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.
https://doi.org/10.1108/IJILT-02-2019-0025

Privacy engineering for learning analytics in a global market – defining a point of reference

Tore Hoel
Oslo Metropolitan University, Oslo, Norway, and
Weiqin Chen
Oslo Metropolitan University, Oslo, Norway and SLATE, University of Bergen, Bergen, Norway

Abstract:

Purpose – Privacy is a culturally universal process; however, in the era of Big Data privacy is handled very differently in different parts of the world. This is a challenge when designing tools and approaches for the use of educational Big Data and learning analytics in a global market. The purpose of this paper is to explore the concept of information privacy in a cross-cultural setting to define a common point of reference for privacy engineering.

Design / Methodology / Approach – The paper follows a conceptual exploration approach. Conceptual work on privacy in educational big data and learning analytics in China and the West is contrasted with the general discussion of privacy in a large corpus of literature and recent research. As much of the discourse on privacy has an American or European bias, intimate knowledge of Chinese education is used to test the concept of privacy and to drive exploration of how information privacy is perceived in different cultural and educational settings.

Findings – The findings indicate that there are problems using privacy concepts found in European and North-American theories to inform privacy engineering for a cross-cultural market in the era of Big Data. Theories based on individualism and ideas of control of private information do not capture current global digital practice. The paper discusses how a contextual and culture-aware understanding of privacy could be developed to inform privacy engineering without letting go of universally shared values. The paper concludes with questions that need further research to fully understand information privacy in education.

Originality / value – As far as we know, this paper is the first attempt to discuss—from a comparative and cross-cultural perspective—information privacy in an educational context in the era of Big Data. The paper presents initial explorations of a problem that needs urgent attention if good intentions of privacy supportive educational technologies are to be turned

into more than political slogans.

Keywords: – Information privacy, Educational Big Data, Learning analytics, Cross-cultural studies, Privacy engineering

1 Introduction

The starting point of this work is a box labeled 'privacy rules' found in a Chinese blueprint for a learning analytics technical architecture. We asked ourselves: What rules? What privacy? What should engineers build? And we banged our heads against the black box, not being able to unpack the concept of privacy rules, being *lost in translation* (did we talk about the same thing?). We were unable to gain any insight into the different contexts within which the need was ascribed, nor any of the practical requirements that could be construed from that need. In this conceptual paper we aim at defining a point of reference for understanding privacy in the context of educational big data[1] (EBD) or learning analytics (LA). We will use our experience working in China as a way to drive and test the exploration of the concept of information privacy with the ultimate aim to enable privacy engineering for global education.

Privacy is recognised as a challenge dealing with Big Data (Polonetsky and Tene, 2013). For some countries in the West privacy has been seen as a show-stopper for learning analytics (Griffiths et al., 2016). It is well known that the discourse on privacy is more central in Europe than in China, especially with the introduction of GDPR (Bennett, 2018). However, when looking more closely at what is happening in real life in terms of collecting and sharing traces of online activity the differences between China and Western countries tend to diminish. Enormous amounts of data are collected and shared all over the globe. What may be different is who collects data, and who has right to access the data (e.g., government or private companies); and what is the ascribed use (surveillance or profit, or both). If this is the case, two questions arise—one related to technology, and one to education: Is privacy in terms of individual control over personal information possible in the era of Big Data? Is students' information privacy too dependent upon culture and political system to be able to define a universal point of reference for EBD or LA?

Why are these questions important? First, it may not be possible to create practical implementations of a particular definition of privacy. If this is the case, then a strong emphasis on privacy in the design and adoption of LA solutions may be reduced to ideological or political markers which signal the virtue of policy maker, but with limited value in terms of actionable requirements for engineering. Second, if students react

[1] Educational Big Data is the term used in China for learning analytics, connecting the analytics more to Big Data and "Internet Plus" political narratives.

negatively to the infringement of norms related to collection and sharing of data exhaust from their learning behaviour, then this will have importance for the design and deployment of data-driven tools and practices in a global market. What do these considerations imply for the 'privacy rules' box in the Chinese blueprint? If the box in the drawing is just a political nod to an international audience, then in terms of practical system design point it has little relevance (although it may be necessary to understand this obfuscation in order to understand the way in which the designed system works in its social context). If, on the other hand, 'privacy' addresses real concerns that affect usage behaviour we need to define the term in a way that allows us to be specific about requirements and 'rules' whatever market we operate in.

