JOURNAL OF LEARNING ANALYTICS
SOLAR SOCIETY for LEARNING ANALYTICS RESEARCH
Volume 9(3), 169–182. https://doi.org/10.18608/jla.2022.7751

Privacy in LA Research: Understanding the Field to Improve the Practice

Olga Viberg[1], Chantal Mutimukwe[2], Åke Grönlund[3]

Abstract
Protection of student privacy is critical for scaling up the use of learning analytics (LA) in education. Poorly implemented frameworks for privacy protection may negatively impact LA outcomes and undermine trust in the discipline. To design and implement models and tools for privacy protection, we need to understand privacy itself. To develop better understanding and build ground for developing tools and models for privacy protection, this paper examines how privacy hitherto has been defined by LA scholars, and how those definitions relate to the established approaches to define privacy. We conducted a scoping review of 59 articles focused on privacy in LA. In most of these studies (74%), privacy was not defined at all; 6% defined privacy as a right, 11% as a state, 15% as control, and 16% used other approaches to explain privacy in LA. The results suggest a need to define privacy in LA to be able to enact a responsible approach to the use of student data for analysis and decision-making.

Notes for Practice

- There is a need to better define privacy in LA to be able to enact a more responsible approach to using student data for analysis and decision-making.
- There is much conceptual unclarity related to understanding privacy in LA.
- Privacy means different things for students, teachers, and educational institutions; systems must be designed to meet the needs of all.
- The context in which stakeholder privacy is targeted must be considered.

Keywords
Learning analytics, privacy, definition, scalability, impact

Submitted: 05/05/2022 — **Accepted:** 27/09/2022 — **Published:** 13/12/2022

Corresponding author [1]Email: oviberg@kth.se Address: KTH Royal Institute of Technology, Department of Human-Centered Technology, Lindstedsvägen 3, 10044 Stockholm, Sweden. ORCID ID: https://orcid.org/0000-0002-8543-3774
[2]Email: chantal.mutimukwe@dsv.su.se Address: Stockholm University, Department of Computer Systems & Sciences, NOD-huset, Borgarfjordsgatan 12, 164 55 Kista, Sweden. ORCID ID: https://orcid.org/0000-0002-5966-7649
[3]Email: ake.gronlund@oru.se Address: Örebro University School of Business, Department of Informatics, Handelshöskolan, 70182 Örebro, Sweden. ORCID ID: https://orcid.org/0000-0002-3713-346X

1. Introduction

Privacy has been reported to be one of the key obstacles that hinders the implementation and adoption of learning analytics (LA) in various educational contexts (e.g., Pardo & Siemens, 2014; Li et al., 2021; Tsai et al., 2020). Privacy issues are of increasing concern to multiple stakeholders in LA settings (Kimmons, 2021; Mutimukwe et al., 2021). There are concerns regarding how student data are collected, used, and analyzed to draw conclusions about learning, attitudes, and behaviours for improved learning in the context of LA. As argued by Reidenberg and Schaub (2018), "the potential of supporting the learning process through educational data mining and learning analytics also carries the risk of privacy harms, particularly with respect to fairness in data processing and with respect to the detriment effects from profiling of students" (pp. 275–276). Scholars also stress that research institutions and private companies operating in education and LA solutions "still rely on ad hoc, red-tape-heavy and inconsistent approaches to privacy protection" (Joksimović et al., 2022, p. 1). Poorly implemented privacy protection mechanisms, which may undermine user trust and lead to poor outcomes, may indeed be a threat to the LA discipline.

To design and implement models and tools for privacy protection, the LA field must better understand privacy itself and the settings in which it must be protected. Privacy is often presented, examined, and discussed in various ways in LA; at times, these are confusing and lacking in clear definitions. Ferguson et al. (2016), for example, posit that the interrelated issues of ethics, data protection, and privacy should be considered separately. Furthermore, LA scholars (Jones, Asher et al.,) emphasize

that there is still a lack of clarity in the conceptualization of student privacy due to its multifaceted and complex characteristics. Others underline the need to unpack the privacy concept in terms of its sociocultural context (Drachsler et al., 2015). Recently, scholars have also stressed a need to approach student data privacy as a social problem as opposed to understanding it as a purely technological issue (Prinsloo et al., 2022).

Contrary to LA research, where there is a clear need to protect stakeholder privacy, the concept of privacy has been defined and thoroughly studied in other fields, including economics and information systems, where researchers frequently offer definitions and conceptualizations of privacy (e.g., Smith et al., 2011). Definitions of privacy vary depending on the field, "ranging from a 'right' or 'entitlement' in law (Wright & Raab, 2014) to a 'state for limited access or isolation' in philosophy and psychology (Panichas, 2014) to 'control' in social sciences and information systems" (Xu et al., 2011, p. 798). The LA field has yet to develop such clarity and in-depth analysis. This is a serious constraint to both LA theory and practice. It may impede not only our understanding of what constitutes privacy in LA, but also what can and should be done in practice to protect student privacy and enable their agency in LA contexts.

Considering the importance of privacy to LA research and practice coupled with the limited understanding of what constitutes privacy in LA, the present study aims fill this gap by examining definitions of privacy in the context of LA. We conducted a scoping literature review that analyzed 59 articles based on the established categorization of privacy definitions suggested by Smith et al. (2011). According to that categorization, privacy definitions can be classified into two key categories: *value-based* and *cognate-based*, where the former consider privacy as a *right* or a *commodity*, and the latter as a *state* or *control* (for details, see section 2, Background).

To better understand how privacy has been defined in LA, this study aims to answer the following research questions:

1. 1) How do the definitions of privacy in learning analytics relate to established approaches to categorizing privacy?
2. 2) What, if any, (other) approaches specific to learning analytics are there to define privacy?

2. Background

2.1. Defining Privacy

It is widely suggested that privacy as a concept "is in disarray and nobody can articulate what it means" (Solove, 2006, p. 477). It may be more accurate to say that in research, there are many perspectives on privacy and in practice, there are many different regulations in different countries. Many attempts to bring together the various perspectives of privacy in different research areas have been undertaken, but "the picture that emerges is fragmented with concepts, definitions, and relationships that are inconsistent and neither fully developed nor empirically validated" (Smith et al., 2011, p. 992). Based on a large interdisciplinary review of information privacy research, grounded in the analysis of 320 articles and 128 books and book chapters, Smith et al. (2011) identified two key definitional approaches to privacy: 1) *value-based* and 2) *cognate-based.* While there are several approaches to structuring the concept of privacy, we chose this framework as our reference point because it emanates from the information systems field, and hence thoroughly considers technology and human-technology relations, and because it is one of the most influential and cited.

The *value-based* approach views privacy as a human right integral to society's moral value system (Smith et al., 2011, pp. 992–993). According to this approach, privacy is defined as a *right* and, as a *commodity.* The former emerges from the literature that sees privacy as "the right to be left alone" (Smith et al., 2011). This view has been adopted from a law review by Warren and Brandeis (1890), in which privacy was viewed as a developing right in U.S. law. Bennett (1995) theorized the notion of privacy as a commodity, suggesting that privacy as an individual and societal value is not absolute. That is, it can be assigned an economic value in a cost–benefit calculation at both the individual and societal levels; this relates to the emergence of the privacy paradox concept, also discussed in the LA context (e.g., Tsai et al., 2020). To explain the phenomenon of voluntarily providing information online (so-called self-surveillance), scholars acknowledge the economic component of privacy: individuals co-operate in the online gathering of data about themselves as economic subjects (Prinsloo & Slade, 2016).

