JOURNAL OF LEARNING ANALYTICS

SOLAR SOCIETY for LEARNING ANALYTICS RESEARCH

Volume 10(3), 102–114. https://doi.org/10.18608/jla.2023.7975

Student Privacy and Learning Analytics: Investigating the Application of Privacy Within a Student Success Information System in Higher Education

Mary Francis[1], Mejai Bola Mike Avoseh[2], Karen Card[3], Lisa Newland[4] and Kevin Streff[5]

Abstract

This single-site case study will seek to answer the following question: how is the concept of privacy addressed in relation to a student success information system within a small, public institution of higher education? Three themes were found within the inductive coding process, which used interviews, documentation, and videos as data resources. Overall, the case study shows an institution in the early stages of implementing a commercial learning analytics system and provides suggestions for how it can be more proactive in implementing privacy considerations in developing policies and procedures.

Notes for Practice

- Learning analytics continues to increase in use. While many articles consider the preception of ethical considerations, including privacy within these systems, little research considers what is done in practice. This article provides a case study of how an institution addresses privacy.
- Overall, users of student success information systems have only a surface-level understanding of privacy. Due to this, more in-depth training and discussion of student privacy is essential when implementing learning analytics.
- When implementing learning analytics, transparency in process and procedure leads to trust from students and users of the system.

Keywords: Learning analytics, privacy, case study, student success information system

Submitted: 16/02/2023 — **Accepted:** 17/07/2023 — **Published:** 12/12/2023

Corresponding author [1]Email: mary.francis@dsu.edu Address: Dakota State University, 820 N Washington Avenue, Madison, SD, 57042.
[2]Email: mejai.avoseh@uds.edu Address: University of South Dakota, 414 E Clark St., Vermillion, SD, 57069. ORCID iD: https://orcid.org/0000-0003-1463-9297
[3]Email: karen.card@usd.edu Address: University of South Dakota, 414 E Clark St., Vermillion, SD, 57069.
[4]Email: lisa.newland@usd.edu Address: University of South Dakota, 414 E Clark St., Vermillion, SD, 57069.
[5]Email: kevin.streff@dsu.edu Address: Dakota State University, 820 N Washington Avenue, Madison, SD, 57042.

1. Introduction

Higher education institutions are being called to demonstrate their effectiveness amid the additional requirements of efficiency and maintaining costs. Meanwhile, technological advances have allowed for the gathering and analysis of data to aid decision-making. The conjuncture of these two circumstances has made learning analytics a critical component for many institutions. Learning analytics involves using the big data techniques utilized in the business sector to improve educational experiences.

While the techniques are similar, there is an essential difference between commercial big data analysis and learning analytics. Rubel and Jones (2016) noted that for learning analytics to have the most significant impact, student data must be connected to the individual. In big data analytics, the information can be used in the aggregate. This differentiation makes learning analytics a more personalized process, which raises additional concerns related to the ethical use of such data.

Proponents of learning analytics highlight the ability to use data to increase students' learning experience, resulting in enhanced education. Yet, concerns remain regarding how these processes may provoke unintended consequences. While there are varied ethical considerations in collecting, analyzing, and using data, one of the most pressing concerns is student privacy. Hoel and Chen (2016) provide the logic for the importance of studying how privacy is addressed in learning analytics. They

note that while institutions have long analyzed behaviour and performance to make changes, learning analytics has changed how that process is done and the impact it can have on individuals. This process necessitates a new agreement between the student and the institution regarding its practice and how goals are met.

Institutions do recognize that privacy is a concern. The *EDUCAUSE 2020 top 10 IT issues* report placed privacy second on the list after security (Grajek, 2020). Burns (2020) notes that while institutions recognize the importance of privacy, they must work to develop and improve policies and procedures dealing with student information. With no dedicated federal law or guidance on addressing privacy concerns within learning analytics, it has been left to each institution to develop its own approach. This study uses a case study to see how a small public institution of higher education in the Midwest addresses students' privacy within a student success information system. As a developing field of study, learning analytics research will mature only through studies looking at all aspects of the field. This case study will provide an in-depth analysis of one institution that has implemented a specific system.

The following research question will guide this study:

- How is the concept of privacy addressed in relation to a student success information system within an institution of public higher education?

1.1. Significance of the Study

Within their systematic review of articles looking at the ethical concerns related to learning analytics, Cerratto Pargman and McGrath (2021) note that most of the research focused on respondents' perceptions and attitudes related to learning analytics rather than the actual use of the systems. They recommended that research looking at "how ethical principles, guidelines, or codes of practices in LA [learning analytics] are put into practice will help us gain a more grounded understanding of how these instruments work in everyday higher education" (p. 13). Kitto and Knight (2019) also stress the need for specific case studies on ethics and learning analytics. This work will help address that need by providing a case study on how privacy is addressed with the student success information system.

1.2. Learning Analytics

1.2.1. Overview

Student data has long been used to make decisions both on the micro level in specific classrooms and at the macro level in how the institution operates. In the past, this data came from faculty use of student grades and in-room discussions while institutions looked at yearly retention and graduation rates. While the use of data is not new, the current interest in learning analytics is due to the conjuncture of several trends: the volume of data collected, the ability to store that data, the computational capacity now available to institutions, the increase in visualization tools, and the increased demand to analyze and use big data (Slade and Prinsloo, 2013; Siemens, 2013). One of the most frequently used definitions of learning analytics comes from Siemens (2013), "Learning analytics is the measurement, collection, analysis, and reporting of data about learners and their contexts, for the purposes of understanding and optimizing learning and the environment in which it occurs" (p. 1382).

With the increased push to utilize learning analytics, institutions must implement structured plans to ensure successful programs. The Data Quality Campaign (2019) provides four policy priorities they recommend institutions consider as they implement learning analytics: measure what matters, be transparent and earn trust, make data use possible, and guarantee access and protect privacy.