This paper presents a conceptual exploration of how the concept of privacy can give rise to design requirements in the context of global EBD and LA. An underlying assumption is that the discourse on privacy till now (Slade et al., 2019; Ifenthaler and Schumacher, 2016; Rubel and Jones, 2016; Drachsler and Greller, 2016; Young, 2015) has not succeeded in providing *implementable* requirements for tools and practices in an international market with different political systems, cultures, and pedagogical approaches.

There is a need to discuss the concept of privacy in a cross-cultural context, and to see if Big Data changes the way we understand the concept of 'information privacy'. The rest of the paper is organised as follows: First we review the literature on information privacy to see how definitions hold up in cross-cultural settings and in defining design requirements. Then we examine how Big Data and cultural differences influence the concept of privacy. In Section 4 we use our findings so far to discuss what privacy engineering will imply in an educational context, legally, conceptually, and technically. The paper concludes with a proposal for a research agenda to develop a point of reference for privacy engineering for EBD and LA in a global market.

2 Information privacy as design requirement – conceptual exploration

In other work we have explored how privacy is conceptualised by the less than a decade young field of Learning Analytics and Knowledge research, which organise yearly conferences and sponsor the Journal of Learning Analytics (Hoel and Chen , 2018, 2016, 2015; Hoel et al., 2017). This body of literature is contrasted with the general discussion of 'privacy' in the huge corpus of research on this issue that goes back more than a century (Warren and Brandeis, 1890). To add the cross-cultural dimension to our exploration we have reviewed literature on 'privacy' and 'China' and other cultural and geographical

markers. However, the literature review for this conceptual paper is not done to provide a representative description of privacy as a concept, but to offer ideas and highlight direction for future inquiry as the focus of a conceptual paper is "on integration and proposing new relationships among constructs" (Gilson and Goldberg, 2015). In this paper we have used intimate knowledge about the Chinese educational system acquired through participant observation to drive and test how the privacy constructs hold up for use in global settings.

Smith, Dinev, and Xu (2011) note that "the recent evolution of the concept of privacy in general—and information privacy in particular—follows the evolution of information technology itself" (p. 990). Westin (2003) identified different eras of privacy development, the last from 1990 to 2002 influenced by the rise of the Internet, Web 2.0, the terrorist attach of 9/11/2001, and the dramatical changed landscape of information exchange. It is a matter of discussion if Big Data represents a distinct new era; however, the point here is to observe the dynamic nature of the concept of information privacy, and how any use of the concept requires a deep understanding of the technological context of information handling. It is widely accepted that, as a concept, privacy is in disarray (Solove, 2002; Smith et al., 2011). "The distinction between physical and information privacy is seldom clarified in public debate or, for that matter, in many areas of research" (Smith et al, 2011, p. 991). Solove observed that "widespread discontent over conceptualizing privacy persists even though the concern over privacy has escalated into an essential issue for freedom and democracy" (Solove, 2002, p. 1089). In analysing a big corpus of privacy articles and books Smith et al. (2011) concluded that a richer focus on international dimensions of privacy research is needed. In this paper, we want to address this international dimension by loosening the grip of value-based—some would say, Western liberal (Bennett, 2018)— discourse on privacy. Instead, we will narrow the perspective to engineering requirements, and what Smith et al. (2011, p. 993) call cognate-based conceptualization of privacy – "related to the individuals mind, perceptions and cognition rather than to an absolute moral value or norm".

Our ambition is to unpack the concept of information privacy to allow engineers serving a global market to make more specific statements about privacy and technology. This is not a new idea. Palen and Dourish (2003) wanted to do so for human-computer interaction (HCI) analyses, offering a framework and vocabulary to foster discussion between technology users, designers and analysts. Their framework suggested analysis of three boundaries, – disclosure, identity, and temporality. Spiekermann and Cranor (2009) introduced a privacy responsibility framework consisting of three spheres: user (the individual and her devices). recipient (company). and joint sphere (where the control is shared). These spheres were related to system operations (data transfer, storage, and processing). They described two approaches to engineering, "privacy-by-policy" (focusing on implementation of the notice and choice principles). and "privacy-by-architecture" (minimizing collection of identifiable

personal data and emphasizing anonymization and client-side data storage and processing).