The *cognate-based* definitions of privacy explain privacy in two ways: privacy as a *state* and privacy as *control.* The concept of privacy as a *state* was introduced by Westin (1967), who defined privacy through four distinct substates: anonymity, solitude, reserve, and intimacy. Later, Schoeman (1984) also defined general privacy as "a state of limited access to a person" (p. 3). Weinstein (1971) explained privacy as a state of "being apart from others" (p. 626). Further, Laufer and Wolfe (1977) conceptualized privacy as a situational concept (state) linked to concrete situations with three dimensions: self-ego, environmental, and interpersonal. Information systems, economics, and marketing scholars narrowed these definitions of general privacy so that they addressed information-based issues. The state of limited access was translated to state of limited access to information. When privacy is viewed as a state, it is natural for researchers to consider it in terms of its role as a sought-after goal (i.e., an individual's desire to exist in a state of privacy).

The concept of privacy as *control* is grounded in Westin's (1967) and Altman's (1975) theories of privacy. Margulis (1977) elaborated on those theories and proposed a control-centred privacy definition: "Privacy, as a whole or in part, represents the

control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability" (p. 10). The control-based definition has since gone into the mainstream of privacy research — "likely because it lends itself more readily to the attributes of information privacy" (Smith et al., 2011, p. 995). Table 1 summarizes the classification of definitions of privacy offered by Smith et al. (2011) and used as the analytical lens in this study.

Table 1. Established Approaches to Define Privacy

1. Value-based definitions	**1.1. Privacy as a *right***	**1.2. Privacy as *commodity***
Privacy is seen as a human right integral to society's moral value system.	In general, privacy is human right. Privacy is "The right to be left alone" (Warren & Brandeis, 1890). Key phrases: Developing right (in U.S. law) Protection for warrantless search Establishes the personal realm by excluding it from public scrutiny	Privacy is not an absolute right but is subject to the economic principles of cost-benefit analysis and trade-off (Bennett, 1995; Cohen, 2001). Key phrases: Voluntary provision of the information online or self-surveillance Individuals co-operate in the online collection of data about themselves as economic subjects
2. Cognate-based definitions	**2.1. Privacy as a *state***	**2.2. Privacy as *control***
The understanding of privacy is related to the individual's mind, perceptions, and cognition rather than to an absolute moral value or norm.	Privacy is "a state of limited access": • "to a person" (Schoeman, 1984, p. 3). • to information (Smith et al., 2011). Privacy is as a state of "being apart from others" (Weinstein, 1971, p. 626). Key phrases: Anonymity Solitude Reserve Intimacy Limited access to information	Privacy, as a whole or in part, represents the control of transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability (Margulis, 1977, p. 10). Key phrases: The ability to control is central Control is a key factor shaping privacy

Source: Adapted from Smith et al., 2011.

The different perspectives are not necessarily mutually exclusive, they go well together in at least some combinations, but less so in others. For example, viewing privacy as a *commodity*, which, at least to some extent and in some contexts, is negotiable, is compatible with the view of privacy as control. In many situations there is likely to be different views among stakeholders about the suitable extent of privacy. For example, in social media, company business models require collecting and trading information about users and this information is legally obtained by having users explicitly accept cookies. Users trade some of their privacy for access to the service. That way, control over the access stays with the user. Control over third-party use of information is also "negotiated" away, but without the user knowing exactly where and for what it will be used. It may be debated how voluntary a user clicking the "accept" button is since there is no other way to access the complete service.

Viewing privacy as a *right* goes well together with seeing it as a *state.* For example, the EU's General Data Protection Regulation (GDPR) is defined to protect citizens' right to privacy, and the state of compliance with GDPR can be measured. A strict review can argue that the current social media practice violates the right — the spirit behind the privacy legislation — as the acceptance is done in an unbalanced power relation, and as it is impossible for users to know how third parties handle the information. Still, this is a practice many people accept. One approach to discussing the problem of combining a legal right with contextual requirements is *contextual integrity*, which suggests that privacy is preserved when information flows generated in some practice "conform to the legal contextual information norms" (Nissenbaum, 2019, p. 224), and consequently violated when these are breached.

2.2. Privacy in LA

Kitchin (2021) stresses that "data-driven endeavours are not simply technical systems but are socio-technical systems" (p. 5). LA has similarly been defined as a sociotechnical practice (Jones, Briney et al., 2020), in which the protection of student

privacy in education is central. Student privacy is not a new concern in LA (Jones, Asher et al., 2020; Pardo & Siemens, 2014; Prinsloo & Slade, 2015) but there are still gaps that must be addressed, including the need to conceptualize the privacy concept in the LA setting (e.g., Jones et al., 2021).

Some researchers have already attempted to perform relevant review studies. In their recent meta-analysis of research in the area of LA, Priedigkeit et al. (2021) focused on the considerations of privacy in the context of usage groups, technologies, and intended users. Based on the analysis of 23 papers, the study found that privacy issues have been mostly addressed in surveys or guides but rarely in actual LA implementations. Also, the authors stress that data usage is not transparent, and consequently, offers a set of privacy risks to analyze in LA systems. They regard several issues, including confidentiality, integrity, availability, and transparency. Through a rapid review of 12 articles, Botnevik (2021) examined student perceptions of privacy principles in LA in educational contexts and found scarce research and inadequate insight. The study found that the privacy principle of *control* is essential for students across countries, but it is not the most explored principle (compared to consent and anonymity). A lack of related studies in Nordic countries, Latin America, Africa, and Asia was also found. In a recent editorial paper, Kimmons (2021) calls for researchers, practitioners, and policy-makers to be more aware of, and responsive to, student privacy in LA systems, stressing that "professional standards in this space remain somewhat nebulous at present and require ongoing leadership, thoughtfulness, and sensitivity to ethical behaviour" (p. 345). To achieve this and to be able to protect stakeholder privacy in LA, the need to define privacy is obvious. As highlighted by Cerratto Pargman and McGrath (2021), "[a] minority of the articles reviewed refer more specifically to theorization on privacy" (p. 132).

3. Method

This study presents a scoping literature review, which is particularly useful when the topic "has not been extensively reviewed or is of complex or heterogeneous nature" (Pham et al., 2014, p. 371). Despite the urgent need to approach student privacy in a more responsible way, the conceptualization of privacy itself in LA has not been extensively reviewed or comprehensively discussed in the literature. The concept itself is multidimensional and it is critical for *practicable LA* (i.e., LA that would lead to improved learning at scale) in education because that practice is heavily — while not necessarily clearly — regulated by law and is important to practitioners who handle sensitive information about students. Furthermore, Munn et al. (2018) posit several purposes of performing a scoping literature review, including clarification of key concepts (or definitions), which is central to this study.

3.1. Literature Search Strategy

We initially searched for publications through PRIMO (Peer-Reviewed Instructional Materials Online Database),[1] which includes several key databases (e.g., Web of Science, SCOPUS, ERIC, DBLP). To complement the search, we also manually examined the field-specific *Journal of Learning Analytics*. Further, we examined articles published in related special issues; for example, *Educational Technology Research and Development* (vol. 69, 2021) and *Journal of Learning Analytics* (vol. 3, 2016). We also conducted a manual search of articles published in the proceedings of the *International Learning Analytics and Knowledge* (LAK) conferences for the years 2011–2021.