1.2.2. Benefits

There have been a range of claims related to how the learning analytics available through student information systems, student success information systems, learning management systems, and other systems will improve education. These include enhanced learning experiences (Long and Siemens, 2011), supported self-regulated learning (Kim et al., 2018), improvement of student learning services (Knight et al., 2014), development of prediction analytics for at-risk students (Saqr et al., 2017), and help for at-risk students (Pardo & Siemens, 2014). Long and Siemens (2011) also discuss the benefits of improved institutional decision-making, advancements in learning outcomes for at-risk students, greater trust in institutions due to the disclosure of data, significant evolutions in pedagogy, sense-making of complex topics, increased organizational productivity, and providing learners with insights into their learning. Foster and Francis (2020) conducted a systematic literature review of 34 learning analytics studies focused on retention goals, academic performance, and engagement. They found that most studies reported increased student outcomes related to those goals.

1.2.3. Challenges/Concerns

While learning analytics aim to improve student learning experiences, this does not negate the fact that gathering data on students poses risks and challenges. Selwyn (2019) poses several possible consequences related to learning analytics, including a reduced understanding of education, ignoring the broader social contexts of education, reducing students' and teachers'

ISSN 1929-7750 (online).

capacity for informed decision-making, a means of surveillance rather than support, a source of performativity, disadvantaging large numbers of people, and serving institutional rather than individual interests. Privacy concerns related to data analytics occur throughout the data lifecycle.

One of the major concerns related to learning analytics is ethical considerations that arise when collecting, using, and storing student data. Some authors have looked specifically at privacy concerns regarding ethics. Slade and Prinsloo (2013) note how the ethical considerations stemming from the increased use of learning analytics come from issues related to privacy and determining who owns the collected data. Gasevic et al. (2016) note that while privacy and ethics have been a concern related to learning analytics since their development, they have not been fully explored in the literature.

Cerratto Pargman and McGrath (2021) conducted a systematic literature review on which ethical topics have been addressed in studies that examine the ethics of learning analytics. The ethical topics addressed include transparency, privacy, informed consent, responsibility, minimizing adverse impacts, validity, and enabling interventions. Some authors have looked at general ethical concerns related to learning analytics, which either mention privacy as a broad category or refer to aspects related to privacy. The following table provides a comparison of those studies. Direct mentions of privacy are bolded, while topics related to privacy are in italics.

Table 1. Comparison of Ethical Concerns

Ferguson et al. (2016)	Slade and Prinsloo (2013)	Khalil and Ebner (2016)	Steiner et al. (2016)	Slade and Tait (2019)	SoLAR (2021)
• student success • trustworthy educational institutions • *respect for private and group assets* • respect for property rights • educators and educational institutions that safeguard those in their care • equal access to education • laws that are fair, equally applied, and observed • freedom from threat • *integrity of self*	• the location and interpretation of data • *informed consent* • **privacy and the de-identification of data** • the management, classification, and storage of data.	• *transparency of data collection, usage, and involvement of third parties* • *anonymization and de-identification of individuals* • *ownership of data* • data accessibility and accuracy of the analyzed results • security of the examined datasets and student records from any threat	• **privacy** • *informed consent, transparency, and de-identification of data* • location and interpretation of data • management, classification, and storage of data • *data ownership* • possibility of error • role of knowing and the obligation to act	• *data ownership and control* • transparency • accessibility of data • validity and reliability of data • institutional responsibility and obligation to act • communications • cultural values • inclusion • *consent* • *student agency and responsibility*	• **privacy** • opaque black box algorithms • basing classifications on biased datasets • incorrectly predicting someone's behaviour

1.3. Defining Data Privacy

Privacy is a concept that is generally understood yet cannot be completely comprehended as each individual within a range of contexts approaches it differently. The most frequently agreed-upon definition of privacy is that there is no universal definition (Allen, 1988; Castelli, 2014; Margulis, 2011; Weimann & Nagel, 2012). Pavlou (2011) states that this ambiguity comes from the fact that privacy is a complex concept that can be addressed from various disciplines and perspectives. Within their review of research on information privacy, Smith et al. (2011) conclude that no definition of privacy crosses all disciplines. Solove (2008) notes that "privacy is not reducible to a singular essence; it is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other" (p. 756).

Instead, definitions of privacy vary depending on context, such as time period, cultural norms, physical location, and field of study. In considering this trait of privacy, Solove looks to "conceptualize privacy from the bottom up rather than the top down, from particular contexts rather than the abstract" (Solove, 2002, p. 1092). Nissenbaum (2011) holds that privacy should be put into larger social contexts. While it is acknowledged that privacy does not have a universal definition, for this study, the operational definition of privacy is the *restriction of access to an individual's personal information.*

1.4. Current Models to Integrate Privacy Into Learning Analytics

There have been various guidelines and structures proposed to guide the design of student information systems and student success information systems to account for privacy needs (Bellotti, 1997; Hoel & Chen, 2016; Horvitz, 1999; Jensen et al.,

2005; Kitto et al., 2015; Langheinrich, 2001; Steiner et al., 2016). Many of these new processes try to operate under a privacy-by-design framework, as put forth by Cavoukian (2012). However, in designing systems, privacy is often simply one component and not a critical one. These proposals focus more on minimizing privacy violations than proactively protecting individual privacy.

Institutions must establish policies and practices beyond the technical integration of privacy into learning analytic systems. Prinsloo and Slade (2013) reviewed the policies of two institutions regarding ethical concerns and learning analytics. They found that institutions were not keeping up with the new abilities of learning analytics. Several guides have been developed to assist institutions in developing learning analytics programs (Cormack, 2016; Drachsler & Greller, 2016; Privacy Technical Assistance Center, 2016; Sclater & Bailey, 2018).

Institutions can also develop and adopt codes of practice to guide the implementation of learning analytics on their campuses. Welsh and McKinney (2015) discuss the need for codes of practice, noting that their development maximizes effectiveness, minimizes risk, and builds trust between the institution and its constituents through transparency. Sclater (2016) provides an in-depth discussion and guide for institutions looking to establish a code of practice related to their learning analytics system. His article discusses the process used by Jisc to develop their code of practice and then details what should be considered by other institutions.

2. Methods

This study was a single-case, descriptive case study. Yin (2009) offers three situations in which a case study is the preferred research method. These include asking *how* or *why* questions, the researcher cannot control events, and the topic deals with a contemporary phenomenon in specific contexts. All three of these situations were present in the current study. The rationale for deciding to perform a single case study focused on the idea that the institution selected would be a representative case. The institution chosen is a typical situation, and as Yin (2009) noted, such cases can be informative about the experiences of an average institution. This case best represents small to mid-sized institutions that have recently implemented student success information systems. This stems from the number of individuals involved in the implementation and use of the system and their experience with such systems.

