International Journal of Artificial Intelligence in Education (2021) 31:769–783
https://doi.org/10.1007/s40593-020-00216-0

ARTICLE

Supporting Privacy, Trust, and Personalization in Online Learning

Mohd Anwar[1]

Accepted: 1 September 2020 / Published online: 30 September 2020

Abstract

Privacy is a rather murky concept, but the absence of privacy is clearly felt in today's digital world. With the significant increase in surveillance power of software and hardware, storage capacity, computing power as well as advancement in data science technologies, the threat to privacy is ever increasing. Within the digital realm, privacy has been studied in different platforms, contexts, and environments. In this capacity, Professor Jim Greer is one of the pioneering thought leaders to study privacy in online learning environment. Additionally, strongly related to privacy, trust and personalization are two important components of online learning. This article reflects on Greer's contributions to grapple with the following questions: (1) To what extent are privacy, trust, and personalization desired in online learning? (2) How can privacy, trust, and personalization be supported in online learning? In this vein, we study three theories (i.e., limitation theory, control theory, and contextual integrity theory) and different mechanisms (e.g., privacy preferences, identity management, contextual information flow) for privacy. Additionally, this article discusses the ways to achieve trust and personalization without compromising privacy.

Keywords Privacy · Online learning · Privacy preferences · Information flow · Trust · Context · Identity management · Personalization

This article belongs to the Topical Collection: *A festschrift in honour of Jim Greer*
Guest Editors: Gord McCalla and Julita Vassileva

✉ Mohd Anwar
manwar@ncat.edu

[1] Secure and Usable Social Media & Networks Lab, North Carolina A&T State University, Greensboro, NC, USA

Introduction

Privacy preserves human dignity, provides autonomy, and lowers barriers to communication. Privacy is at risk of erosion when our online activities create a trove of information that can easily be captured, stored, and disseminated at scale through technological means. This risk permeates every facet of online activity, and online learning is no exception. Professor Jim Greer was one of the earliest thought leaders to be concerned about privacy in online learning as well as information privacy in general (Anwar and Greer 2006, 2008a, b, 2009, 2011, 2012; Kettel et al. 2004; Richardson 2005; Anwar et al. 2006; Anwar 2008).

The global e-learning market will reach $325 billion by 2025 (McCue 2018). While 77% of online companies used online learning in 2017 to speed up employees' training, 49% of students have taken an online course in last 12 months in 2015 (Chernev 2019). From identity credentials to learning activities to transcripts, everything is stored online in the cloud. As a result, online learning environments have become prospective targets of data leakage attacks and the consequence of privacy breaches in online learning is quite significant. The increasing privacy concerns limit user trust on online learning systems as well as their level of disclosure – a prerequisite for personalized learning. Therefore, it has increasingly become urgent to have online learning platforms that support privacy, trust, and personalization.

Privacy is a nebulous concept as the need for privacy is elastic and both privacy and disclosure are desirable under different communicative contexts. Some of the early definitions of privacy such as "right to be let alone" (Warren and Brandeis 1890) are more fitting to physical privacy. With the advancement of Internet and Web technology, the online world has become an essential part of our lives. As a result, online privacy issues started to overwhelm us. Three major privacy theories that we find very relevant to today's online privacy concerns are: limitation theory, control theory, and contextual integrity theory. This article surveys these theories together with Greer & Anwar's approach on information privacy in online learning environment.

After surveying the notion of privacy, we discuss the need for information privacy in online learning environment. We highlight the need for suitable privacy policies and survey the privacy mechanisms introduced by Anwar and Greer. Specifically, we seek answers to following research questions:

1. To what extent are privacy, trust, and personalization desired in online learning?
2. How can privacy, trust, and personalization be supported in online learning?

The rest of this article is organized as follows. Section "Definition and Theories" discusses definitions and theories related to privacy, trust, and personalization. Section "Privacy, Trust, and Personalization in Online Learning" highlights the interactions among privacy, trust, and personalization in online learning. Section "Mechanisms for Privacy, Trust, and Personalization" discusses mechanisms for supporting privacy, trust, and personalization employed by Anwar & Greer in online learning. Section "Discussions" offers discussions on open problems and we conclude in "Conclusion".