The degree to which these two approaches hold up in the era of Big Data will be discussed in the next section. Both groups of authors build on Altman's influential privacy theory (Altman, 1975). which states that privacy is neither static nor rule-based, stressing the dialectic and dynamic process of selectively controlling the access to the self. How does this value of 'controlling access to the self' stand the *Chinese test;* is this a universal value that should underpin all design?

To get an understanding of how Chinese users look at the role of the self in information privacy we need to look at great many factors of history, culture, economy, policy, and law related to the higher level concept of general privacy. First, we have to acknowledge that most privacy studies "are based in the United States and are written in English, leading to language-based assumptions about privacy terminology" (McDougall, 2004, p. 1). In the Western tradition, Li et al. (2017) point out, the concept of privacy is said to arise out of an 1890 article by Samuel Warren and Louis Brandeis where privacy is described a right to privacy as the right of an individual to be left alone. In Chinese, privacy (yinsi) is an imported word, consisting of two words (yin – 'hidden from view'; and si – 'private' or 'do not want to disclose in public'). Yinsi has not necessarily positive connotations; a more narrow interpretation of yinsi is 'shameful secret'. Li et al. (2017) claim that Chinese privacy laws can be understood through the lens of 'saving face'. China does not have a separate privacy law, but privacy is acknowledged by the courts as a value worth protecting, and there are a number of laws that could be used to that end (e.g., tort legislation). Looking at what is protected, China differs from the West. The legal system has often sided with protecting the rights, values, and morals of the community over protecting the privacy rights of the individual; "privacy law and regulation in Chinese culture supports the individual's role in the community rather than protecting the individual against the community as in the West" (Li et al., 2017, p. 12).

From a Western point of view, the Chinese government's massive surveillance and intrusion into personal information (Wang and Yu, 2015) may seem over the top if the aim is to support the individual's role in society. However, one cannot a priori assume that there is a conflict between the individual and the government in these matters. From a privacy point of view, if the system protects against the citizen's right of reputation, the government intrusion on the private sphere might be seen as both in the interest of the public and the citizen.

In a society where the concept of 'self' is tied more to the family this will influence how privacy is viewed. According to McDougall (2004). privacy in traditional China resides

primarily in the family unit, which is distinct from the public sphere. Seen through the lens of 'saving face' the Chinese privacy laws can be seen as a protection from exposing personal information. This perspective is still compatible with Altman's definition of privacy as a "dynamic process of selectively controlling the access to the self" (Altman, 1975). The individualistic perspective so prevalent in American privacy research (Marwick and boyd, 2014). is softened by Altman's further development of his theory in relationship to culture. His framework emphasizes the dialectic and boundary control features of privacy, "whereby people can make themselves accessible or inaccessible to others" (Altman, 1977, p. 82). Privacy is a culturally universal process, but it is also highly culturally specific and contextual (Altman, 1975, 1977; Palen and Dourish, 2003). In a Chinese context, Altman's pre-Internet definition of privacy could need updating to "… accessible or inaccessible to *some significant* others". The individual could hope to control accessibility within certain contexts that are important for their self-esteem; however, absolute control in today's Internet society is an illusion. Some would claim this is also the case in a Western context after Edward Snowdon's disclosure of contemporary surveillance (Page, 2016).

The idea of selective control gives priority to context. The most recognized contextual privacy theory is developed by Nissenbaum (2010) revolved around the concept of 'contextual integrity'. The norms that govern "the flow of personal information in a given context" (Nissenbaum, 2010, p. 127) are dependent on the type of information being shared; the social roles of the sender, subject, and recipient; and how information is transmitted. Nissenbaum's theory holds up to our *China test*, as it gives room for social norms that are rooted in Chinese culture and political context.

In the next section we will explore the individual's room for manoeuvre in the era of Big Data; what our discussion so far shows is that the contextual aspects of privacy needs a better understanding.

3 Big data and privacy

In the era of Big Data, the challenges of privacy become more visible—on conceptual, technical, legal, and political levels. The privacy challenges need to be addressed on all these levels, which have implications for how we approach privacy engineering. In order to turn information privacy into actionable design requirements for engineering we need to leave an idealised world of absolutes and see how higher level values, laws, technologies, and users' practices interact in a globalised setting. Grounding privacy protection policies within the individualistic and liberal notion of 'privacy' may, according to Bennett (2018) overlook what is at stake in the broader debate over contemporary surveillance.