2.1. Site Selection

The institution of higher education (IHE) chosen was used to represent the abstraction of student privacy within a student success information system. The IHE is a public university within a statewide system in the Midwest. The IHE has an FTE enrollment of ~2,000 students. It is a residential campus with a robust online course offering. Over half of the students come from within the state, and 76% of students receive financial aid. It offers associate through doctoral degrees with a particular focus on technology. The unit of analysis for the study was the institution's student success information system.

The IHE has been working with the company since 2018, with the system's official launch in March 2020. The system provides a systematic method to collect student data and serves as a means of communication between students, faculty, and other departments on campus. The company has over 500 educational institutions using the system, highlighting how this study may apply to other institutions and situations.

2.2. Data Collection

As a case study, data was gathered from multiple sources to allow for triangulation of results. Yin (2009) discusses how triangulation of data occurs when the facts of a case study are supported by more than one piece of evidence. This is one of the strengths of case studies, as they allow for internal confirmation of the research findings. This triangulation helps with the research validity and credibility of the study. Confirming findings from different sources also provides confirmability (Shenton, 2004).

2.2.1. Interview Data Collection

Semi-structured interviews were conducted with the system director at the IHE. Two interviews were held with this individual, with coding occurring after each interview to ensure a comprehensive understanding of the system was developed. From the system director, snowball sampling was employed to get the contact information of faculty members and administrators who were users of the system. A semi-structured interview was also conducted with a representative from the company. After the interviews, the transcripts were shared with the participants to allow for member checking, which impacts validity and credibility. Overall, nine total interviews were held with eight individuals. Details on the interviewees, including pseudonyms, are included in the following table.

Table 2. Interviews Conducted

Interviewee	Connection with system	Times interviewed	Pseudonym
System Director	Oversaw the implementation of the system and manages the daily operations necessary for the continued use of the system. Provides training.	2	Judy
Administrator #1	Part of the team that implemented the system.	1	Paul
Administrator #2	Utilizes the system as an administrator, looking for trends and data to reach decisions.	1	John
Administrator #3	Part of the team that implemented the system. Utilizes the system as an administrator and as a faculty member.	1	Jim
Faculty #1	Utilizes the system within their roles as a faculty member teaching courses and as a student advisor.	1	Bob
Faculty #2	Utilizes the system within their roles as a faculty member teaching courses and as a student advisor.	1	Bill
Faculty #3	Utilizes the system within their roles as a faculty member teaching courses and as a student advisor.	1	Rose
System Representative	Employee of the system's company. Aids institutions utilizing the system.	1	Chris

2.2.2. Resource Data Collection

In addition to an interview with a representative from the company, data was also gathered through the analysis of company-supplied material. This included training materials and their online help centre. Institutional documents were also analyzed. These included any written reports and updates on the system, emails sent about the system, policies and procedures related to the system, documentation created by the institution, and training sessions offered for the faculty and staff members who utilize the system. Overall, 53 additional data resources were analyzed.

2.2.3. Ethical Considerations

This case study was approved by the University of South Dakota's IRB panel. Confidentiality of the interviewees was maintained. Participants gave consent to have the audio of the interviews recorded. Transcripts were first generated automatically using the Zoom captioning capabilities. These transcripts were then reviewed and confirmed with identifying names removed and the inclusion of pseudonyms. The recordings were deleted, and the transcripts will be kept for three years on a protected computer in compliance with the IRB requirements.

2.3. Data Analysis

The data was analyzed using open coding within an inductive approach. In this process, themes were developed through an open reading of the sources. The data was reviewed several times to allow for refinement of the final themes shared in the reporting of results. The themes developed by the open coding were analyzed by considering how they relate to the research questions noted earlier. The inductive coding utilized a categorical aggregation approach where a collection of instances was analyzed from the data in order to develop issue-relevant meanings. This approach worked well as the interviews each provided a unique instance of working with the system, and through this analysis, similar themes were uncovered. These themes were then confirmed through analysis of the data resources.

2.4. Researcher Background

Within qualitative research, the researcher participates actively in the study. This study was conducted as part of a doctoral dissertation, which meant the first author engaged most deeply with the research process, and the other authors provided support as the dissertation chair and committee. Because my engagement with the participants and resources directly impacted the results, I must clarify my background and relationship with the topic. I selected this topic due to my interest and past research on privacy. Since January 2019, I have been a part of a privacy research lab on my campus. This work has reaffirmed my belief in the importance of protecting and maintaining individual privacy. Recognizing my belief in the importance of privacy, I was conscientious to remain impartial in my interactions with the interviewees within the study.

2.5. Verification of Study

Tracy (2010) provides eight criteria that can be considered when looking at the quality of qualitative research. The need for articles addresses specific instances of learning analytics rather than just perceptions, highlighting the criteria of a worthy topic and significant contribution, as Tracy (2010) noted. The triangulation of in-depth data addresses the criteria of rich rigour and

credibility. The criteria of ethical and sincerity are addressed in the prior sections on ethical considerations and researcher background. Meaningful coherence will be found as each of the themes found in the data analysis is then connected to prior literature on the topic.

3. Results and Discussion

3.1. Background of Student Success Information System

The IHE contracted with the company to implement the student success information system. In one of their early training videos, the IHE provided an overview of the system to faculty, noting the following:

> [It] helps advisors and support teams quickly and easily reach out to students in need of extra guidance, connects everyone on campus, from deans and faculty to financial aid, tutoring, and residential life in a collaborative network to support students. Empowers students with the tools they need to stay on track and plan their college journey. And gives leadership the insights they need to make informed, strategic decisions and build a culture of student success. (Artifact 15)

The system was able to meet these claims due to the use of student data. In a guide on using student data, the IHE highlighted that "student data is one of the most important tools we have to foster student success" (Artifact 55).