In the databases, the search terms "learning analytics" AND "privacy" and "learning analytics" AND "ethics" as well as "learning analytics" AND "privacy" AND "ethics" were used. Titles, keywords, and abstracts were searched. To ensure reliability and validity, we carefully read the title, abstract, and keywords of the articles and searched for the explicit mention of the term "privacy." The original search resulted in 1137 papers, but after employing the selection criteria below, the final data set comprised 59 research articles. Figure 1 presents an overview of the search process using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses)[2] flow chart, following Moher et al. (2009). The following selection criteria (or "reasons," as indicated in Figure 1) were applied. We included empirical, theoretical, and technical research studies that focus on privacy in LA published between 2011 and July 2021 (see Figure 1). These were our selection criteria:

3. Due to the emergent nature of privacy in LA, we included journal and conference papers, as well as book chapters.
4. Only peer-reviewed papers in English were included.
5. We included papers that used the term "privacy" in the title, and/or the abstract, and/or keywords.
6. Studies with explicit focus on ethics only (without mentioning "privacy") were excluded.
7. Editorial papers and review papers were also excluded.

The study uses only purely research-based publications and does not include implementation attempts in actual educational establishments rolling out LA as part of their services (e.g., codes of practice, consent forms, and ethical codes).

[1] https://www.kth.se/en/biblioteket/soka-vardera/primo-hjalp-1.863377
[2] https://www.prisma-statement.org//

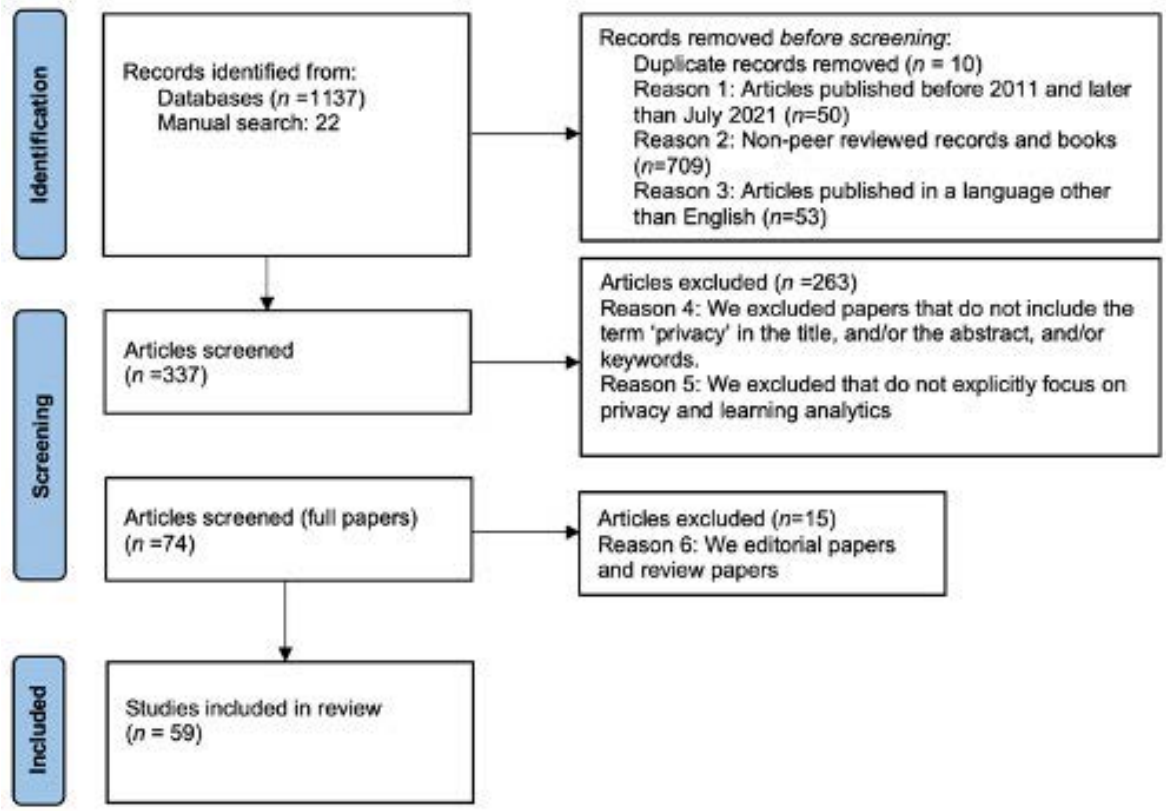

Figure 1. Flow chart depicting the search and selection process.

3.2. Data Analysis

All papers were examined to assess the research in terms of their definitions and conceptualizations of privacy. The first two authors coded the papers independently. To verify the coding, 15% of the reviewed articles were independently coded by both authors, which is in line with the recommended 10–25% (see e.g., O'Connor & Joffe, 2020). Considering the rather limited sample of papers (*N*=59) included in this review and the strong level of coding agreement, 15% was seen to be satisfactory. Cohen's kappa values were calculated at .89, which suggests a strong level of agreement (McHugh, 2012). When any discrepancy in the coding was encountered, we discussed the differences and recoded the papers until a consensus was achieved. Thereafter, the remaining dataset was split into two equally sized parts and coded by the two coders independently.

To analyze how the definitions of privacy in the LA context relate to the established approaches to conceptualize privacy, we first examined whether the privacy concept was defined or not. Papers in which we identified some related definition or conceptualization were analyzed using the categorization by Smith et al. (2011; Table 1) as a starting point. We added a category of "other definitions" for those that did not fit into the Smith et al. categorization, and "no definition" for the articles that addressed varying degrees of privacy without explicitly defining privacy. After categorizing the selected samples, we then looked for the key phrases (or variations of them) presented in Table 1. For example, Ifenthaler and Schumacher (2016) explained privacy as a legal definition in terms of stakeholder ability to control information (i.e., "control over data"), referring explicitly to Warren and Brandeis (1890), who defined privacy as freedom from interference or intrusion (Ifenthaler & Schumacher, 2016, p. 924). This is in line with Smith et al.'s understanding of privacy as *control.*

4. Results

4.1. Privacy Definitions in LA

Our analysis shows that a majority (74%; Figure 2) of the papers in our sample addressed privacy in the setting of LA without defining or conceptualizing it; 6% defined privacy as a *right*, 11% as a *state*, 15% as *control*, and 16% used other approaches to explain privacy. None of the reviewed articles defined privacy as a *commodity*.

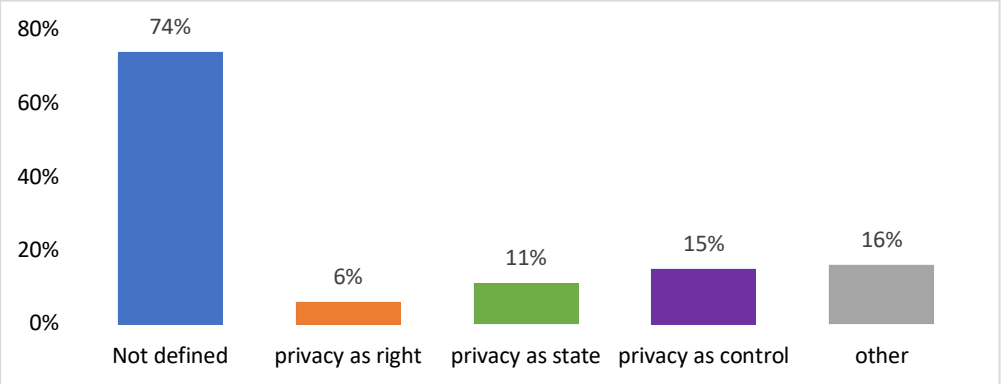

Figure 2. Privacy definitions in LA.*
**Percentages equal more than 100% since some articles included more than one definition.*

Among the papers that did not define privacy, 6% examine the challenges of LA implementation, where privacy was one of several considerations (Berg et al., 2016; Potgieter, 2020; Wang, 2016). Many of conceptual and theoretical studies (27%) propose related principles and frameworks and provide insights to guide and support practices of privacy protection but without explicitly unpacking the concept of privacy (e.g., Cormack, 2016; Hoel & Chen, 2018; Khalil & Ebner, 2016; Sclater, 2016).