> Thus, data protection law does not halt surveillance; it manages it. It may produce a fairer and more efficient use and management of personal data, but it cannot effectively control the voracious and inherent appetite of modern organizations for more and more increasingly refined personal information, especially when those data are central to the business models of the platform economy (Bennett, 2018).

When jaywalking has the immediate effect of exposing name and picture of the culprit on a gigantic public screen (Niu, 2017) a Chinese citizen will have no illusions of privacy being protected by the laws. Before European citizens feel overly protected by the new General Data Protection Regulation (GDPR) they should take a second to ponder the implications of the full title of the regulation: "Regulation of the European parliament and of the Council on the protection of individuals with regard to the processing of personal data and *on the free movement of such data*" (European Commission, 2012). Bennett (2018, p. 244) observes that "contemporary information privacy legislation is designed to manage the processing of personal data, rather than to limit it".

What if the individual does not want privacy? Users information technology in the networked society may have other priorities than the older generation. Marwick and boyd (2014) looked at how teenagers negotiate context in social media and found, "simply put, they are trying to be in public without always being public" (Ibid., p. 1052). This complies with the Chinese laws that "protect Chinese citizens from having their personal information exposed, thus allowing individuals to present their identity (or personal information) to the community in ways that they choose" (Li et al., 2017, p. 2). Young people see value in being online; however, they also "have a sense that data are reused and repurposed in myriad ways" (Pangrazio and Selwyn, 2018, p. 7). In experiments, Pangrazio and Selwyn (Ibid.) worked with young mobile media users to move them towards a practice of 'informed resistance' towards privacy threats. They found that their participants remained unenthusiastic about the 'agentic' choices that they were attempting to support them in making.

> [M]anaging personal data also requires advanced technical skills and ongoing maintenance. The question then becomes *should* it be up to the individual to ensure their data privacy? Self-responsibilization might be beyond the individual, suggesting that more collective and centralized approaches to data privacy are the only realistic way forward. (Pangrazio, and Selwyn, 2018, p. 8)

Neither technical skills nor technical solutions are going to solve information privacy. Young (2015) observes that the notion of anonymity as a "placeholder for privacy" (Ibid., p. 560) is becoming increasingly questionable, such that existing consent to the collection, analysis and use of personal data is "effectively illusory" (Ibid., p. 561). She found "there is also no empirical evidence that suggests that "de-identification works either in theory or practice" (Ibid., p. 561).

Rubinstein (2013, p. 1) argues that GDPR relies too heavily on an informed choice model and data minimization, "and therefore fails to fully engage with the impeding Big Data tsunami". Data minimization and anonymization were pivotal engineering instruments in the Spiekermann and Cranor approach that we introduced in the previous section (Spiekermann and Cranor, 2009). If these measures are not working in the era of Big Data, what are the alternatives to promote privacy? The discourse framework suggested by Palen and Dourisch (2003) for HCI could only be part of a solution. Rubenstein's proposal is to combine legal reform with encouragement of new business models premised on consumer empowerment and supported by a personal data ecosystem.

Our understanding of information privacy is not set in stone. The rest of the paper will explore possible developments from a legal, conceptual, and technical point of view.

4 Envisioned privacy developments – in an educational context

When de-identification of personal information is an illusion and the 'big data tsunami' makes us run to save face we could, as well, give up the idea of information privacy? Or in the words of Sun Microsystems' CEO, Scott McNealy, "You have zero privacy anyway. Get over it!" (Sprenger, 1999). However, this is not the adequate response to handling risks in society (Rauhofer, 2008). This was shown in debate spurred by Paul Ohm's 2009 article "Broken Promises of Privacy: Responding to the surprising failure of anonymization". Even if the danger of re-identification is immanent with Big Data, 'good enough' approaches work (Ohm, 2009; Narayanan and Felten, 2014; Cavoukian and Castro, 2014). Real life is more than worst cases.

In this paper we are concerned with privacy engineering, defined by Kenny and Borking (2002) as "a systematic effort to embed privacy relevant legal primitives into technical and governance design". In the following, we will discuss how we foresee this being done in an educational context with both Chinese and Western students in mind.