Definition and Theories

Privacy

The notion of privacy was expressed in many different ways for myriad of online environments. This article is responsive to the privacy concerns of online learning. Therefore, we deconstruct three prominent theories of privacy in the context of online learning: limitation/restriction theory (Allen 1988), control theory (Altman 1975), and contextual integrity theory(Nissenbaum 2009). The limitation theory of privacy recognizes the need for limiting others from accessing to one's personal information. The control theory of privacy realizes the need for one's having control over their information. The main criticism of control theory is that it is an unreasonable expectation to have control over all information, especially when our online presence exposes us to different observers. Contextual integrity theory defines privacy in terms of context-relative informational norms (Nissenbaum 2009). Informational norms have following key parameters: actors (sender, recipient, subject), attributes (types of information), and transmission principles (constraints under which information flows).

Greer's work covers various aspects of all three major theories. Additionally, his work provides a unique perspective of tying identity and presentation to privacy. In his work, privacy is defined as the user's capacity to control the conditions under which their identity information will be presented. This notion of privacy is inspired by Irving Goffman's "presentation of self" (Goffman 1978) theory. Goffman argued that the elements of human interactions are dependent upon time, place, and audience. Time, place, and audience represent an information context and users conceal and reveal information based on the information context, Greer and Anwar argued (Anwar and Greer 2011). The concealing of information is in essence limiting access. The ability to conceal and reveal require users' control over their information.

Like Nissenbaum (2009), Anwar & Greer also defined contexts and contextual flow of information in online learning environment. They developed mechanisms to enforce contextual boundary of information through identity management. For privacy preservation, Anwar and Greer saw the need of different partial identity information to be presented to different audiences. Through partial identity boundaries, individuals should be able to: (1) exert control over data collection and (2) prevent data collected for one purpose to be used for another purpose.

Trust

Trust is defined as a mental state comprising of expectancy of a specific behavior from a trustee, belief that the expected behavior occurs, and willingness to take risk for that belief (Huang and Nicol 2010). In the context of online learning, this expectancy is from a user (e.g., learner) on another user (e.g., co-learner, instructor, etc.) as well as on the environment (e.g., LMS). For example, Wang (2014) observed that prospective students employ trust in the decision-making process of enrolling in online courses.

Trust is a precondition for self-disclosure. Trust reduces the perceived risks involved in disclosure of sensitive information.Trust determines the relevance or justification of a purpose for seeking data in a given context. Reputation is more of a social notion of trust (Golbeck and Hendler 2004). In our lives, we each maintain a set of reputations for the people we know. Anwar and Greer presented a model for facilitating trust integrating reputation with policies (Anwar and Greer 2011).

Personalization

Bol et al. define personalization as, "the strategic creation, modification, and adaptation of content and distribution to optimize the fit with personal characteristics, interests, preferences, communication styles, and behaviors (Bol et al. 2018)." Online activities generate a large amount of user information that companies use to tailor online services based on individuals' interests, behaviors, and needs. Personalization is an essential element of today's data-driven economy. Therefore, companies are more driven to accumulate data and less concerned about protection and proper use of data, putting users at risk of privacy breaches. Kobsa and Schreck have described the risks to privacy posed by personalization (Kobsa and Schreck 2003b).

Privacy, Trust, and Personalization in Online Learning

Anwar observed that the crux of the privacy concerns lies in the fact that a user has inadequate control over the flow (with whom information to be shared), boundary (acceptable usage of personal information), and persistence of information (duration of use) (Anwar 2008). Anwar and Greer further investigated the need for privacy in online learning (Anwar and Greer 2011). We revisit their findings in search of the first research question: **To what extent are privacy, trust, and personalization desired in online learning?** Privacy promotes safe learning. Therefore, privacy is required in the following popular learning activities: peer-tutoring, peer-reviewing, learning object selection, collaboration, group learning, evaluation, role-playing, and personalization.