Another portion (27%) are empirical papers that study student engagement in the LA design process and privacy-focused practices (e.g., Rosenberg & Staudt Willet, 2021; Silvola et al., 2021), student perceptions of privacy, stakeholder expectations and preferences concerning data collection practices in LA (e.g., Arnold & Sclater, 2017; Whitelock-Wainwright et al., 2020), and student propensity to consent to LA (e.g., Krieter et al., 2020; Rosenberg & Staudt Willet, 2021; Whitelock-Wainwright et al., 2020). In 13% of the articles, researchers offer technical tools to map data protection problems and solutions (e.g., Hoel & Chen, 2016), and recently, privacy-preserving tools (e.g., Amo et al., 2019; Amo et al., 2021).

4.2. How Do Definitions of Privacy in Learning Analytics Relate to Established Approaches?

The definition of ***privacy as a right*** was present in 6% of the reviewed papers (Figure 1; Appendix). Heath (2014) carried out a contemporary review of privacy theories to provide clearly articulated, comprehensive conceptualizations of privacy that can be considered in LA. The study pointed to "the rights of an individual to be left alone and free from intrusion and interference" (p. 141) as one of the earlier established conceptualizations of privacy. The understanding of privacy as right was also offered by Drachsler and Greller (2016) who presented the DELICATE checklist, a practical tool for establishing trusted LA within any data-driven educational organization. In their exploration of the critical ethical issues regarding the use of LA, Corrin et al. (2019) also referred to privacy as a right. They elucidated the distinction between ethics and privacy concepts and stressed that privacy refers to "the right to freedom from surveillance or unauthorized disclosure of one's personal information" and it is also "a legal principle and basic human right" (p. 10). Finally, Hoel and Chen (2019) explored the concept of information privacy in a cross-cultural setting to define a common point of reference for privacy engineering (i.e., privacy by design) in the context of LA, specifying that in the Western tradition, privacy is seen as "the right of an individual to be left alone" (p. 290).

The definition of ***privacy as control*** was present in 15% of the reviewed articles. Heath (2014), in her early overview of privacy theory contributions to LA, underlined that some LA studies define privacy as a concept that relates to the ability of individuals to control information about themselves. Ifenthaler and Schumacher (2016) explained privacy as a legal definition, i.e., privacy is understood as a person's right to control access to their own personal information. Other LA scholars (Corrin et al., 2019; Drachsler & Greller, 2016) argued that privacy involves self-determination in that individuals can determine their level of privacy or disclosure of personal information. Moreover, privacy has been identified as an ethical challenge of LA by Ferguson (2019) who explained it as "a freedom from unauthorized intrusion: the ability of an individual or a group to seclude themselves or the information about them, and thus to express themselves selectively" (p. 27).

While developing a set of ethical and privacy principles to aid LA designers and researchers in their work, Pardo and Siemens (2014) defined privacy in terms similar to the concept of opacity (i.e., the quality of lacking transparency or translucence). However, this vision evolved from the aspect of *control,* which refers to "the capability of individuals to influence the flow of their personal information" (p. 442). In another study examining student perceptions of privacy principles for LA, Ifenthaler and Schumacher (2016) provided a legal definition of privacy as "a person's right to control access to his or her personal information" (p. 924). Ifenthaler and Schumacher (2019) consider the same definition of privacy as a control in another study that investigated student intentions towards releasing personal information to inform LA systems.

Jones (2019) discussed issues related to student informed consent in relation to LA, and defined privacy as an "individual's right to determine for themselves when, how, and to what extent information about them is communicated to others" (p. 6). Based on this privacy-as-control approach, Jones (2019) further argued that privacy as control of personal information is autonomy promoting, and that students should be informed about these information flows and to what ends their institution is using them. Jones et al. (2021) recently offered a similar approach to privacy — information control, or controlling the information generated about themselves.

Privacy defined as ***a state*** was present in 11% of the articles (Figure 2; Appendix). In examining student expectations of privacy issues in LA, Tsai et al. (2020) defined privacy as "a state in which an individual is free from being disturbed or observed by others" (p. 231). Pardo and Siemens (2014) also emphasized that earlier descriptions of privacy embed the aspect limitations, which relates to the possibility of preventing others from accessing private data. Jones and VanScoy (2019) pointed out that there are different facets of the concept of privacy, and one of them is "limiting access to oneself" (p. 1334). Others explain that the earlier theories of privacy embed control and limitation, with limitations referring to the possibility of limiting access to personal information (Ifenthaler & Schumacher, 2016, 2019). Correspondingly, Hoel and Chen (2019) explored the concept of information privacy in a cross-cultural setting (Norway and China) to define a common point of reference for privacy in the context of LA. They underline that in the Chinese context, privacy is seen as a protection from access to personal information (Hoel & Chen, 2019, p. 291), compared to viewing privacy as *a right* as in the Western tradition.

4.3. Are There Other Approaches Specific to Learning Analytics to Define Privacy?

Of the reviewed papers, 16% provided other, still emerging conceptualizations of privacy. Some researchers (e.g., Gursoy et al., 2017; Hoel & Chen, 2015; Ifenthaler & Schumacher, 2016; Kyritsi et al., 2019) consider privacy under the umbrella of the *contextual integrity* framework (Nissenbaum, 2004), in which the understanding of privacy is associated with and regulated by the flow of information based on relative norms. These norms include context, actors, attributes, and transmission principles, affecting the flow of information from information senders to information receivers to information subjects. Some of the studies that include other definitions of privacy (e.g., Heath, 2014) emphasize that the concept of privacy as contextual integrity is harmonious to the context of LA. Drachsler and Greller (2016) also stated that "[a]nother important aspect of privacy especially in the age of Big Data is contextual integrity" (p. 92). It is essential to note that in the studies examined, contextual integrity is not proposed as a full definition of privacy (Drachsler & Greller, 2016), but rather as a framework for evaluating the flow of information between agents (individuals and other entities) with a particular emphasis on explaining why specific patterns of flow provoke public outcry in the name of privacy (Drachsler & Greller, 2016). Finally, Jones et al. (2021) underline the contextual dimension of privacy, among others (i.e., personal privacy, relational privacy, information access, intellectual privacy), and provide the following explanation: "[p]rivacy determines the flow of information (e.g., access, re-use, disclosure) about me [an individual] in a given context" (e.g., healthcare, education; p. 1533).

Privacy in the LA setting has also been recently explained in terms of *intellectual privacy* (e.g., Jones, 2019; Jones & VanScoy, 2019; Jones et al., 2021), grounded in Richards's (2015) conceptualization of *intellectual privacy* that stresses that our ideas and values keep pace with our technologies. Based on this understanding, Jones et al. (2021) define intellectual privacy as protection when one is doing intellectual activities such as searching for information, writing, and thinking. Aiming to understand how instructors discuss student data and information privacy, Jones and VanScoy (2019) argue that in education, privacy plays an important role in such processes as contemplation, idea generation, and speech acts expressing individual thoughts and beliefs. They further posit that "intellectual privacy provides the protections necessary to introspectively and socially engage in ideation; it provides a 'zone of protection' (Richards, 2015), that is, specific 'places and spaces (real and virtual) in which to read, to think, to explore' (p. 97), which enable individuals to develop 'new and possibly heretical ideas [...] before they are ready (p. 101) for public reception and scrutiny'" (Jones & VanScoy, 2019, p. 1134). *Intellectual privacy* is also associated with student autonomy, and is seen as a condition for it (e.g., Hoel & Chen, 2015; Jones, 2019). Overall, this type of privacy definition provides the protections necessary to engage in ideation introspectively and socially.

