and enhance academic outcomes through data-driven insights (Papadopoulos & Hossain, 2023). Consequently, it is imperative for higher education institutions to employ LA to enhance student learning experiences. This should be done with respect to students' willingness to share pedagogical data, while also promoting policies on LA that are specifically designed to foster educational purposes, thereby ensuring a balanced integration of technology with educational objectives.

Students' willingness to trade off their privacy for their pedagogical needs

Students expressed that their primary motivation for accepting the trade-off between privacy and educational benefits is their aspiration to achieve academic success (Ifenthaler & Schumacher, 2016). This stance is reinforced by the results of RQ4, which reveal that students are reluctant to share their data unless it directly contributes to their learning enhancement.

The study found five significant predictors for this trade-off: age – the younger the students are, the more they are willing to trade off privacy for pedagogical benefits; the type of data shared – students' willingness to trade off personal information decreases as the information becomes more personal (and less pedagogical); and students are more willing to trade off privacy for pedagogical benefits – if their sense of security in the academic institution is higher, they have a more positive perception of the way in which their data is managed by the academic institution and they have fewer privacy concerns about data misuse (Figure 5).

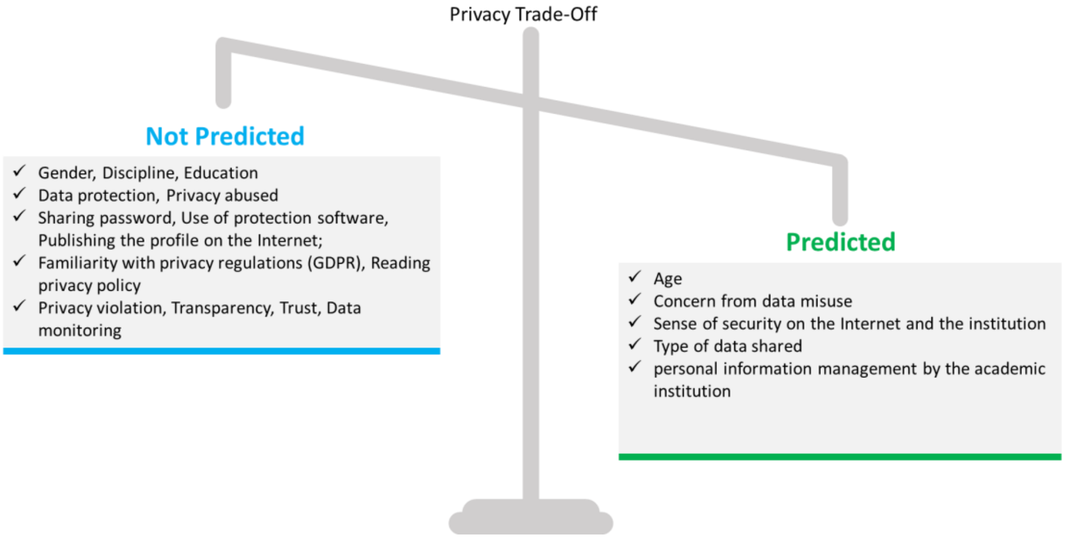
Privacy Trade-Off
Not Predicted
✓ Gender, Discipline, Education
✓ Data protection, Privacy abused
✓ Sharing password, Use of protection software, Publishing the profile on the Internet;
✓ Familiarity with privacy regulations (GDPR), Reading privacy policy
✓ Privacy violation, Transparency, Trust, Data monitoring
Predicted
✓ Age
✓ Concern from data misuse
✓ Sense of security on the Internet and the institution
✓ Type of data shared
✓ personal information management by the academic institution

Figure 5. Privacy trade-off predictors

The present study contributes both theoretically and practically to the understanding of the privacy calculus theory, initially introduced by Laufer and Wolfe (1977). This theory offers a comprehensive framework for understanding the complex decision-making process individuals engage in when evaluating the benefits and risks associated with disclosing personal information. Within the academic context, this theory illuminates the divergent expectations and concerns of key stakeholders, namely students, teachers and policymakers. Students are often found to balance their desire for a personalised and improved learning experience against apprehensions concerning the security and application of their personal data (Ifenthaler & Schumacher, 2016). They anticipate that institutions will safeguard their privacy while harnessing data to bolster academic achievement. In navigating the delicate balance between using student data for pedagogical improvement and maintaining student privacy, teachers seek access to relevant data that informs teaching methods without breaching ethical norms. Policymakers in academic settings face the challenge of developing policies that harmonise these interests, ensuring data is utilised ethically to advance educational objectives while instituting rigorous data protection measures (Jones et al., 2020). It should be noted that in scenarios without personal information, LA can aggregate data to overview a learner group, aiding instructors in refining teaching strategies and providing learners insights into their relative performance. On the other hand, incorporating identifiable details allows LA to tailor personalised learning experiences, offering precise guidance on content, learning styles and challenges to enhance engagement and reduce dropout risks. Thus, the application of the privacy calculus theory underscores the complex challenge of reconciling these diverse expectations, emphasising the importance of transparent communication and robust privacy measures to foster a trust-based educational ecosystem. This includes, for example, anonymising the data as much as possible, monitoring and controlling which authorised staff have access to the data and implementing technical procedures to ensure privacy and data protection.