With the purpose of the system in mind, the IHE contracted with the company and set up the behind-the-scenes structure of the system. The system was ready to be rolled out to the campus in Spring 2020. This was when the IHE moved to remote learning with the expansion of the COVID-19 safety protocols. This was both a benefit and a detriment to the new system. The timing was positive because the new system allowed additional communication capabilities between faculty and students. Faculty could now text students to check in on their health and academic concerns. The push to all online courses also highlighted those additional communication features as face-to-face options were no longer available. These system features resulted in some faculty members' early adoption.

However, rolling out a new system during such a time of upheaval also caused issues. Faculty were not given an introduction and complete training to the system before they went remote. This meant there were issues with faculty not understanding the need, functions, and use of the system. The Fall 2020 trainings offered at the beginning of the next school year saw faculty asking what exactly this system was.

Since the initial rollout, the IHE has offered various training sessions on the use of specific features of the system. These were provided virtually, in a hybrid format, and via one-on-one training. Video recordings of the trainings were available for faculty to view, and email notices went out to faculty when they needed to engage with the system. For example, at the beginning of each semester, the faculty were requested to complete a progress report on students during the first weeks of class to note whether the students were attending or engaging with course content.

The IHE used the system to accomplish several institutional needs. First, it is used as a progress check early in the semester to determine if a student attended or participated in a course. This helps in correcting and ensuring appropriate registration records. The institution also used the alerts and communications sent within the system to make decisions. An email sent by the provost's office noted, "The primary source I have to make decisions about students' continued enrollment and respond to complaints from students and parents is your alerts and comments" (Artifact 59). Finally, the IHE used the system to set up appointments with various offices, such as advising, student housing, and financial aid. While allowing for a more focused, unified, and systematic approach, this also means the students have little choice in using the system.

3.2. Inductive Coding to Answer Research Questions

After conducting interviews and gathering resources from the IHE and the company, an inductive coding process was utilized to uncover themes. Overall, three main themes were discovered relating to the main research question: *How is the concept of privacy addressed in relation to a student success information system within an institution of public higher education?* The first theme was that privacy could be contained within the institution's adherence to the Family Educational Rights and Privacy Act of 1974 (FERPA). The second theme highlighted specific methods used to maintain privacy, including limiting access to information based on individual roles and ensuring technological security protocols. The final theme highlighted concerns raised about the relationship between students and their data.

3.2.1. FERPA Means Privacy

FERPA and other mentions of legal limitations were addressed across all the data sources, including interviews, company documents, and institutional documents. The company often provided a default mention of FERPA to provide a warning to institutions as they worked with different data sources and features, such as adding student demographic information to the system or adding notes to a student's record. Within one of their help centre articles, they note, "Do not do this unless you are aware of your institution's IT policies on data imports, privacy, FERPA, and other relevant policies" (Artifact 22). As mentioned in the company's training guides and help centre, institutions must be aware of FERPA as "any information you

enter into [the system] pertaining to a student becomes part of their official student record. It may be subpoenaed by the student as outlined in the Family Education Rights and Privacy Act (FERPA)" (Artifact 27). The company avoided providing specific guidance on how to comply with FERPA regulations.

This generic mention of FERPA was also seen in the training materials put out by the IHE. When discussing using the system during an in-person faculty training, it was noted, "We do have FERPA as a law and something that we follow" (Artifact 56). While it was not described in any detail, FERPA was invoked by describing how the system was initially set up by one of the administrators who took part in that process, "[The institution] adheres to the system level FERPA policy" (Artifact 49). The IHE made a conscious effort to address FERPA. It was also noted how the IHE went beyond some definitions of directory information from FERPA and included student emails as personally identifiable information. As one of the individuals involved in the original setup of the system, Paul noted, "Ours is a little bit more restrictive than the [governing] board level" (Artifact 49).

Even though FERPA was frequently mentioned, most documents and interviewees provided a cursory understanding of what FERPA entailed. The most detailed note on FERPA was from an email from the system administrator sent to faculty members, noting, "FERPA expressly allows for sharing of students' educational records with staff who have a legitimate educational interest in providing a service that benefits students" (Artifact 6). However, in the other trainings and documents reviewed, FERPA was acknowledged as important in relation to student privacy, but specific aspects of the law were not discussed. There was a general consensus in the IHE interviews that FERPA was being followed. Jim noted in an interview, "Part of the tight lockdown on access to the information was […] concern about FERPA compliance" (Artifact 57). This belief in the adherence to FERPA led to a belief that student privacy was being protected. After describing FERPA, administrator John noted in the interview, "I think those are the basic things that keep student information secure" (Artifact 50). After being asked about privacy, faculty member Rose stated, "We just got an email today saying that the FERPA instruction were online" (Artifact 60).

The literature did not stress compliance with FERPA since the activities involved with learning analytics were permissible under the law. While FERPA required students' consent to share their academic records with a third party, it did not impact any sharing within the institution. This exception was highlighted in the resources provided by the IHE. Beyond internal use, Parks (2017) noted that institutions were "Free to share any information in a student's academic record with any third party that they designate a 'school official'" (p. 26). This then addressed any concerns about the external company collecting student data.

Given that FERPA was not impacting the use of student data in this situation, it was concerning that it appeared so frequently within the discussion of student privacy at the IHE. Some interviewees focused almost solely on FERPA as the answer to privacy. While there are numerous other issues related to student privacy, FERPA appeared to be the extent of the individuals' knowledge on privacy for many interviewees. There appeared to be a sincere belief that student privacy was addressed. Interviewees at the IHE were unaware of the additional privacy issues related to learning analytics. While the IHE acted in good faith by addressing current FERPA requirements, the literature called for movement beyond the law. Parks (2017) concluded, "FERPA is unable to address many legal and ethical concerns around current uses of student data" (p. 24). Due to this, some authors called for institutions to move beyond FERPA (Jones, 2019; Prinsloo & Slade, 2015; Tene & Polonetsky, 2013).

3.2.2. Methods to Maintain Privacy

While FERPA was seen as a general aspect of privacy, when asked about more specific measures taken to protect privacy, several interviewees could not come up with additional items. Faculty member Bob noted, "I don't know of any. I really don't" (Artifact 47). Administrator John responded similarly, "I don't know" (Artifact 50). Faculty member Bill also shared this level of understanding, "Nope, I don't. I would have no idea" (Artifact 58).