4.4. Conceptual Unclarity

Overall, our findings show a conceptual unclarity in how privacy and its related concepts (e.g., ethics, anonymization, informed consent, and security) are used in the LA setting. Some LA scholars also stress this issue explicitly. For example, to differentiate between ethics and privacy, Drachsler and Greller (2016) state that "privacy is an intrinsic part of a person's identity and integrity, whereas ethics is a moral code of norms and conventions that exists in society externally to a person" (p. 91). Thus privacy forms the boundary of one's person or identity against other entities. It implies that the understanding of privacy can diverge based on living conditions, family situation, culture, etc.

Our study also shows that the concepts of privacy and ethics have been used interchangeably or in overlapping ways in several articles. Privacy has sometimes been classified among other ethical issues, and this has been observed both in the papers that defined privacy and in those that did not. For example, Roberts et al. (2016) states that "the key ethical issues related to the use of big data and learning analytics are privacy, consent, and how data is used, stored, and protected and acted

upon" (p. 4). Other studies (Jones & Salo, 2018; Lawson et al., 2016; Slade & Prinsloo, 2013) correspondingly list privacy among the ethical issues that should be addressed in the LA domain. This observation is in line with several other scholars' concerns that ethics and privacy are often conflated in the literature on LA, while there are some important distinctions between the two terms (see e.g., Corrin et al., 2019; Drachsler & Greller, 2016; Ferguson, 2019). Corrin et al. (2019) state: "While ethics is a branch of philosophy that seeks to resolve moral questions around what is wrong and right, privacy relates to the right of freedom from surveillance and authorized disclosure of one's personal information" (p. 10). Pardo and Siemens (2014) also explicitly differentiate between the concepts of privacy and ethics, where "privacy is defined as the regulation of how personal digital information is being observed by the self or distributed to other observers" (p. 438). By personal digital information, we adopt a broad definition including the information about persons captured by any means and then encoded in digital format. They also explain ethics as "the systematization of correct and incorrect behaviour in virtual spaces according to all stakeholders" (Pardo & Siemens, 2014, p. 440).

We also observed some overlaps between privacy and security in some of the reviewed papers that proposed privacy or security preserving tools (Romansky & Noninska, 2017; Seanosky et al., 2016; Tobarra et al., 2021). Privacy has also been conflated with anonymity. For example, Gursoy et al. (2017) presented privacy-preserving methods for LA, which address privacy problems through data anonymization. They claim that the goal of anonymization is to transform a dataset to enforce a certain definition of privacy.

5. Discussion

Considering the critical importance of understanding and addressing privacy issues in LA, this study aimed at examining how privacy has been defined thus far by LA researchers. Our scoping review shows that in 74% of the examined papers, privacy is not defined at all. This is in line with Hoel (2020), who examined whether privacy was defined in the LAK conference proceedings of 2016–2018, which showed that privacy was mentioned in 33 papers, but defined only by Drachsler and Greller (2016). Our review shows some improvement since then, but most articles still lack definitions. It is not enough to come up with "student views," through which privacy has frequently been studied by LA researchers. Privacy is not up to anybody's views. It is one of the most critical success factors for technology use in education. In fact, it alone can stop any project or procurement. The EU's strongly enforced GDPR legislation, for example, has stopped further use of software and services from U.S. companies such as Google and Microsoft.[3] Any software developer must comply with that regulation. As for research, any study must obtain a positive decision from its institutional ethics board in every country involved. Hence, any R&D field concerned with software development must take this into consideration. Since privacy is not straightforward, it is not a simple checklist but concerns data handling in depth and detail to develop a thorough understanding.

Overall, the findings of the present study suggest that without this clear understanding and definition of what privacy is in a targeted study setting, the LA community is indeed challenged to design and enable a responsible approach to student data. "Responsibility" implies being response-able with the obligation to act (Prinsloo & Slade, 2018), which, among other things, includes the development and implementation of effective privacy-protecting mechanisms and practices. Heath (2014) has earlier stressed that the effective integration of existing privacy principles and frameworks in LA would be found in a valuable privacy theory/conceptualization. Yet, as shown by the results of this study — eight years later — this is still not the case, even though there are some emerging related attempts. Further, Heath pointed out that in the understanding and application of privacy theories in LA, it is also important to recognize the role of student engagement in determining privacy solutions. To engage students in this task, one could take advantage of participatory or user-centred design methods, originating in the field of human–computer interaction (as an example of such studies in the LA setting, see e.g., Ahn et al., 2021); in particular, the Scandinavian approach to design sees participatory design as a democratic process (Gregory, 2003). Participatory design includes stakeholders (i.e., students and teachers) in the early stages of the design process to adequately meet their needs. This is in accordance with the call for student-centred LA, which aims to put students — rather than researchers, instructors, or LA systems — "in the driver's seat with respect to the use of their own data [which will give] students a powerful tool and source of information to manage the increased self-regulatory demands of the current shift to digital" (Ochoa & Wise, 2021).

In educational settings where LA is to be used, much information flows between teachers and users. Teachers need information about students to teach and grade them, including not only study results but also work methods and personal factors that may make learning more or less difficult. For younger students, the information can be very personal since understanding and regulating social situations is part of the teacher's job. In a physical classroom, this information stays between the participants, but in LA applications, it may be used by other actors, such as school administrations, manufacturers of teaching and learning materials, and even governments. In the traditional classroom, there was a norm, a sort of social

[3] European Court ruling Schrems II.

agreement between teachers and students/parents that the information necessary for doing the teacher's job can be collected but not disseminated.[4] Contextual integrity was thus preserved.

LA systems create new contexts, hence a need for new social contracts. It is not likely that the social media model with an "accept" button will do because the information provided by students to teachers in the course of their everyday "normal" work may be much more sensitive. As well, many students are children under the custody of their parents, in the context of K–12 education. As with social media, information from LA systems may also reach third-party actors, not only for the purpose of improving systems and services, but also for advertising and market analysis. Clearly stakeholders external to the actual teaching and learning, such as software manufacturers and governments, may have different views of privacy protection than those immediately involved, but so will actors within the system — teachers, students, and parents.

This variety of stakeholders and potential data users means that LA systems span several social contexts. Preservation of contextual integrity (Gstrein & Beaulieu, 2022) is therefore a matter of concern, and requires understanding of what these social systems are and how information sensitive to privacy can be kept within a socially accepted context of exchange.

The results of this study also indicate that in 26% of the examined articles, LA researchers provided explicit definitions and conceptualizations of privacy. Some of these definitions could be categorized under the umbrella of already established definitional approaches, largely accepted in other fields, where privacy has been under examination for some time. The identified definitions vary between explaining student privacy in the setting of LA as *contro*l, as *a state*, as well as *a right* (Figure 2). Yet, the prevailing part of those studies (15%) defined privacy as *control*, which is in line with the findings of earlier research that investigated the definitional approaches to privacy in the information systems research area (Smith et al., 2011). It is interesting to note that while several definitions and lenses to information privacy were offered in the examined papers, it was often unclear how they were applied in research design and in analysis of the results of empirical studies. Some definitions of privacy could be categorized under more than one category (Drachsler & Greller, 2016; Ifenthaler & Schumacher, 2016; Pardo & Siemens, 2014). This illustrates not only the multidimensional nature of privacy in the context of LA, but also the potential complexity of effectively addressing it in educational practice.

The framework used for analysis in this article (see Table 1) is useful for distinguishing different views of privacy, but defining privacy in principle is not enough, there is also a need to discuss all the specific situations in which privacy must be "operationalized" by means of specifications of information content and flows and of whom should have access to what. Our study found such situations discussed in various articles as either 1) *intellectual privacy*, referring to intellectual freedom and property, or 2) *contextual privacy,* referring to the fact that LA systems (as information systems in general) often connect several social arenas.