This study was conducted based on a questionnaire and analysed quantitatively. Further research is needed to elaborate on the results using open-ended questions and qualitative methods. It was also conducted nationally; thus; it is not representative on an international level. Further international research will provide more cultural insights regarding students' perceptions towards privacy and data protection in light of the rapid penetration of emerging technologies in higher education. Moreover, it would be interesting to conduct a similar study to explore the perceptions of the teaching staff on these issues.

Understanding students' perceptions of their privacy protection is crucial as they are the main beneficiaries of the data produced by the LMS. Therefore, it is important to engage students in the process of implementing LA in higher education (Ochoa & Wise, 2021) and build trust between them and the institution regarding privacy and data protection (Slade et al., 2019). Looking to the future, students' attitudes towards data protection and privacy are among the critical factors that will shape the policies and practices governing the successful use of LA in higher education. Specifically, the rapid penetration of generative artificial intelligence into higher education and its effects on LA have raised significant concerns. Additionally, a follow-up study focusing on the teaching staff's perceptions of this issue, specifically, their feelings (e.g., perceived threats, challenges and incentives) regarding the quality of teaching with LA-based artificial intelligence, could offer a valuable complementary perspective that contributes to more holistic policy recommendations (Chan, 2023).

Author contributions

The authors contributed to the manuscript equally.

Acknowledgements

This research is part of a large study funded by the Blavatnik Interdisciplinary Cyber Research Center at Tel Aviv University.

References

Ahituv, N., Bach, N., Birnhack, M., Soffer, T., & Luoto, L. (2014). New challenges to privacy due to emerging technologies and different privacy perceptions of younger generations: The EU PRACTIS project. *Proceedings of Informing Science & IT Education Conference (InSITE), 14*, 1–23. https://doi.org/10.28945/1995

Alzahrani, A. S., Tsai, Y. S., Iqbal, S., Marcos, P. M. M., Scheffel, M., Drachsler, H., Kloos, C., Aljohani, N., & Gasevic, D. (2023). Untangling connections between challenges in the adoption of learning analytics in higher education. *Education and Information Technologies, 28*(4), 4563–4595. https://doi.org/10.1007/s10639-022-11323-x

Antón, A. I., Earp, J. B., & Young, J. D. (2010). How internet users' privacy concerns have evolved since 2002. *IEEE Security & Privacy*, *8*(1), 21–27. https://doi.org/10.1109/MSP.2010.38

Baek, C., & Doleck, T. (2023). Educational data mining versus learning analytics: A review of publications from 2015 to 2019. *Interactive Learning Environments*, *31*(6), 3828–3850. https://doi.org/10.1080/10494820.2021.1943689

Belanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–1041. https://doi.org/10.2307/41409971

Bharti, S. S., & Aryal, S. K. (2023). The right to privacy and an implication of the EU general data protection regulation (GDPR) in Europe: Challenges to the companies. *Journal of Contemporary European Studies, 31*(4), 1391–1402. https://doi.org/10.1080/14782804.2022.2130193

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S. C., Strycharz, J., Helberger, N., & De Vreese, C. H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication, 23*(6), 370–388. https://doi.org/10.1093/jcmc/zmy020

Botnevik, S., Khalil, M., & Wasson, B. (2020). Student awareness and privacy perception of learning analytics in higher education. In C. Alario-Hoyos, M. J. Rodríguez-Triana, M. Scheffel, I. Arnedillo-Sánchez, & S. M. Dennerlein (Eds.), *Lecture notes in computer science: Vol. 12315. Addressing global challenges and quality education* (pp. 374–379). Springer. https://doi.org/10.1007/978-3-030-57717-9_30

Campbell, J. P., DeBlois, P. B., & Oblinger, D. G. (2007). Academic analytics: A new tool for a new era. *EDUCAUSE Review*, *42*(4), 40–57. https://er.educause.edu/articles/2007/7/academic-analytics-a-new-tool-for-a-new-era

Caspari-Sadeghi, S. (2023). Learning assessment in the age of big data: Learning analytics in higher education. *Cogent Education, 10*(1)*,* 1–11. https://doi.org/10.1080/2331186X.2022.2162697

Chan, C. K. Y. (2023). A comprehensive AI policy education framework for university teaching and learning. *International Journal of Educational Technology in Higher Education, 20*, Article 38. https://doi.org/10.1186/s41239-023-00408-3