4.1 Legal development

What legal primitives are relevant to education in a global setting? First, international privacy legislation is dynamic, with GDPR just being implemented in Europe with ramifications for the understanding of privacy also in other parts of the world trading with Europe (Bennett, 2018; Hoel and Chen, 2018). This means that ideas of the individual's role

in managing personal information, data minimization, etc are recognised (even if they are not part of national legislation). and that they may influence policy development around the globe, e.g., institutional codes of ethics. This consensus around principles of a code of practice, information collection, information processing and information dissemination is demonstrated in international standardization developing requirements for privacy and data protection for learning analytics (ISO 20748-4:2019). Second, laws are interpreted, and this leaves space for privacy engineering that addresses sector or culturally specific interests. We have argued (Hoel and Chen, 2018) that privacy in an educational context should be led by pedagogical principles. This means that student agency should be strengthened by negotiating data sharing with each student; supporting openness and transparency, and promoting personal data literacies. This proposal takes the 'privacy-by-policy' approach (see Section 2, Spiekermann and Cranor, 2009) one step further and contextualize the Fair Information Principles of the OECD and APEC frameworks (Hoel and Chen, 2018) for education. There is no doubt that also in Chinese education for the 21st century values like transparency, notice, student agency, have priority (Stanaland and Lwin, 2013) and could be integrated into a digital literacy curriculum.

In choosing what legal primitives should inform engineering there is still a need for conceptual work, which principles will be discussed in the next section.

4.2 Conceptual development

The cultural diversity of a global market requires systems that are capable of runtime cultural adaptation. That means technologies must be 'cultural aware', which in turn means that we need to formalise our understanding of culture (as well as law, social norms, and pedagogy) in a model that can be implemented in systems that can handle different contexts.

In HCI, the concept of context and how it relates to culture has been discussed for years (Dourish, 2001). Context is a notoriously fuzzy concept having an infinite dimension that does not allow it to be described completely. Blanchard et al. (2011) launched the concept of 'centred context', "seen as a limited context, whose focus is on the description of specific, more or less complex, dimensions (for instance the spatial one, the social one, the cultural one, and so on"(Ibid., p. 13). This concept allows a modelling of dimensions that could be useful for adaptive systems. Blanchard et al. (2011) have proposed to structure the cultural domain with an upper ontology and discuss methods to do so.

We suggest that the ontology engineering approach of Blanchard et al. (2011) could be used to create an upper ontology of the concept of privacy as well. Culture-aware learning

technologies using EBD and LA would need a number of upper ontologies describing culture, privacy, pedagogy, emotions (affective domain). etc. In such an ontology key concepts in European legislation, like purpose limitation and data minimization, would need to be defined in a way that allows design of adaptive technologies that also work in a Chinese context.

In EBD and LA, it is no surprise that technology itself plays an important role in what ways privacy is constrained. This is the topic of the next section of this paper.

4.3 Technical development

In Rubinstein's proposal for an international solution to the big data privacy problem he included a personal data ecosystem (Rubinstein, 2013). Rubinstein left to others to specify what such a system involves, and there is no lack of proposals being debated as the consequences of Big Data start to be understood. Even if we have pointed to the pedagogical opportunity of strengthening learner agency and personal digital literacy we do not think the privacy challenges could only be met with measures taken by the individual. Privacy needs to be built into the technology, much according the principles of Privacy-by-Design promoted by GDPR (Cavoukian, 2012).

This challenge is taken on board by Tim Berners Lee, who as we all know played an important role in inventing the most used Internet technology, the World Wide Web. He is now involved in building a technology that "changes the current model where users have to hand over personal data to digital giants in exchange for perceived value" (Berners-Lee, 2018). Berners-Lee's ambition is to challenge what Shoshana Zuboff has termed 'surveillance capitalism' (Zuboff, 2019). evolving the web in order to restore balance—by giving every one of us complete control over data, personal or not. Berners-Lee wants to build an Internet protocol that enables users to decouple content from the application itself, giving the users freedom to choose where their data resides. Seamless switching between apps and personal data storage servers will avoid vendor lock-in and secure innovation, while giving the user control of their data. It is in the same vein other researchers are exploring how blockchain technologies can be used in education to allow students to exercise control of their own learning records (Grech and Camilleri, 2017; Ocheja et al., 2019).