Trust is a crucial enabler for meaningful and mutually beneficial interactions that build and sustain collaboration (e.g., collaborative learning). However, in most online learning environments, the (possibly pseudonymous) users are strangers whose interactions are limited to mostly written communications. Identity management (in the form of various degree of anonymity) is one technology-based approach to protect privacy. However, privacy-enhancing identity management (PIM) impedes trustworthiness assessment of an actor.

Anwar and Greer observed that privacy and trust are equally desirable, and one influences another (Anwar and Greer 2012). Privacy promotes safe learning while trust promotes collaboration and healthy competition. As part of the solution to privacy, Anwar and Greer also focused on trust relationships through identity management models. Due to lack of bodily presence of online actors, it is hard to establish trust relationship among them. Table 1 summarizes the observation

Table 1 Online learning activities and associated privacy/trust issues (Anwar and Greer 2011)

Activities	Associated Privacy/Trust Issues
Peer tutoring	Peer tutoring is a widely-practiced learning method. A learner needs to trust: (a) competence and benevolence of their peer tutors, (b) the online learning environment for enforcing privacy preferences. In a tutoring activity, a tutee shares her weakness with an expectation that her privacy will be preserved. Privacy and trust concerns can easily demotivate learners from participating in peer-tutoring activities.
Peer reviewing	Online portfolios are commonly used to engage learners in peer reviewing and assessment. These portfolios contain various sensitive information such as tests and test scores, projects, and self-reflections. Learners need to decide who they should trust with their e-portfolio items and whether they can trust the online learning environment.
Collaboration	Trust is essential to successful collaboration among e-learners (Mason and Lefrere 2003; Haythornthwaite 2006). In a learning environment, various key relationships of recommender-recommendation seeker, peer-peer, helper-helpee, and mentor-mentee are formed based on mutual trust. Therefore, privacy and trust are interconnected in a collaborative environment. The privacy concerns in collaborative activities stem from individuals' desire to control how one is perceived by another (Patil and Kobsa 2005) .
Group learning	A discussion forum or a reading group offers valuable learning experience to learners. A group functions well when each member trusts each other and respects each other's privacy preferences. As a result, an online learning system needs to facilitate trust and privacy. Privacy can also be breached by a learner's own behavior of too much exposing of self.
Evaluation	Confidentiality is a prerequisite for learner assessment and evaluation process. Learners may experience various biases such as gender, ethnic, or connectedness (more connected to the evaluator). Biases in learner evaluation can be prevented through privacy-preserving techniques (Aimeur et al. 2007). In a trust relationship, learners' confidence can grow regarding the fairness of evaluation.
Role playing	Role playing is an effective technique for exploring complex social issues in certain courses (such as Sociology). Safety is an essential condition for authentic role playing. Learners' safety can be assured through trustworthy and privacy-protecting learning environments.

of Anwar and Greer about the need for privacy and trust in popular learning activities.

Personalization is an essential component of today's online learning. Because of continuous monitoring of learners for personalized learning, and amassing learner's data into large databases to generate learner analytics, privacy threats are real.

Personalization of learning objects can increase the motivation and interest of learners (Bates and Wiest 2004). As a result, in recent time, we have witnessed an increasing volume of research and development efforts to offer personalized e-learning. Trust has been identified as a prerequisite (Kobsa and Schreck 2003a) and a consequence of good personalization practice (Karat et al. 2004) . Anwar et al. define key characters of an e-learning environment that offers personalization together with trust and privacy (Anwar et al. 2006).

Mechanisms for Privacy, Trust, and Personalization

In this section, we explore, **"How can privacy, trust, and personalization be supported in online learning?"** Anwar and Greer proposed mechanisms for privacy preferences (Kettel et al. 2004), identity management (IM) (Anwar and Greer 2008a, 2009, 2012; Richardson 2005), contextual flow of information (Anwar and Greer 2012; Kettel et al. 2004), trust (Anwar and Greer 2006, 2008b, 2011), and personalization (Anwar et al. 2006) to protect the privacy of learners. Identity management *provides a form of privacy* (the protection of personal information) through users' anonymity or pseudonymity. The users are allowed to operate multiple identities or can adopt new pseudonymous personas as long as contextual norms are maintained, and the integrity of the reputation systems is not undermined. As a result, they proposed a reliable and trustworthy mechanism for reputation transfer from one partial identity to another. This reputation transfer system prevents linkability of learners' identities and personas. For the need of concealing, privacy concerns can be mitigated through anonymization. Identity management system can assist users negotiating the calculus of trust and privacy.