The users' lack of understanding of student privacy is an important consideration moving forward for the IHE. While some of the literature on learning analytics considered the place of faculty members within the system, to the best of my knowledge, no studies looked at faculty and privacy specifically. These answers provided examples of some users' experience and knowledge.

Two main methods were discussed by interviewees who did have ideas on measures taken to promote and protect student privacy. The first dealt with limiting the type of student data accessible to individuals based on their roles. During an interview, faculty member Rose stated:

> I always assumed anything that I was limited to was based upon a law. I assume that whoever set this up does so with as much positive intent as possible. That faculty and administrative staff know the law and that we've done a good job of informing people of what they can and cannot show. So for that reason, I guess I just assume that whatever I don't have access to is a legal restriction, not somebody just restricting it because it's not necessary. (Artifact 60)

This role-based access to the system was one of the foundational considerations when the system was set up. Paul, who was part of the team that set up the system, noted, "Permission access points were migrated from the shared student information system in terms of roles" (Artifact 49). Jim, who helped in the setup of the system and uses it as a faculty member, described the setup of the roles, noting the following:

> [They were] very thoughtful about what sort of information should be collected and who has access. […] That was very deliberate. And there was actually a lot of conversation about that, and that's also why in the beginning it was restricted so much, was in protection of students. (Artifact 57)

Within the ethical guidelines put out by the IHE was a section telling users to "access only student data that is relevant to your role. Some […] may allow access […] outside your role […]. By using data related to your role, you can make the greatest impact and maintain compliance with federal guidelines, such as FERPA" (Artifact 55). The company itself also noted the importance of roles, describing the following in a help centre article:

> [The system] provides the granular permissions necessary to ensure that only educational representatives that have legitimate need and right to see a student's information (courses scheduled, credit accumulation, degree progression, etc.) can access that information. The system provides role-based access, allowing access to certain data to only those users with sufficient privileges. (Artifact 34)

The importance of using roles to limit access to types of data mirrors the privacy and learning analytics literature, which talks extensively about the limitation of data. In their discussions on privacy, Pavlou (2011) and Moor (1997) noted that it should be up to each individual to decide who can access their data. Austin (2019) built on this idea, noting that it was not the quantitative amount of information available that caused privacy concerns but rather who had access to that information and their relationship with the individual. Within the learning analytics literature, Slade and Prinsloo (2013) noted how limiting access to data to authorized individuals was one feature of a secure system. This was seen within the documents and interviews of the case study. This understanding of the importance of access was highlighted in the UK's *Code of Practice for Learning Analytics* as it included access as one of the features institutions should consider when establishing a learning analytics system (Sclater & Bailey, 2018). While developed in the UK, this code covered general aspects of learning analytics while allowing for individualized implementation based on location and local needs.

At the IHE, privacy was also seen through the lens of technology security. The system director noted, "There's a lot of stops that we have in place that would try to make it so that nobody would just get in, you know, it's all in a single sign on" (Artifact 48). When asked about privacy measures in the system, Administrator John noted, "It is password protected, so I think those are the basic things that keep student information secure" (Artifact 50). Users of the system were also encouraged to use standard security practices. During an in-person training, it was noted to users that when using the system in places where others could view their computer, "Don't leave it open […] or walk away" (Artifact 56). The company also provided details related to the technological security aspects of the service within their help centre:

> All emails stored in the […] platform are encrypted at rest, which prevents unauthorized access or theft in the unlikely event that the raw data is accessed by unauthorized agents. The encryption keys are stored separately from the data and are updated on a regular basis. (Artifact 33)

The learning analytics literature also revealed the importance of the technical security issues addressed in the interviews. Privacy and technical security are connected as security is required for privacy. Cavoukian's (2012) privacy by design framework includes end-to-end security as one of the seven principles. Due to this connection, security is often mentioned in lists of ethical concerns related to learning analytics (Khalil & Ebner, 2016; Slade & Prinsloo, 2013; Steiner et al., 2016). Pardo and Siemens (2014) also noted how security impacted learning analytics.

3.2.3. Students' Connection With Their Data

In general, the administrators and users of the system did not have concerns about student privacy. Faculty member Bob stated, "It's kind of the unspoken expectation that we respect that kind of stuff" (Artifact 47). Administrator and faculty member Jim noted, "We have to trust the people that you hire. That they'll use the material in the right way" (Artifact 57). These comments highlighted the idea that privacy was only a problem when misused by faculty and staff to benefit themselves. There was no nuanced belief that privacy could be violated without a specific breach or harm. For example, there was no mention of concern with the type of data gathered or how long it was maintained. Overall, the system was seen as an institutional good, and as such, the procedures were also seen as good.

There were a couple of suggestions offered that interviewees felt would increase the privacy of the system. During the interview, Bob noted, "I don't know if students know what kind of system this is and if they've signed off saying, 'I'm okay with that'" (Artifact 47). This concern with student consent moved beyond basic agreement to deep comprehension, with Bob expressing a desire for students to "really understand it with all the other things going on in their life when they first arrive on campus" (Artifact 47).

Creating a system that allows students to provide informed consent is critical in the literature surrounding learning analytics (Slade & Prinsloo, 2013; Slade & Tait, 2019; Steiner et al., 2016). Jones (2019) noted how, historically, the idea that an individual had a right to control who knows specific information about themselves had long been central to privacy. This loss of control might occur either through institutions not asking for consent or by asking for consent without providing a clear description as to how the data would be used. The requirement of having a clear description was also noted in the interview, as consent without understanding does not allow for meaningful consent. Slade and Prinsloo (2013) added that when asking for consent, institutions should also provide details on the possible benefits and harms resulting from sharing or not sharing the information.

Another concern brought forward by faculty was the ability to correct data if necessary. Faculty member Rose noted in the interview, "It'd be cool if students could update certain aspects like demographic or stuff that wouldn't require another person to integrate" (Artifact 60). The ability of an individual to correct information is vital as it addresses two components related to privacy. First, this means that students have access to the data connected to them. This openness and transparency on the information collected about them allows for greater trust and cooperation. Second, the ability to make corrections allows students to keep a more accurate record of themselves. Slade and Tait (2019) noted that students should have access to their raw and analyzed data so they can make corrections as necessary. Ferguson et al. (2016) also included, in their list of challenges with learning analytics, that institutions should offer opportunities to correct data but added that this process should be publicized so students would know it. This ability to make corrections is codified within FERPA, with students being able to correct errors in their educational records (Daggett, 2008).