Tools for EBD and LA are just starting to hit the market, and privacy aspects are still open for design. This is therefore the right time to make sure that technical design of EBD and LA solutions are based on a sound understanding of information privacy in a global setting.

5 Conclusions – towards a research agenda

A 'black box' labelled 'privacy rules' introduced this paper. With China and a Western country like Norway in mind, we know that rules regulating students' daily life are very different. In China, "dorms' face recognition gets thumbs-up for convenience" (Ma and Lin, 2018); while in Norway, student id app users are assured that "the data is stored locally on your device and you may delete them whenever you want" (Felles studentsystem, 2018). Even if the output of privacy rules differs enormously between the two countries this paper supports the idea that it is worthwhile to specify input for privacy engineering that allows design of solutions that could be implemented both in China and Norway.

Through comparative analysis and reflection, we have found that there are limitations in European and North-American privacy theories when the aim is to inform privacy engineering for a global market of analytics tools and services. This finding also implies that the discourse we have had till now on privacy in the context of EDB and LA research has limitations. Too much focus has been on discussing values and norms, and too little effort has been on getting knowledge about students' perceptions and cognition of privacy in the actual settings where EDB and LA systems are used. This is also a limitation of this study, which only explore concepts and do not generate empirical findings. However, before we can engage in empirical studies, we need to have our theoretical constructs right.

This paper rejects that privacy is something that only can be found in liberal societies based on individualistic culture. As Altman concluded

> (a) people in all cultures engage in the regulation of social interaction—sometimes being accessible to others and sometimes being inaccessible to others, and (b) the behavioral mechanisms by which accessibility is controlled are probably unique to the particular physical, psychological, and social circumstances of a culture. (Altman, 1977, p. 82)

Altman's observations hold also in a digital age. However, in the era of Big Data it is not enough to analyse relationships among friends and family members; we need analysis of cross-cultural networked practices in the shadow of what Zuboff has termed the 'Big Other". Zuboff (2015, p. 81) describes the Big Other as "a ubiquitous networked institutional regime that records, modifies, and commodifies everyday experience from toasters to bodies, communication to thought, all with a view to establishing new pathways to monetization and profit".

If we find that what Zuboff describes is more than a shadow, that surveillance capitalism is a social formation of global reach, this will also impact the agenda for student privacy. Notwithstanding East or West, the challenge will be to design tools for education that promote knowledge about the use of data and the students' own relation to its use. In order

to know more about what input to be fed into the *privacy rule box* future cross-cultural research should focus on

A) Aspects of contextual integrity: What types of learning activity data are collected and shared? What norms govern the flow of personal data in education? What roles do students, teachers, technologies, and other actors play?

B) Aspects of culture and policies that constrain educational priorities: What role does student agency play in education? And what educational priorities could influence design of learning tools?

C) Aspects of technological development: What technologies could strengthen the students' ability to negotiate boundaries related to data sharing?

Finally, our cross-cultural perspective on privacy engineering has made us aware of the need to discuss the relationship between EDB and LA, the two concepts we have used to capture both Chinese and Western discourse on these issues. EBD comes with a notion of Big Data, and nowadays, more and more ideas of the use of Artificial Intelligence (AI). The discourse on LA on the other hand, seems to have a narrower scope in line with the much used definition[2] coined by the Society for Learning Analytics Research (SoLAR) (Siemens, and Gasevic, 2012). The SoLAR definition does by no means exclude use of AI, however, LA could be more focussed on "understanding and optimising" specific learning tasks that could be described by use of 'small data'. A more limited and targeted use of analytics related to pedagogically well-defined *learning moments* may imply less challenging privacy issues than Big Data approaches, where data collection tends to come first and pedagogical reasoning second.

Reference List

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

Altman, I. (1977), "Privacy Regulation: Culturally Universal or Culturally Specific?" *Journal of Social Issues*, 33(3), 1–19.

Bennett, C. J. (2018), "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?" *Information Polity*, 23(2), 239–246. http://doi.org/10.3233/IP-180002

Berners-Lee, T. (Sep 29, 2018), "One Small Step for the Web…", available at: https://medium.com/@timberners_lee/one-small-step-for-the-web-87f92217d085 (accessed 10

[2] Learning analytics is the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising learning and the environments in which it occurs.