Privacy Preferences

Information about learners is diverse and may include a wide range of activities and assessments such as quiz results, assignment marks, submission times, how often and when learner accessed course materials, postings made and read on web-based discussion boards, ratings of posting quality by participants, chat interaction logs, and opinions held about the learner by others. Kettel, Brooks, and Greer raise the question, with deep meaningful information shared about learners, who is protecting the privacy rights and desires of the learners? (Kettel et al. 2004). In a complex, multi-role, multi-user environment, it is hard to impart necessary personal information of users for learning activities such as group building, social navigation, locating appropriate helper, etc. while protecting their privacy. Building around semantic web and web service technologies, they offered a proposed implementation of a privacy filter approach.

To allow users to control their own level of privacy, they designed to control access to the stream of events and information that flow through learning environments. Every time users interact with the learning environment, an event is triggered within the system and passes through the system's Event Stream. It is assumed that each user has their own personal agent and that users configure their agent with their own individual privacy preferences. The personal agent captures a user's level of sensitivity to their information and seeks privacy accordingly. The user describes which kinds of information can be passed on to different types of users (e.g. grades to my teachers and interest indicators to my friends), and in which format (e.g. identified by name, alias, or anonymously). However, there is a knowledge gap about how much users know the consequences of decisions they make when they configure their agent.

Identity Management (IM) for Privacy

A proponent of more control for users over their personal information, Richardson and Greer proposed identity management architecture that allows users to decide on a per business basis what personal information is provided (Richardson 2005). The identity management architecture helps users manage personal information and improves a user's awareness of and access to his or her personal information and help businesses to more easily comply with privacy legislation. Persona and identity are two main components of identity management system. A persona is essentially an identity. However, multiple personas can each use the same personal information from a single identity. A user may create two identities with two set of personal information. However, a user may create two personas with same identity information to maintain separate relationships with two businesses. In essence, identities and personas help create contextual boundaries.

Another important identity management-based privacy solution proposed by Anwar & Greer is role- and relationship-based identity management (RRIM) (Anwar and Greer 2009, 2012). The processes associated with RRIM are described in Table 2.

Contextual Information Flow for Privacy

Anwar and Greer defined communicative context through roles and relationships (Anwar and Greer 2008a). In online learning, there are well-structured roles such as instructor, grader, teaching assistants, learners, etc. and relationships such as one-to-one (e.g., mentor-mentee), one-to-many (e.g., instructor-class), hierarchical (e.g., instructor-grader) are relatively predictable. In their approach, there are two kind of identities: role-based and relationship-based. A role-based identity hides an actor in the crowd of same roles and a relationship-based identity draws the boundary of communication to specific relationship. Moreover, they assigned guarantor privileges to public roles to sanction foul acting and to facilitate usage control.

Supporting Trust

Reputation, which is a longitudinal social evaluation on a person's actions, can be used as a measure of trustworthiness of an actor's future behavior. A good reputation is a return on a long term investment of good behavior. Anwar & Greer proposed a reputation transfer model that would allow reputation transfer among multiple pseudo-identities (e.g. pseudonyms) without letting anyone associate these pseudo-identities (Anwar and Greer 2006, 2008b). As a result, this model facilitates both privacy and trust.