3.3. Policies Lead to Trust

The IHE in this case study was at a crucial juncture. They had been utilizing the student success information system for over two years. During that time, they started getting students and faculty comfortable with using the system as a communication tool. As they begin to prepare to take full advantage of the learning analytics functionality, they have the opportunity to take a strategic approach by developing policies and codes of practice that address all aspects of the system, including privacy. Developing clear and straightforward policies with the input of stakeholders, including students, provides a framework for successful implementation due to the trust and buy-in that would be established (Long & Siemens, 2011).

While the current policies provide a baseline and the ethical use document created by the IHE provides some specific contexts, it would be best for the IHE to develop and adopt specific policies related to using student data within the student success information system. These policies, while addressing student privacy, are also needed to define other considerations within the system, such as questions related to ethical, legal, and logistical issues; a list of stakeholders with responsibilities; and a proposed action plan with steps to take in developing a code of practice (Sclater, 2016). In developing these policies, the institution would be able to have conversations related to the larger impact of the system.

In developing their code of practice for learning analytics for Jisc, a digital, data, and technology agency that focuses on education, research, and innovation, Sclater and Bailey (2018) highlighted the need for institutions to have complete transparency in their use of learning analytics including purpose, data collected, processes, and how the data would be used. This transparency helps to establish trust. Pavlou (2011) listed several research studies examining the relationship between trust and privacy. Overall, individuals showed less concern with privacy if they had established trust with the institution.

Austin (2019) highlighted how it was not enough to provide individuals with choice concerning their privacy. Her essay noted that while personal control had long been a critical component of maintaining privacy, it was not enough if the choices must occur in situations that do not provide real options. She proposed providing an environment where meaningful choices could be made, allowing for various states of privacy. Her critique of individual control through informed consent was also highlighted by Jones (2019), who noted that individuals did not truly understand what they were consenting to or how their information would be utilized. Choice and options were not addressed meaningfully by the IHE. While students could opt out of receiving text messages and limit how much they used the system personally, they could not remove themselves from the system as a whole. Their data was included in the system, and they had to utilize the system to engage with some departments on campus.

Focusing exclusively on users' choices puts the onus on individuals to protect their privacy rather than developing structures in the systems themselves that support privacy. For student data systems to establish trust, they must build privacy into their systems. This "requires a shift from focusing on particular informational interaction between individuals and others and taking a more systemic view of the informational environment to ask whether it generally supports privacy" (Austin, 2019, p. 56).

Hoel and Chen (2016) noted that trust was one of the main barriers to adopting learning analytics. For students to feel comfortable sharing their information, they must trust that the institution will use it appropriately. Several researchers noted that trust was critical for the ongoing use of learning analytics (Cormack, 2016; Green & Baumal, 2019; Pardo & Siemens,

2014; Prinsloo & Slade, 2015; Steiner et al., 2016). Rubel and Jones (2016) discussed how transparency about learning analytics provided personal autonomy and trust in the system. They suggested syllabi should include statements noting the use of learning analytics and the end result of that use.

Currently, documentation produced by the IHE for students, faculty, and staff focuses on how to use the system rather than the result of using the system. It is essential to understand what students think of learning analytics as their information is being used. For institutions to "push forward with learning analytics *without* considering student privacy preferences — or ignoring such preferences altogether — is foolhardy and morally suspect" (Jones, 2019, p. 12).

Not only is it critical to include students in the use of learning analytics, but Ifenthaler and Schumacher (2016) also noted the need to include other stakeholders, such as instructors and instructional designers, to ensure that the data collected supported student learning. Having the ability to collect information does not mean it is necessary or proper to do so. The IHE did consider what data to collect when setting up the system. The process that was used brought in different individuals, which allowed for various viewpoints. For example, student birthdays were not included in the system. While it is possible to include it as a data point, someone spoke up about how it should not be included.

4. Conclusion

4.1. Implications for IHE

Currently, the IHE has opportunities to improve the level of privacy considerations they make for student data. Those changes could be made at an administrative level, such as developing a process for data breaches. However, the IHE must also work with the faculty and staff users of the system to promote appropriate approaches to protecting student privacy. Official policies may have little impact if the day-to-day procedures do not follow best practices.

The interviews within the case study highlighted little concern among users regarding the privacy issues related to accessing and using student information. This lack of concern may result in the careless use of the information and system. It is crucial for the IHE to provide guidance for faculty on how to appropriately use student information and include possible consequences for misuse. The consequences vary from simple loss of confidentiality to financial and psychological harm, which may result in negative publicity or legal action. All consequences, however, will mean a loss of trust, which, as noted earlier, is critical in ensuring a successful implementation of student success information systems.

4.2. Recommendations, Limitations, and Future Work

The use of student data for learning analytics will continue to expand; as Judy noted, "I think that it's getting more and more robust, and there's more and more things that we can do with it" (Artifact 48). Higher education institutions would be best served by ensuring that the system meets not only the academic needs of the students and the institution but also the personal privacy needs of the students as well.

One of the main recommendations for higher education institutions, such as the IHE, as they begin a more focused push with learning analytics is to spend time developing policies and procedures. This focused time will allow for buy-in and uncover possible issues that can be addressed early in the process. When such processes are developed, special attention should be paid to how learning analytics can impact student privacy. The IHE herein appeared to be unaware of some of the privacy concerns addressed in the learning analytics literature, such as black box algorithms, where the criteria used to make decisions are unknown by the institution (Oakleaf, 2016; SoLAR, 2021) and biased analytics where the data points selected for analysis might cause inherent bias in the results (Romei & Ruggieri, 2014). Thus, before the policies and procedures are developed, it may be necessary for the system director and administrators of higher education institutions to review prior research on ethical concerns with learning analytics as well as review some best practice examples from other institutions that are further along in their implementation of learning analytics.