Cohen, A., Soffer, T., Henderson, M. (2022). Students' use of technology and their perceptions of its usefulness in higher education: International comparison. *Journal of Computer Assisted Learning 38*(5), 1321–1331. https://doi.org/10.1111/jcal.12678

Crutzen, R., Peters, G. J.Y. & Mondschein, C. (2019). Why and how we should care about the general data protection regulation. *Psychology & Health*, *34*(11), 1347–1357. https://doi.org/10.1080/08870446.2019.1606222

Drachsler, H., & Greller, W. (2016). Privacy and analytics: It's a DELICATE issue a checklist for trusted learning analytics. In D. Gaševi, & G. Lynch (Chairs), *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge* (pp. 89–98). Association for Computing Machinery. https://doi.org/10.1145/2883851. 2883893

European Parliament and Council Regulation. (2016). *General Data Protection Regulation (*2016/679). https://gdprinfo.eu/

Falcao, T. P., Ferreira, R., Rodrigues, R. L., Diniz, J., & Gasevic, D. (2019). Students' perceptions about learning analytics in a brazilian higher education institution. In Kinshuk, N. S.Chen & I. Bittencourt (Chairs), *Proceedings of the 19th International Conference on Advanced Learning Technologies* (pp. 204-206). IEEE. https://doi.org/10.1109/ICALT.2019.00049

Fisher, J. A., Valenzuela, F., & Whale, S. (2014). *Learning analytics: A bottom-up approach to enhancing and evaluating students' online learning*. Australian Government Office for Learning and Teaching. https://ltr.edu.au/resources/SD12_2567_Fisher_Report_2014.pdf

Gursoy, M. E., Inan, A., Nergiz, M. E., & Saygin, Y. (2017). Privacy-preserving learning analytics: Challenges and techniques. *IEEE Transactions on Learning Technologies*, *10*(1), 68–81. https:doi.org/10.1109/TLT.2016.2607747

Ifenthaler, D. (2015). Model-based approaches. In J. M. Spector (Ed.), *The SAGE Encyclopedia of educational technology* (Vol. 2, pp. 512–525). Sage. https://doi.org/10.4135/9781483346397

Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development, 64*(5), 923–938. https://doi.org/10.1007/s11423-016-9477-y

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*(9), 1044–1059*.* https://doi.org/10.1002/asi.24358

Khalil, M., Slade, S., & Prinsloo, P. (2024). Learning analytics in support of inclusiveness and disabled students: A systematic review. *Journal of Computing in Higher Education, 36*(24), 202–219*.* https://doi.org/10.1007/s12528-023-09363-4

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Korir, M., Slade, S., Holmes, W., & Rienties, B. (2022). Eliciting students' preferences for the use of their data for learning analytics: A crowdsourcing approach. In B. Rienties, R. Hampel, E. Scanlon, & D. Whitelock (Eds.), *Open world learning: Research, innovation and the challenges of high-quality education* (pp. 144–156). Routledge. https://doi.org/10.4324/9781003177098

Korir, M., Slade, S., Holmes, W., Héliot, Y., & Rienties, B. (2023). Investigating the dimensions of students' privacy concern in the collection, use and sharing of data for learning analytics. *Computers in Human Behavior Reports, 9,* Article 100262. https://doi.org/10.1016/j.chbr.2022.100262

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42.

Lim, L. A., Dawson, S., Gašević, D., Joksimović, S., Pardo, A., Fudge, A., & Gentili, S. (2021). Students' perceptions of, and emotional responses to, personalised learning analytics-based feedback: An exploratory study of four courses. *Assessment and Evaluation in Higher Education, 46*(3), 339–359. https://doi.org/10.1080/02602938.2020.1782831

Macfadyen, L. P., & Dawson, S. (2010). Mining LMS data to develop an "early warning system" for educators: A proof of concept. *Computers & Education*, *54*(2), 588–599. https://doi.org/10.1016/j.compedu.2009.09.008

Marković, M. G., Debeljak, S., & Kadoić, N. (2019). Preparing students for the era of the general data protection regulation (GDPR). *TEM Journal, 8*(1), 150–156. https://doi.org/10.18421/TEM81-21

Norris, D. M. (2011). 7 things you should know about first-generation learning analytics. *EDUCAUSE Learning Initiative*. https://library.educause.edu/resources/2011/12/7-things-you-should-know-about-firstgeneration-learning-analytics

Ochoa, X., & Wise, A. F. (2021). Supporting the shift to digital with student-centered learning analytics. *Educational Technology Research and Development*, *69*(1), 357–361. https://doi.org/10.1007/s11423-020-09882-2