March 2019)

Blanchard, E. G., Mizoguchi, R., and Lajoie, S. P. (2011), "Structuring the Cultural Domain with an Upper Ontology of Culture", *Handbook of Research on Culturally-Aware Information Technology*, Vol. 14, pp. 179–212, IGI Global. http://doi.org/10.4018/978-1-61520-883-8.ch009

Cavoukian, A. and Castro, D. (2014), "Big data and innovation, setting the record straight: de-identification does work", Privacy by Design, Ontario, Canada.

Cavoukian, A. (2012), "Privacy by Design: From Rhetoric to Reality", available at: https://www.ipc.on.ca/images/Resources/PbDBook-From-Rhetoric-to-Reality.pdf, accessed 13 February 2015.

Dourish, P. (2001), "Seeking a foundation for context-aware computing", *Human-Computer Interaction*, 16(2), 229-241.

Drachsler, H. and Greller, W. (2016), "Privacy and learning analytics – it's a DELICATE issue", *6th Learning Analytics and Knowledge Conference 2016*, April 25-29, 2016, pp. 89- 98. Edinburgh, UK. DOI: http://dx.doi.org/10.1145/2883851. 2883893.

European Commission. (2012), REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data . COM(2012) 11 final.

Felles studentsystem, (2018), "Privacy Policy", available at: https://www.fellesstudentsystem.no/english/applications/student-id/privacy-policy.html, (accessed10 March 2019).

Gilson, L. and Goldberg, C. B. (2015), "Editors' Comment: So, What Is a Conceptual Paper?" Group and Organization Management, 1–5. http://doi.org/10.1177/1059601115576425.,

Grech, A. and Camilleri, A. F. (2017), "Blockchain in Education". Publications Office of the European Union (pp. 1–136).

Griffiths, D., Drachsler, H., Kickmeier-Rust, M. D., Steiner, C. M., Hoel, T., and Greller, W. (2016), "Is Privacy a Show-stopper for Learning Analytics? A Review of Current Issues and Solutions", *LACE Review* (pp. 1–32).

Hoel, T. and 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*, DOI: 10.1186/s41039-018-0086-8.

Hoel, T., Griffiths, D., and Chen, W. (2017), The influence of data protection and privacy frameworks on the design of learning analytics systems (pp. 243–252), Proceedings of the Seventh International Learning Analytics and Knowledge Conference, New York, New York, USA: ACM Press. http://doi.org/10.1145/3027385.3027414

Hoel, T., and 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. http://dx.doi.org/10.18608/jla.2016.31.9

Hoel, T. and Chen, W. (2015), "Privacy in Learning Analytics – Implications for System Architecture", in Watanabe, T. and Seta, K. (Eds.) (2015), Proceedings of the 11th

International Conference on Knowledge Management, ISBN 978-4-9908620-0-8, presented at ICKM 15 in Osaka, Japan, 4 - 6 November 2015 ickm.kis.osakafu-u.ac.jp

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

ISO/IEC 20748-4:2019, "Information technology for Learning, education, and training — Learning Analytics Interoperability — Part 4: Privacy and data protection requirements".

Kenny S. and Borking J, (2002), "The Value of Privacy Engineering", *The Journal of Information, Law and Technology* (JILT): available at: http://elj.warwick.ac.uk/jilt/02-1/kenny.html, (accessed 10 March 2019).

Li, T., Bronfman, J. and Zhou, Z. (2017), "Saving Face: Unfolding the Screen of Chinese Privacy Law", *LawArXiv, 19 Aug. 2017*, https://doi.org/10.31228/osf.io/ndyus

Ma, Z. and Lin, Y. (2018), "Dorms' face recognition gets thumbs-up for convenience", *China Daily*, available at:
http://global.chinadaily.com.cn/a/201809/15/WS5b9c4583a31033b4f465630c.html, (accessed 10 March 2019).

McDougall, B. S. (2004), "Privacy in Modern China", *History Compass*, 2(1), Blackwell Publising, http://doi.org/10.1111/j.1478-0542.2004.00097.x

Marwick, A. E. and boyd, D. (2014), "Networked privacy: How teenagers negotiate context in social media", *New Media & Society*, 16(7), 1051–1067,
http://doi.org/10.1177/1461444814543995.

Narayanan, A. and Felten, E. W. (2014), "No silver bullet: De-identification still doesn't work", available at: http://www.randomwalker.info/publications/no-silver-bullet-de-identification.pdf, (accessed 10 March 2019).