The assumption is that both the transferring and receiving identities are just two pseudo-identities for one entity. A pseudonymous entity can update the reputation of one pseudonym by transferring its reputation from another pseudonym. A guarantor vouches for an entity in two ways: i) responding to the queries about the pseudonym, ii) responding to the entity's reputation transfer request from one pseudonym to another. Since both the transferring and receiving entities are registered users of a guarantor, any bad acting can be traced and verified. All the communication between

Table 2 The exemplar tasks and processes associated with role- and relationship-based identity management for privacy-preserving yet accountable online learning activities

Tasks	Processes
Context constructions	Based on purposes of learning, various information contexts are enumerated. Each context has a time-to-live stamp to indicate an expiration after fulfilling its purpose.
Role-based identity creation	Based on a user's expected role and activities in the context, each user account is granted various potential roles and associated default pseudonyms (e.g., academic10, learner007, etc.).
Relationship-based identity creation	A user in a given information context may construct a relationship-based identity for a relationship type permitted for the assumed role (e.g., one-to-one student-teacher relationship) from the system. The system provides a default pseudonym (e.g., Bill).
Identity awareness	To facilitate contextual information flow, a user is presented with contextual identity information upon logging on to the system. Before posting a message, a user sees the preview of the message, underpinning context, assumed role, and the pseudonym.
Identity assumptions	Upon a single sign-on, a user may choose a desired context, role, or relationship node from the contextual identity dashboard to participate in a respective capacity under a respective context. A user may use an identity from a context to its sub-contexts.
Identity expirations	A role- or a relationship-based identity and its associated interactions are expunged from the system at the end of the context for which the identity is created. If a role-based identity from an information context is used at any of its child contexts, the identity and the associated interactions are expunged only from that child context at its end. A user may shed any of their role- or relationship-based identity at anytime unless the identity is locked (see Identity Locking task). For that matter, the user may request the system to remove any interaction under their disowned identity.
Identity locking	The user of a locked identity is barred from changing their pseudonym, and the user is not allowed to construct a new identity in the same context. For example, when a student with $Student\_007$ pseudonym is sanctioned for bad acting in a CMPT250 course forum, that student is locked in their $Student\_007$ pseudonym.
Digital forgiveness	When a bad actor is forgiven, they are allowed to change their pseudonym associated with the bad acting or to create a new identity.

an entity and the guarantor takes place using each the other's public key. Moreover, the integrity of reputation can be checked using the reputation digest.

Supporting Personalization

In the context of online learning, personalization refers to the selection or customization of learning content as well as sequences of learning activities to meet the needs

of individual learners (O'Keeffe et al. 2012). One of the primary uses of learning analytics is to support personalization. Greer's research shows that personalization is possible without compromising personal space of the learners. With a call for proper policy and mechanism (technical framework), Anwar et al. (2006) made recommendations and implemented a privacy-enhanced learning environment that also supports content personalization through pseudonymization of learner identifiers. For personalization, a pseudonym allows correlating datasets from one learner, however, the system allows anonymization for total non-disclosure and can de-psrudonymize the learner if accountability is warranted.

Learning analytics are utilized to understand and improve learning experience of the learners. Pardo and Siemens (2014) observe that in the context of learning analytics, privacy is tightly connected with trust and transparency. Learning Analytics can be utilized to create a personalized learning environment that can provide recommendations to learners concerning peers and the learning objects. Potts et al. (2018) proposed an open-source course-level recommendation platform to provide reciprocal peer recommendation for learning purposes. Troussas et al. developed a multi-module model which identifies learners' cognitive states and predicts their behavior in order to provide learning object recommendations, curriculum improvement supporting personalized instruction (Troussas et al. 2020).

Table 3 highlights some privacy features of a learning environment that can ease the issue of trusting the learning environment.

Discussions

With the wide adoption and acceptance of online learning, privacy has become a critical issue. However, the need for privacy cannot be described in absolute term. Privacy is strongly connected with the issues of trust and the value of personalization. Therefore, any policy or mechanism for privacy also needs to take trust and personalization into consideration.

The notion of context is ambiguous and it is onus of users to understand the context Privacy, trust, and personalization– all depends on context. Therefore, context is an essential element in privacy protection. However, it is hard to operationalize context. It also creates cognitive burden on users to maintain contextual boundaries as they share information. The environment has to facilitate contextual awareness or provide suggestions of context to users. The online learning environment needs to help users maintain contextual flow of information.