Osakwe, I., Chen, G., Fan, Y., Rakovic, M., Singh, S., Molenaar, I., & Gašević, D. (2024). Measurement of self-regulated learning: Strategies for mapping trace data to learning processes and downstream analysis implications. In B. Flanagan, B., Wasson, & D. Gašević (Chairs), *Learning analytics in the age of artificial intelligence—Proceedings of the 14th International Conference on Learning Analytics and Knowledge* (pp. 563–575). Association for Computing Machinery. https://doi.org/10.1145/3636555.3636915

Papadopoulos, D., & Hossain, M. M. (2023). Education in the age of analytics: Maximizing student success through big data-driven personalized learning. *Emerging Trends in Machine Intelligence and Big Data, 15*(9), 20-36. https://orientreview.com/index.php/etmibd-journal/article/view/19

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, *45*(3), 438–450. https://doi.org/10.1111/bjet.12152

Pentina, I., Zhang, L., Bata, H., & Chen, Y. (2016). Exploring privacy paradox in information-sensitive mobile app adoption: A cross-cultural comparison. *Computers in Human Behavior*, *65*, 409–419. https://doi.org/10.1016/j.chb.2016.09.005

Presthus, W., & Sørum, H. (2018). Are consumers concerned about privacy? An online survey emphasizing the general data protection regulation. *Procedia Computer Science, 138*, 603–611. https://doi.org/10.1016/j.procs.2018.10.081

Reis, S., Ferreira, A., Vieira-Marques, P., Santos-Pereira, C., & Cruz-Correia, R. (2018). Do patients want to know who accesses their personal health information? A questionnaire to university students. In *Proceedings of the 13th Iberian Conference on Information Systems and Technologies* (pp. 1–6). IEEE. https://doi.org/10.23919/CISTI.2018.8399207

Regan, P. M., & Jesse, J. (2019). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology*, *21*, 167–179. https://doi.org/10.1007/s10676-018-9492-2

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*. https://doi.org/10.3389/fpsyg.2016.01959

Romero, C., & Ventura, S. (2020). Educational data mining and learning analytics: An updated survey. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *10*(3), Article e1355. https://doi.org/10.1002/widm.1355

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

Schumacher, C., & Ifenthaler, D. (2018). Features students really expect from learning analytics. *Computers in Human Behavior, 78*, 397–407. https://doi.org/10.1016/j.chb.2017.06.030

Shukla, S., George, J. P., Tiwari, K., & Kureethara, J. V. (2022). *Data ethics and challenges*. Springer. https://doi.org/10.1007/978-981-19-0752-4

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

Slade, S., Prinsloo, P., & Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. In S. Hsiao, J. Cunningham, K. McCarthy, & G. Lynch (Chairs), *Proceedings of the 9th International Conference on Learning Analytics & Knowledge* (pp. 235–244). Association for Computing Machinery. https://doi.org/10.1145/3303772.3303796

Smith, V. C., Lange, A., & Huston, D. R. (2012). Predictive modeling to forecast student outcomes and drive effective interventions in online community college courses. *Journal of Asynchronous Learning Networks*, *16*(3), 51–61. https://doi.org/10.24059/olj.v16i3.275

Soffer, T., & Cohen, A. (2019). Students' engagement characteristics predict success and completion of online courses. *Journal of Computer Assisted Learning*, *35*(3), 378–389. https://doi.org/10.1111/jcal.12340

Sun, K., Brooks, C., Mhaidli, A. H., Schaub, F., & Watel, S. (2018). Taking student data for granted? A multi-stakeholder privacy analysis of a learning analytics system. In M. E. Zurko, H. Richter Lipford, S. Chiasson, & R. Reeder (Eds.), *Proceedings of the 14th Symposium on Usable Privacy and Security* (pp. 1–5). Association for Computing Machinery. https://dl.acm.org/doi/proceedings/10.5555/3291228

Tang, Y., & Ning, X. (2023). Understanding user misrepresentation behavior on social apps: The perspective of privacy calculus theory. *Decision Support Systems, 165,* Article 113881. https://doi.org/10.1016/j.dss.2022.113881

Tsai, Y. S., Whitelock-Wainwright, A., & Gašević, D. (2020). The privacy paradox and its implications for learning analytics. In C. Rensing & H. Drachsler (Chairs), *Proceedings of the Tenth International Conference on Learning Analytics & Knowledge* (pp. 230–239). Association for Computing Machinery.. 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*(2), 42–51. https://jofdl.nz/index.php/JOFDL/article/view/350/249

Warren, S. D., & Brandeis, L. D. (1890). Right to privacy. *Harvard Law Review*, *4*(5), 193–220. https://doi.org/10.2307/1321160

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Corresponding author: Anat Cohen, anatco@tauex.tau.ac.il

Please cite as: Soffer, T., & Cohen, A. (2024). Privacy versus pedagogy – students' perceptions of using learning analytics in higher education. *Australasian Journal of Educational Technology*, *40*(5), 14–30. https://doi.org/10.14742/ajet.9130