Another recommendation for higher education institutions would be to establish and communicate clear goals related to using the system. While the interviews uncovered similar goals shared by the administrators and faculty users of the system, there were differences in the importance the different individuals placed on the goals. This variety would result in different foci when using the system, which then leads to variety in the importance placed on student data and privacy. This means higher education institutions must create clear communication plans surrounding their learning analytic systems to meet the goals ascribed to those systems.

While this case study herein was undertaken to fulfill a gap in the literature calling for specific case studies looking at learning analytic systems, as noted by Kitto and Knight (2019) and Cerratto Pargman and McGrath (2021), additional studies could provide more insight into how institutions are implementing learning analytics. The case study herein offered a look at an IHE that had a functional communications component of a student success information system but had not fully implemented the learning analytics component. To address this limitation, additional case studies could consider institutions

within different stages of implementing learning analytics. Such studies could provide insight into practices that have gone well or not.

The case study herein also provided an example of how faculty understand privacy related to learning analytics. This area could see additional research with surveys of faculty members to understand what faculty know and think about learning analytics. Lastly, this case study looked at interviews and documents on users' thoughts about the system. Future work can consider how users implement and engage with the system by observing faculty and students using it to uncover possible privacy issues.

Declaration of Conflicting Interest

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors declared no financial support for the research, authorship, and/or publication of this article.

References

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society.* Rowman & Littlefield.

Austin, L. M. (2019). Rereading Westin. *Theoretical Inquiries in Law, 20*(1), 53–81. https://doi.org/10.1515/til-2019-0003

Bellotti, V. (1997). Design for privacy in multimedia computing and communications environments. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape* (pp. 63–98). MIT Press.

Burns, S. (2020, November 19). *The evolving landscape of data privacy in higher education*. EDUCAUSE. https://www.educause.edu/ecar/research-publications/the-evolving-landscape-of-data-privacy-in-higher-education/introduction

Castelli, C. J. (2014, October 3). *NIST's draft privacy-engineering concepts avoid defining privacy*. Inside cybersecurity. https://insidecybersecurity.com/share/1850

Cavoukian, A. (2012). *Privacy by design: From rhetoric to reality.* Information and Privacy Commissioner, Ontario.

Cormack, A. N. (2016). A data protection framework for learning analytics. *Journal of Learning Analytics, 3*(1), 91–106. https://doi.org/10.18608/jla.2016.31.6

Data Quality Campaign. (2019, December 4). *Time to act: Connecting policy to practice to make data work for students*. https://dataqualitycampaign.org/resource/time-to-act-2019/

Daggett, L. M. (2008). FERPA in the twenty-first century: Failure to effectively regulate privacy for all students. *Catholic University Law Review, 58*, 59–113. https://scholarship.law.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=3151&context=lawreview

Drachsler, H., & Greller, W. (2016). Privacy and analytics — it's a DELICATE issue: A checklist for trusted learning analytics. *Proceedings of the 6th International Conference on Learning Analytics and Knowledge* (LAK '16), 25–29 April 2016, Edinburgh, UK (pp. 89–98). ACM Press. https://doi.org/10.1145/2883851.2883893

Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (1974).

Ferguson, R., Hoel, T., Scheffel, M., & Drachsler, H. (2016). Guest editorial: Ethics and privacy in learning analytics. *Journal of Learning Analytics, 3*(1), 5–15. http://dx.doi.org/10.18608/jla.2016.31.2

Foster, C., & Francis, P. (2020). A systematic review on the deployment and effectiveness of data analytics in higher education to improve student outcomes. *Assessment & Evaluation in Higher Education, 45*(6), 822–841. https://doi.org/10.1080/02602938.2019.1696945

Gasevic, D., Dawson, S., & Jovanovic, J. (2016). Ethics and privacy as enablers of learning analytics. *Journal of Learning Analytics, 3*(1), 1–4. https://doi.org/10.18608/jla.2016.31.1

Grajek, S. (2020). Top 10 IT issues 2020: The drive to digital transformation begins. *EDUCAUSE Review Special Report.* https://er.educause.edu/-/media/files/articles/2020/1/er20sr201.pdf

Green, P., & Baumal, B. (2019). Legal, ethical and privacy issues affecting data sharing among Ontario's higher education institutions in interinstitutional collaboration. *College Quarterly, 22*(2). https://files.eric.ed.gov/fulltext/EJ1221437.pdf

Hoel, T., & Chen, W. (2016). Privacy-driven design of learning analytics applications: Exploring the design space of solutions for data sharing and interoperability. *Journal of Learning Analytics, 3*(1), 139–158. https://doi.org/10.18608/jla.2016.31.9

Horvitz, E. (1999). Principles of mixed-initiative user interfaces. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '99), 15–20 May 2009, Pittsburgh, PA, USA (pp. 159–166). Human Factors in Computing Systems. https://doi.org/10.1145/302979.303030

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

Jensen, C., Tullio, J., Potts, C., & Mynatt, E. D. (2005). STRAP: A structured analysis framework for privacy. *GVU Technical Report.* http://hdl.handle.net/1853/4450

Jones, K. M. L. (2019). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Education Technology in Higher Education, 16*(1), 24. https://doi.org/10.1186/s41239-019-0155-0

Khalil, M., & Ebner, M. (2016). De-identification in learning analytics. *Journal of Learning Analytics*, *3*(1), 129–138. https://doi.org/10.18608/jla.2016.31.8

Kim, D., Yoon, M., Jo, I.-H., & Branch, R. M. (2018). Learning analytics to support self-regulated learning in asynchronous online courses: A case study at a women's university in South Korea. *Computers & Education*, *127*, 233–251. https://doi.org/10.1016/j.compedu.2018.08.023

Kitto, K., Cross, S., Waters, Z., & Lupton, M. (2015). Learning analytics beyond the LMS: The connected learning analytics toolkit. *Proceedings of the 5th International Conference on Learning Analytics and Knowledge* (LAK '15), 16–20 March 2015, Poughkeepsie, NY, USA (pp. 11–15). ACM Press. https://doi.org/10.1145/2723576.2723627

Kitto, K., & Knight, S. (2019). Practical ethics for building learning analytics. *British Journal of Educational Technology, 50*(6), 2855–2870. https://doi.org/10.1111/bjet.12868

Knight, S., Buckingham Shum, S., & Littleton, K. (2014). Epistemology, assessment, pedagogy: Where learning meets analytics in the middle space. *Journal of Learning Analytics, 1*(2), 23–47. https://doi.org/10.18608/jla.2014.12.3

Langheinrich, M. (2001). Privacy by design—Principles of privacy-aware ubiquitous systems. In G. D. Abowd, B. Brumitt, & S. Shafer (Eds.), *Ubicomp 2001: Ubiquitous Computing* (pp. 273–291). Springer Berlin Heidelberg. https://doi.org/10.1007/3-540-45427-6_23

Long, P., & Siemens, G. (2011). Penetrating the fog: Analytics in learning and education. *EDUCAUSE Review, 46*(5), 30–40.