Privacy matters to all actors Privacy solutions should not only focus on learners. Privacy matters to all the actors in online learning (instructors, administrators, tutors, etc.). Besides, with the increased participatory and contributory nature of web, there is no fixed consumer or producer of content in social learning portals or communities of practices. Therefore privacy solutions have to be all inclusive to all actors in the system.

Table 3 Recommended features of a privacy-protecting personalized online learning environment

Privacy features	Description
Allow pseudonymity	A user should be allowed for multiple pseudonyms to be used in different information contexts. As a result, personalization can be offered within a context to pseudonymous learners without compromising privacy.
Allow anonymity when possible	Personalization does not always enhance user experience. A user should be able to perform low risk activities (e.g. asking a question in a class discussion forum) anonymously.
Facilitate trust-based information sharing	A user should be able to share personal information with other trusted users. The system should help a user evaluate the trustworthiness of other actors or the system and help them make informed choices about sharing information based on trust. As a result, trust improves both personalization and privacy. On the other hand, Lawani et al. (2015) showed that fine-grained control over data leads to improved trust on the system.
Allow attaching contextual cues with information	An actor plays different roles in different contexts (e.g. socialization, collaboration with fellow learners, one-to-one communication with the instructors, etc.). The system should support context separation so that information from different contexts are not fused together to gain the knowledge of identity. Personalization needs to be supported based on the role an actor plays in a given context.
Attach verbal and non-verbal cues	Since verbal and certain non-verbal cues reveal the intention of an interlocutor, the system should provide a way to attach cues to information to avoid misunderstanding and grow trust among the participants of the e-learning environment. Verbal cues can be supported by providing readily available easy to attach tags (e.g. jokingly, hypothetically, sincerely, etc.), as well as emoticons (small pictorial representations of the emotional state of the user). Information cues also support personalization.
Detect and purge unnecessary personal information	When an actor immerses themselves into e-learning activities they cannot always judge the private nature of information they share with other users. The system should take the job of judging the nature of information and warn the users about any accidental privacy slip.
Allow information to expire	We view users as the rightful owner of their personal information even when the information is shared or observed by someone else. A user may share some of their information to somebody for a period of time. However, they should be able to destroy the information after that time is over. We suggest attaching 'time to live' tag for each piece of information and making it inaccessible when the time expires.

Table 3 (continued)

Privacy features	Description
Promote privacy awareness	Some users may not readily understand the need for privacy. The system could play the role of a privacy coach (similar to Teaching Privacy[2] (Bernd et al. 2015)) by providing privacy tips, presenting privacy policy of its own, and asking users for their privacy preferences. The preferences for privacy need to be respected while offering personalization.
Punish bad actors	The system could employ a reputation system that would recognize the good users with a higher reputation score and thereby facilitating trust. Many different levels of sanction could be applied to bad actors from restricting anonymity to revoking the privilege of participation in certain activities.

A partial identity of a user needs to have a temporal dimension A Partial identity or an identifier needs to have a temporal dimension. There has to be well-defined lifetime of identities and any information anchored on identities also need to expire.

Balancing of privacy and accountability is needed In online learning, privacy is important along with accountability. We need to preserve privacy but support community building for which accountability is very important.

Privacy in the age of learning analytics Research shows that users are willing to share personal information for benefits as longs as they trust the context for sharing and have control over their data. Slade et al. (2019), (Prinsloo and Slade 2016) found that students greatly trust their university to use their data appropriately and ethically. On the other hand, a Pew research study found that most internet users (86%) would like to be anonymous and a significant 59% of them have taken steps to avoid observations by people, organizations, or governments (Rainie et al. 2013). Ivanova et al. (2019) underlines the need for effective mechanisms and digital competence for a responsible use and sharing of own and others private data in personal learning environments (PLEs) such as informal Web 2.0 / Social Media PLEs, mobile PLEs, ePortfolio-based PLEs, etc.