They connect several stakeholders with different interests, uneven power relations, and different views of what privacy means — and by which social contracts it is regulated — in the particular social arena in which they operate. While the principal views of the Smith et al. model (2011) can adequately cover the discussion of the concept of privacy, the specific operationalization in different social systems — such as the various educational situations where LA is applied — must be designed based on a thorough understanding of the social contacts that stakeholders develop over time to be able to pursue their work in a way acceptable to them all. One benefit of the Smith et al. framework is that it allows for all such situation-specific discussions to rest on common ground regarding the definition of the basic concept of privacy.

6. Future Research

Our results also exhibit that some LA scholars define privacy in several ways that are distinct from the established definitional approaches. Examples include seeing privacy in terms of *contextual integrity* (e.g., Heath, 2014; Hoel & Chen, 2019) and referring to *intellectual privacy* (e.g., Jones et al., 2021) in the LA setting. Both approaches are still emerging and are not seen as the only ways to define privacy in the context of LA, but rather as important dimensions for LA communities of research and practice to carefully consider. As for the more established definitions mentioned above, we still know little about their application to LA research and practice. Consequently, we expect scholars to fill this gap in future studies. Moreover, future research should focus on a thorough examination of the privacy concept in relation to other interwoven concepts — such as ethics, anonymity, informed consent, and trust — and the contexts within which they have been examined in LA, including privacy practices, stakeholder attitudes and perceptions, and more. Also, considering the evolving nature of privacy and the fact that contexts may differ considerably across countries and cultures, LA scholars would benefit from the direct involvement of key stakeholders, not only in the process of LA design, but also in defining its main concepts, including privacy. For example, what privacy means for a learner in Scandinavian culture may differ from what it means in Chinese culture. This is in line with Hoel and Chen's (2019) way of approaching privacy in LA, and with related findings in other fields (e.g., Milberg et al., 2000). Yet, to elucidate relevant culturally aware understandings and definitions of privacy can be a challenging task. In

[4] It should be noted, however, that the details of that agreement may differ across countries.

this, LA scholars may take advantage of the established design methods in other areas (e.g., human–computer interaction) to improve the design of culturally aware and value-sensitive LA systems (see e.g., van Boeijen & Zijlstra, 2020; Friedman & Hendry, 2019).

7. Limitations

A recognized limitation to this scoping review is in using the search tool PRIMO, which may exclude some databases. Yet, the key databases were systematically searched. Another limitation relates to the fact that the LA field is interdisciplinary, which at times uses terminology in non-coherent and overlapping ways, especially regarding the responsible use of student data. Finally, because several other disciplines, such as educational data mining and human–computer interaction have also focused on privacy issues in the LA context, some relevant studies maybe have been overlooked in our sample. Again, this can be an area for further investigation.

8. Conclusions

In sum, the overall lack of privacy definition and conceptualization in LA can serve to further slow down the development of effective data-driven decision-making in educational settings for improved learning and teaching. To address this gap, LA scholars may start from the already existing understandings and definitions of privacy established in other fields (e.g., Margulis, 2003; Smith et al., 2011; Xu et al., 2011) and different legal and conceptual approaches to privacy protection in the broader context of datafication (Gstrein & Beaulieu, 2022). At the same time, the LA community should consider the contextual nature of privacy in LA (e.g., Hoel & Chen, 2019; Jones, Rubel et al., 2020; Jones et al., 2021). Contextual integrity has also been recently pointed out as one of the emerging conceptual approaches to privacy protection in a datafied society, along with differential privacy and group privacy (Gstrein & Beaulieu, 2022).

Furthermore, it is important to stress that what privacy means for different stakeholders (e.g., students, teachers, and educational institutions) may differ considerably across contexts, and this must be considered in the actual LA setups. Contexts will also differ across countries and cultures; to use a tool properly, and in a way that people can trust, users must first understand how handles data and, when necessary, adapt it by changing some setting or making use arrangements, for example.

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

Ahn, J., Campos, F., Nguyen, H., Hays, M., & Morrison, J. (2021). Co-designing for privacy, transparency, and trust in K–12 learning analytics. *Proceedings of the 11th International Conference on Learning Analytics and Knowledge* (LAK '21), 12–16 April 2021, Irvine, CA, USA (pp. 55–65). ACM Press. https://doi.org/10.1145/3448139.3448145

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Brooks/Cole Publishing.

Amo, D., Cea, S., Jimenez, N. M., Gómez, P., & Fonseca, D. (2021). A privacy-oriented local web learning analytics JavaScript library with a configurable schema to analyze any edtech log: Moodle's case study. *Sustainability, 13*(9). https://doi.org/10.3390/su13095085

Amo, D., Fonseca, D., Alier, M., García-Peñalvo, F. J., & Casañ, M. J. (2019). Personal data broker instead of blockchain for students' data privacy assurance. *Advances in Intelligent Systems and Computing, 932*, 371–380. https://doi.org/10.1007/978-3-030-16187-3_36

Arnold, K. E., & Sclater, N. (2017). Student perceptions of their privacy in leaning analytics applications. *Proceedings of the 7th International Conference on Learning Analytics and Knowledge* (LAK '17), 13–17 March 2017, Vancouver, BC, Canada (pp. 66–69). ACM Press. https://doi.org/10.1145/3027385.3027392

Bennett, C. J. (1995). *The political economy of privacy: Review of the literature.* Center for Social and Legal Research.

Berg, A. M., Mol, S. T., Kismihók, G., & Sclater, N. (2016). The role of a reference synthetic data generator within the field of learning analytics. *Journal of Learning Analytics, 3*(1), 107–128. https://doi.org/10.18608/jla.2016.31.7

Botnevik, S. (2021). Student perceptions of privacy in learning analytics: A quantitative study of Norwegian students. The University of Bergen. https://bora.uib.no/bora-xmlui/handle/11250/2757115

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://learning-analytics.info/index.php/JLA/article/view/7254

Cohen, J. E. (2001). Privacy, ideology, and technology: A response to Jeffrey Rosen. Georgetown Law Faculty Publications and Other Works, vol. 809. https://scholarship.law.georgetown.edu/facpub/809

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

Corrin, L., Kennedy, G., French, S., Shum, S. B., Kitto, K., Pardo, A., West, D., Mirriahi, N., & Colvin, C. (2019). The ethics of learning analytics in Australian higher education. Discussion Paper. https://melbourne-cshe.unimelb.edu.au/__data/assets/pdf_file/0004/3035047/LA_Ethics_Discussion_Paper.pdf

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

Drachsler, H., Hoel, T., Scheffel, M., Kismihók, G., Berg, A., Ferguson, R., Chen, W., Cooper, A., & Manderveld, J. (2015). Ethical and privacy issues in the application of learning analytics. *Proceedings of the 5th International Conference on Learning Analytics and Knowledge* (LAK '15), 16–20 March 2015, Poughkeepsie, NY, USA (pp. 390–391). ACM Press. https://doi.org/10.1145/2723576.2723642

Ferguson, R. (2019). Ethical challenges for learning analytics. *Journal of Learning Analytics, 6*(3), 25–30. https://doi.org/10.18608/jla.2019.63.5

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. https://doi.org/10.18608/jla.2016.31.2

Friedman, B., & Hendry, D. (2019). Value sensitive design: Shaping technology with moral imagination. MIT Press. https://doi.org/10.7551/mitpress/7585.001.0001

Gregory, J. (2003). Scandinavian approaches to participatory design. *International Journal of Engineering Education, 19*(1), 62–74.