Margulis, S. T. (2011). Three theories of privacy: An overview. In S. Trepte & L. Reinecke (Eds.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (pp. 9–17). Springer. https://doi.org/10.1007/978-3-642-21521-6_2

Moor, J. H. (1997). Towards a theory of privacy in the information age. *Computers & Society, 27*(3), 27–32. https://doi.org/10.1145/270858.270866

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus*, *140*(4), 32–48. https://doi.org/10.1162/DAED_a_00113

Oakleaf, M. (2016). Getting ready & getting started: Academic librarian involvement in institutional learning analytics initiatives. *The Journal of Academic Librarianship*, *42*(4), 472–475. https://doi.org/10.1016/j.acalib.2016.05.013

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

Cerratto Pargman, T., & McGrath, C. (2021). Mapping the ethics of learning analytics in higher education: A systematic literature review of empirical research. *Journal of Learning Analytics*, *8*(2), 123–139. https://doi.org/10.18608/jla.2021.1

Parks, C. (2017). Beyond compliance: Students and FERPA in the age of big data. *Journal of Intellectual Freedom & Privacy, 2*(2), 23–33. https://doi.org/10.5860/jifp.v2i2.6253

Pavlou, P. A. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly, 35*(4), 977–988. https://doi.org/10.2307/41409969

Prinsloo, P., & Slade, S. (2013). An evaluation of policy frameworks for addressing ethical considerations in learning analytics. *Proceedings of the 3rd International Conference on Learning Analytics and Knowledge* (LAK '13), 8–12 April 2013, Leuven, Belgium (pp. 240–244). ACM Press. https://doi.org/10.1145/2460296.2460344

Prinsloo, P., & Slade, S. (2015). Student privacy self-management: Implications for learning analytics. *Proceedings of the 5th International Conference on Learning Analytics and Knowledge* (LAK '15), 16–20 March 2015, Poughkeepsie, NY, USA (pp. 83–92). ACM Press. https://doi.org/10.1145/2723576.2723585

Privacy Technical Assistance Center. (2016). Protecting student privacy while using online educational services: Model terms of service. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Mar2016.pdf

Romei, A., & Ruggieri, S. (2014). A multidisciplinary survey on discrimination analysis. *The Knowledge Engineering Review, 29*(5), 582–638. https://doi.org/10.1017/S0269888913000039

Rubel, A., & Jones, K. M. L. (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

Saqr, M., Fors, U., & Tedre, M. (2017). How learning analytics can early predict under-achieving students in a blended medical education course. *Medical Teacher, 39*(7), 757–767. https://doi.org/10.1080/0142159X.2017.1309376

Sclater, N. (2016). Developing a code of practice for learning analytics. *Journal of Learning Analytics, 3*(1), 16–42. http://dx.doi.org/10.18608/jla.2016.31.3

Sclater, N., & Bailey, P. (2018). *Code of practice for learning analytics*. Jisc. https://repository.jisc.ac.uk/6985/1/Code_of_Practice_for_learning_analytics.pdf

Selwyn, N. (2019). What's the problem with learning analytics? *Journal of Learning Analytics, 6*(3), 11–19. https://doi.org/10.18608/jla.2019.63.3

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information, 22*(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist, 57*(10), 1380–1400. https://doi.org/10.1177/0002764213498851

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., & Tait, A. (2019). Global guidelines: Ethics in learning analytics. *International Council for Open and Distance Education.* https://www.aace.org/review/global-guidelines-ethics-in-learning-analytics/

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015. https://doi.org/10.2307/41409970

Society for Learning Analytics Research (SoLAR). (2021). *What is learning analytics?* https://www.solaresearch.org/about/what-is-learning-analytics/

Solove, D. J. (2002). Conceptualizing privacy. *California Law Review*, *90*(4), 1087–1155. https://doi.org/10.2307/3481326

Solove, D. J. (2008). 'I've got nothing to hide' and other misunderstandings of privacy. *San Diego Law Review, 44,* 745–772. https://ssrn.com/abstract=998565

Steiner, C. M., Kickmeier-Rust, M. D., & Albert, D. (2016). LEA in private: A privacy and data protection framework for a learning analytics toolbox. *Journal of Learning Analytics, 3*(1), 66–90. https://doi.org/10.18608/jla.2016.31.5

Tene, O., & Polonetsky, J. (2013). Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property, 11*(5), 239–274. https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

Tracy, S. J. (2010). Qualitative quality: Eight "big-tent" criteria for excellent qualitative research. *Qualitative Inquiry, 16*(10), 837–851. https://doi.org/10.1177/1077800410383121

Weimann, T., & Nagel, D. (2012). Agreeing on a definition for data protection in a globalized world. *IEEE Technology and Society Magazine*, *31*(4), 39–42. https://doi.org/10.1109/MTS.2012.2225673

Welsh, S., & McKinney, S. (2015). Clearing the fog: A learning analytics code of practice. *Proceedings of the 32nd Annual Conference of the Australasian Society for Computers in Learning and Tertiary Education* (ASCILITE 2015), 29 November–2 December 2015, Perth, Western Australia (pp. 588–592). Australasian Society for Computers in Learning in Tertiary Education. https://www.researchgate.net/publication/290436709_Clearing_the_Fog_A_Learning_Analytics_Code_of_Practice

Yin, R. K. (2009). *Case study research: Design and methods* (4th ed.). Sage.

ISSN 1929-7750 (online).