Nissenbaum H.F. (2010), *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Niu, J., (2017), "Shenzhen targets jaywalking with face recognition", available at:
http://www.china.org.cn/china/2017-04/20/content_40658907.htm, (accessed 13 February 2019].

Ocheja, P., Flanagan, B., Ueda, H., and Ogata, H. (2019), "Managing lifelong learning records through blockchain", *Research and Practice in Technology Enhanced Learning*, 14(1), 11. http://doi.org/10.1186/s41039-019-0097-0.

Ohm, P. (2009), "Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, 57, 1701.

Page, D. (2016), "The surveillance of teachers and the simulation of teaching", *Journal of Education Policy*, 32(1), http://doi.org/10.1080/02680939.2016.1209566.

Palen, L. and Dourish, P. (2003), "Unpacking "privacy" for a networked world", in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI '03), ACM, New York, NY, USA, 129-136, DOI=http://dx.doi.org/10.1145/642611.642635.

Pangrazio, L. and Selwyn, N. (2018), ""It's Not Like It's Life or Death or Whatever": Young People's Understandings of Social Media Data", *Social Media + Society*, 4(3), 205630511878780–9. http://doi.org/10.1177/2056305118787808.

Polonetsky, J. and Tene, O. (2013), "Privacy and Big Data: Making Ends Meet", *Stanford Law Review Online*, 66, 25.

Rauhofer, J. (2008), "Privacy is dead, get over it! 1 Information privacy and the dream of a risk-free society", *Information & Communications Technology Law*, 17(3), 185–197. http://doi.org/10.1080/13600830802472990.

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

Rubinstein, I. S. (2013), "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, 3(2), 74–87, http://doi.org/10.1093/idpl/ips036.

Siemens, G. and Gasevic, D. (2012), "Guest editorial-learning and knowledge analytics", *Educational Technology and Society*, 15(3), 1–2.

Slade, S., Prinsloo, P., and Khalil, M. (2019), "Learning analytics at the intersections of student trust, disclosure and benefit", 1–1. *Proceedings of the 9th Learning analytics and Knowledge Conference 2019 (LAK 19), Tempe, Arizona, USA May 4- 8, 2019.*

Smith, H. J., Dinev, T., and Xu, H. (2011), "INFORMATION PRIVACY RESEARCH: AN INTERDISCIPLINARY REVIEW", *Mis Quarterly*, 35(4), 989–1015.

Solove, D. J. (2002), Conceptualizing Privacy. California Law Review, 90(4), 1087–1155. http://doi.org/10.2307/3481326?ref=no-x-route:b2978ad7e6a023a38f6a0148804669e1

Spiekermann, S., and Cranor, L. F. (2009), "Engineering Privacy", *IEEE Transactions on Software Engineering*, 35(1), 67–82. http://doi.org/10.1109/tse.2008.88.

Sprenger, P. (1999), "Sun on privacy: 'Get over it'", *Wired*, available at: http://www.wired.com/politics/law/news/1999/01/17538 (accessed 14 February 2019),

Stanaland, A. J. S., and Lwin, M. O. (2013), ONLINE PRIVACY PRACTICES: ADVANCES IN CHINA. *Journal of International Business Research*, 12(2), 1–146.

Wang, Z. and Yu, Q. (2015), "Privacy trust crisis of personal data in China in the era of Big Data: The survey and countermeasures", *Computer Law and Security Review*, 31(6), 782–792. http://doi.org/10.1016/j.clsr.2015.08.006.

Warren, S.D. and Brandeis, L. D. (1890), "The Right to Privacy", 4 HARV. L REV. 193.

Westin, A. F. (2003), "Social and Political Dimensions of Privacy", Journal of Social Issues, 59(2), 431–453. http://doi.org/10.1111/1540-4560.00072.

Young, E. (2015), "Educational privacy in the online classroom: FERPA, MOOCs, and the big data conundrum", *Harvard Journal of Law Technology*, 28(2).

Zuboff, S. (2019), "Surveillance Capitalism and the Challenge of Collective Action", *New Labor Forum*, 28(1), 10–29. http://doi.org/10.1177/1095796018819461.

Zuboff, S. (2015), "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology*, 30(1), 75–89. http://doi.org/10.1057/jit.2015.57/jit.2015.5.