Gstrein, S., & Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. *Philosophy and Technology, 35*(3). https://doi.org/10.1007/s13347-022-00497-4

Gursoy, M., Inan, A., Nergiz, M., & 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

Heath, J. (2014). Contemporary privacy theory contributions to learning analytics. *Journal of Learning Analytics, 1*(1), 140–149. https://doi.org/10.18608/jla.2014.11.8

Hoel, T. (2020). *Privacy for learning analytics in the age of big data: Exploring conditions for design of privacy solutions*. Doctoral Dissertation. University of Jyväskylä. https://jyx.jyu.fi/handle/123456789/69680

Hoel, T., & Chen, W. (2015). Privacy in learning analytics: Implications for system architecture. In T. Watanabe & K. Seta (Eds.), *Theory and Practice for Knowledge Management: Proceedings of the 11th International Conference on Knowledge Management* (ICKM 2015), 4–6 November, Osaka, Japan. https://www.semanticscholar.org/paper/Privacy-in-Learning-Analytics-%E2%80%93-Implications-for-Hoel-Chen/46f32e1193d2cbe4a2b049bfa40c28cd252160ef

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

Hoel, T., & Chen, W. (2018). Privacy and data protection in learning analytics should be motivated by an educational maxim: Towards a proposal. *Research and Practice in Technology Enhanced Learning, 13*(1). https://doi.org/10.1186/s41039-018-0086-8

Hoel, T., & Chen, W. (2019). Privacy engineering for learning analytics in a global market: Defining a point of reference. *International Journal of Information and Learning Technology, 36*(4), 288–298. https://doi.org/10.1108/IJILT-02-2019-0025

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

Ifenthaler, D., & Schumacher, C. (2019). Releasing personal information within learning analytics systems. In D. Sampson, J. M. Spector, D. Ifenthaler, P. Isaías, & S. Sergis (Eds.), *Learning technologies for transforming large-scale teaching, learning, and assessment* (pp. 3–18). Springer. https://doi.org/10.1007/978-3-030-15130-0_1

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 Educational Technology in Higher Education, 16*(24). https://doi.org/10.1186/s41239-019-0155-0

Joksimović, S., Marshall, R., Rakotoarivelo, T., Ladjal, D., Zhan, C., & Pardo, A. (2022). Privacy-driven learning analytics. In E. McKay (Ed.), *Manage your own learning analytics*. Smart Innovation, Systems and Technologies, vol. 261. Springer. https://doi.org/10.1007/978-3-030-86316-6_1

Jones, K. M. L., 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

Jones, K. M. L., Briney, K. A., Goben, A., Salo, D., Asher, A., & Michael, R. P. (2020). A comprehensive primer to library learning analytics practices, initiatives, and privacy issues. *College and Research Libraries, 80*(3). https://doi.org/10.5860/crl.81.3.570

Jones, K. M. L., Rubel, A., & LeClere, E. (2020). A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal of the Association for Information Science and Technology, 71*(10), 1227–1241. https://doi.org/10.1002/asi.24327

Jones, K. M. L., & Salo, D. (2018). Learning analytics and the academic library: Professional ethics commitments at a crossroads. *College and Research Libraries, 79*(3), 304–323. https://doi.org/10.5860/crl.79.3.304

Jones, K. M. L., & VanScoy, A. (2019). The syllabus as a student privacy document in an age of learning analytics. *Journal of Documentation, 75*(6), 1333–1355. https://doi.org/10.1108/JD-12-2018-0202

Jones, K. M. L., VanScoy, A., Bright, K., & Harding, A. (2021). Do they even care? Measuring instructor value of student privacy in the context of learning analytics. *Proceedings of the 54th Hawaii International Conference on System Sciences* (HICSS-54), 5–8 January 2021, Grand Wailea, Maui, HI, USA (pp. 1529–1537). IEEE Computer Society. https://doi.org/10.24251/hicss.2021.185

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

Kimmons, R. (2021). Safeguarding student privacy in an age of analytics. *Educational Technology Research and Development, 69*(1), 343–345. https://doi.org/10.1007/s11423-021-09950-1

Kitchin, R. (2021). Data lives: How data are made and shape our world. Bristol University Press.

Krieter, P., Viertel, M., & Breiter, A. (2020). We know what you did last semester: Learners' perspectives on screen recordings as a long-term data source for learning analytics. In C. Alario-Hoyos, M. J. Rodríguez-Triana, M. Scheffel, I. Arnedillo-Sánchez, & S. M. Dennerlein (Eds.), *Addressing global challenges and quality education* (pp. 187–199). Springer.

Kyritsi, K. H., Zorkadis, V., Stavropoulos, E. C., & Verykios, V. S. (2019). The pursuit of patterns in educational data mining as a threat to student privacy. *Journal of Interactive Media in Education, 2*(1), 1–10. https://doi.org/10.5334/jime.502

Laufer, R. S., & Wolfe, M. (1977). Privacy as a concept and a social issue: Multidimensional developmental theory. *Journal of Social Issues, 33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lawson, C., Beer, C., Rossi, D., Moore, T., & Fleming, J. (2016). Identification of "at risk" students using learning analytics: The ethical dilemmas of intervention strategies in a higher education institution. *Educational Technology Research and Development, 64*(5), 957–968. https://doi.org/10.1007/s11423-016-9459-0

Li, W., Sun, K., Schaub, F., & Brooks, C. (2021). Disparities in students' propensity to consent to learning analytics. *International Journal of Artificial Intelligence in Education*, 32, 564–608. https://doi.org/10.1007/s40593-021-00254-2

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues, 33*(3), 5–21. https://doi.org/10.1111/j.1540-4560.1977.tb01879.x

Margulis, S. T. (2003). Privacy as a social issue and behavioral concept. *Journal of Social Issues, 52*(2), 243–261. https://doi.org/10.1111/1540-4560.00063

McHugh, M. (2012). Interrater reliability: The kappa statistic. *Biochemia Medica, 22*(3), 276–282. https://pubmed.ncbi.nlm.nih.gov/23092060/

Milberg, S., Smith, J., & Burke, S. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*(1), 35–57. https://doi.org/10.1287/orsc.11.1.35.12567

Moher, D., Liberati, A., Tetzlaff, J., Altman, D. G., & PRISMA Group (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *PLoS Medicine, 6*(7), e1000097. https://doi.org/10.1371/journal.pmed.1000097

Munn, Z., Peters, M., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology, 18*, 143. https://doi.org/10.1186/s12874-018-0611-x

Mutimukwe, C., Twizeyimana, J. D., & Viberg, O. (2021). Students' information privacy concerns in learning analytics: Towards model development. *Proceedings of the Nordic Learning Analytics Summer Institute*, Stockholm. http://ceur-ws.org/Vol-2985/paper3.pdf

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*(1), 119–157.

Nissenbaum, H. (2019). Contextual integrity up and down the data food chain. *Theoretical Inquiries in Law, 20*(1), 221–256. https://doi.org/10.1515/til-2019-0008

O'Connor, C., & Joffe, H. (2020). Intercoder reliability in qualitative research: Debates and practical guidelines. *International Journal of Qualitative Methods, 19*, 1–13. https://doi.org/10.1177/1609406919899220

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

Panichas, G. E. (2014). An intrusion theory of privacy. *Res Publica, 20*, 145–161. Springer. https://doi.org/10.1007/s11158-014-9240-3

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

Pham, M., Rajic, A., Greig, J., Sargeant, J., & Papadopoulos, A. (2014). A scoping review of scoping reviews: Advancing the approach and enhancing the consistency. *Research Synthesis Methods, 5*(6), 371–385. https://doi.org/10.1002/jrsm.1123

Potgieter, I. (2020). Privacy concerns in educational data mining and learning analytics. *The International Review of Information Ethics, 28*, 1–6. https://doi.org/10.29173/irie384

Priedigkeit, M., Weich, A., & Schiering, I. (2021). Learning analytics and privacy: Respecting privacy in digital learning scenarios. In M. Friedewald, S. Schiffner, & S. Krenn (Eds.), *Privacy and identity management* (pp. 134–150). Springer. https://www.springerprofessional.de/en/learning-analytics-and-privacy-respecting-privacy-in-digital-lea/19025572

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

Prinsloo, P., & Slade, S. (2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics, 3*(1). https://doi.org/10.18608/jla.2016.31.10

Prinsloo, P., & Slade, S. (2018). Mapping responsible learning analytics: A critical proposal. In B. H. Khan, J. R. Corbeil, & M. E. Corbeil (Eds.), *Responsible analytics & data mining in education: Global perspectives on quality, support, and decision-making*. Routledge.

Prinsloo, P., Slade, S., & Khalil, M. (2022). The answer is (not only) technological: Considering student data privacy in learning analytics. *British Journal of Educational Technology, 53*(4), 876–893. https://doi.org/10.1111/bjet.13216

Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education, 16*(3), 263–279. https://doi.org/10.1177/1477878518805308

Richards, N. (2015). Intellectual privacy: Rethinking civil liberties in the digital age. Oxford University Press.

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*, 1–11. https://doi.org/10.3389/fpsyg.2016.01959

Romansky, R., & Noninska, I. (2017). An approach for investigation of secure access processes at a combined e-learning environment. *AIP Conference Proceedings* (Vol. 1910). AIP Publishing. https://doi.org/10.1063/1.5013995

Rosenberg, J. M., & Staudt Willet, K. B. (2021). Balancing privacy and open science in the context of COVID-19: A response to Ifenthaler & Schumacher (2016). *Educational Technology Research and Development, 69*(1), 347–351. https://doi.org/10.1007/s11423-020-09860-8

Schoeman, F. D. (1984). Philosophical dimensions of privacy: An anthology. Cambridge University Press.

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

Seanosky, J., Jacques, D., Kumar, V., & Kinshuk. (2016). Security and privacy in bigdata learning analytics. In V. Vijayakumar & V. Neelanarayanan (Eds.), *Proceedings of the 3rd International Symposium on Big Data and Cloud Computing Challenges* (ISBCC '16) (pp. 43–55). Springer.

Silvola, A., Näykki, P., Kaveri, A., & Muukkonen, H. (2021). Expectations for supporting student engagement with learning analytics: An academic path perspective. *Computers & Education, 168*, 104192. https://doi.org/10.1016/j.compedu.2021.104192

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

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

Solove, D. J. (2006). Taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

Tobarra, L., Utrilla, A., Robles-Gómez, A., Pastor-Vargas, R., & Hernández, R. (2021). A cloud game-based educative platform architecture: The Cyberscratch project. *Applied Sciences, 11*(2). https://doi.org/10.3390/app11020807

Tsai, Y., Whitelock-Wainwright, A., & Gašević, D. (2020). The privacy paradox and its implications for learning analytics. *Proceedings of the 10th International Conference on Learning Analytics and Knowledge* (LAK '20), 23–27 March 2020, Frankfurt, Germany (pp. 230–239). ACM Press. https://doi.org/10.1145/3375462.3375536

van Boeijen, A., & Zijlstra, Y. (2020). *Culture sensitive design: A guide to culture in practice*. BIS Publishers. https://www.bispublishers.com/culture-sensitive-design.html

Wang, Y. (2016). Big opportunities and big concerns of big data in education. *TechTrends, 60*(4), 381–384. https://doi.org/10.1007/s11528-016-0072-1

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

Weinstein, W. L. (1971). The private and the free: A conceptual inquiry. In J. R. Pennock & J. Chapman (Eds.) *Privacy, Nomos XIII: Yearbook of the American Society for Political and Legal Philosophy*. Atherton Press.

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

Whitelock-Wainwright, A., Gašević, D., Tsai, Y.-S., Drachsler, H., Scheffel, M., Munoz-Merino, P., Tammets, K., & Kloos, C. (2020). Assessing the validity of a learning analytics expectation instrument: A multinational study. *Journal of Computer Assisted Learning, 26*(2), 209–240. https://doi.org/10.1111/jcal.12401

Wright, D., & Raab, C. (2014). Privacy principles, risks and harms. *International Review of Law, Computers & Technology, 28*(3), 277–298. https://doi.org/10.1080/13600869.2014.913874

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems, 12*(12), 798–824. https://doi.org/10.17705/1jais.00281

Appendix 1: Mapping of the Privacy Definitions in LA.

The list of articles included in this review can be found at: https://docs.google.com/document/d/1LzzLRcdR2t_f-Bk-AMwTehLShBL7wHTU2ei--VyCMBc/edit?usp=sharing

No	Authors	No definition	Privacy as a right	Privacy as a commodity	Privacy as a state	Privacy as control	Other definitions
1	Ahn et al. (2021)	X					
2	Amo et al. (2019)	X					
3	Amo et al. (2021)	X					
4	Arnold & Sclater (2017)	X					
5	Berg et al. (2016)						
6	Brown & Klein (2020)	X					
7	Chaurasia & Rosin (2017)	X					
8	Cormack (2016)	X					
9	Corrin (2021)	X					
10	Corrin et al. (2019)		X			X	
11	Drachsler & Greller (2016)		X			X	X
12	Dyckhoff et al. (2012)	X					
13	Ferguson (2019)					X	
14	Greller and Drachsler (2012)	X					
15	Gursoy et al. (2017)						X
16	Heath (2014)		X			X	X
17	Hoel & Chen (2015)						X
18	Hoel & Chen (2016)	X					
19	Hoel et al. (2017)	X					
20	Hoel & Chen (2018)	X					
21	Hoel & Chen (2019)		X		X		
22	Ifenthaler & Schumacher (2016)				X	X	X
23	Ifenthaler & Schumacher (2019)				X		
24	Jones (2019)					X	X
25	Jones & Salo (2018)	X					
26	Jones & Vanscoy (2019)				X		X
27	Jones, Asher et al. (2020)	X					
28	Jones, Rubel et al. (2020)					X	X
29	Jones et al. (2021)					X	X
30	Khalil & Ebner (2016)	X					
31	Krieter et al. (2020)	X					
32	Kyritsi et al. (2019)						X
33	Lawson et al. (2016)	X					
34	Li et al. (2021)	X					
35	Pardo & Siemens (2014)				X	X	
36	Potgieter (2020)	X					
37	Praharaj et al. (2018)	X					
38	Preuveneers et al. (2021)	X					
39	Prinsloo & Slade (2015)	X					

No	Authors	No definition	Privacy as a right	Privacy as a commodity	Privacy as a state	Privacy as control	Other definitions
40	Prinsloo & Slade (2016)	X					
41	Reidenberg & Schaub (2018)	X					
42	Roberts et al. (2016)	X					
43	Rodríguez-Triana et al. (2016)	X					
44	Romansky & Noninska (2017)	X					
45	Rosenberg & Staudt Willet (2021)	X					
46	Rubel & Jones (2016)	X					
47	Sclater (2016)	X					
48	Seanosky et al. (2016)	X					
49	Silvola et al. (2021)	X					
50	Slade & Prinsloo (2013)	X					
51	Slade et al. (2019)	X					
52	Steiner et al. (2016)	X					
53	Tobarra et al. (2021)	X					
54	Tsai et al. (2020)				X		
55	Viswanathan & VanLehn (2019)	X					
56	Wang (2016)	X					
57	Whitelock-Wainwright et al. (2019)	X					
58	Whitelock-Wainwright et al. (2020)	X					
59	Whitelock-Wainwright et al. (2021)	X					