Ethical perspectives of privacy Pardo and Siemens (2014) discussed ethical issues arising from capture and use of personal information in online learning. Drachsler and Greller (2016) discuss the issues of privacy and ethical use of learning analytics. Although the scope of this paper is limited to privacy and its relationship with personalization and trust, the ethical side of privacy is of significance and that should guide the practices of data collection and dissemination. The developers of online learning systems need to grapple with ethical questions of surveilling users and using and disseminating their information without allowing the users to make an informed choice.

Lately, the privacy-by-design principles have received wide recognition, however, Verhagen et al. (2016) observes that clashes between values are unavoidable and collaboration between ethicist and software designers at early stage of design is required for the implementation of privacy-by-design.

Legal perspectives of privacy In recent times, privacy laws have emerged to protect user privacy. In the United States, there are several privacy laws to address different aspects of privacy. For example, the Health Insurance Portability and Accountability Act (HIPAA) (https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf) protects personal health information. The Fair and Accurate Credit Transaction Act (FACTA) protects against theft of credit information. The Children's Online Privacy Protection Act (COPPA) protects the privacy of those under the age of 13. US Department of Education (2014) recommends checking if student information used in online educational services is protected by Family Educational Rights and Privacy Act (FERPA). On the other hand, the core of Europe's digital privacy legislation is General Data Protection Regulation (GDPR) (Voigt and Von dem Bussche 2017) for data protection and privacy in the European Union and the European Economic Area. These privacy laws provide some framework for protecting privacy, but is not adequate to ensure control or transparency. For example, Schaub et al. (2017) observed that regulatory compliance produces long and complex privacy policies but not transparency to users. Greer and colleagues strived for developing technical means to empower users and provide transparency for privacy.

Privacy in the age of data Greer's more recent works (e.g., Books et al. 2014) were focused on data-assisted approaches to develop intelligent technology-enhanced learning environments where learner activities are modeled with actors (learners, instructors, instruction assistants), artefacts (videos, tests, webpages), interaction behaviors (watching, answering, clicking). Increasingly, data driven approaches with disruptive technologies such as various mobile and virtual reality technologies will be prevalent in online learning. As the new technologies provide novel ways to make learning personalized, informal, and life-long; learners need to make decisions on the trade-offs of sharing vs. withholding personal information. As a result, the future success of online learning will lie at the intersections of privacy, trust, and personalization.

In summary, privacy in online learning is an interesting microcosm of the broader issues of privacy in online communities. As a result, all the issues discussed here is very relevant to online privacy in general. In this age of information and data analytics, users gain some short-term benefits from sharing personal information without fully grasping the cost of long-term privacy. This paper surveyed the work of Greer and others on building privacy-preserving online learning system that supports contextual boundary regulation by the users for information disclosure and dissemination. The future of the information society is strongly tied to its citizen's ability in maintaining the contextual boundary of their personal information through privacy-protecting technologies, policies, ethics, and laws.

Conclusion

Privacy provides protection from misuse of information, it is a prerequisite to any relationship like collaboration, and privacy encourages free thinking. As a result, privacy is critical for online learning. Because learning is one of the fastest growing online activity, the breaches of privacy can significantly damage online learning platform. Due to lack of bodily presence, trust is not only harder to establish online, but also misplaced trust have severe consequences. Privacy can help build trust. Realizing the need for privacy and trust and the relationship thereof, Greer and his coauthors proposed various methods to provide privacy and trust in online learning. In addition to supporting theory of limitation, control, and context, Greer et al. utilized a unique aspect of identity management for privacy. In the future, the protection of privacy will increasingly be challenged by powerful technologies to capture, store, and disseminate data. The online service providers need to maintain a strong privacy posture as well as take on a larger role in supporting privacy in their respective environments.

Acknowledgesments This article is dedicated in memory of Professor Jim Greer, to whom the author is indebtedly grateful for the support in his intellectual growth.

References

Aimeur, E., Hage, H., Onana, F.S.M. (2007). A framework for privacy-preserving e-learning. In *IFIP International Conference on Trust Management* (pp. 223–238). Boston: Springer.

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

Altman, I. (1975). The environment and social behavior: privacy. Personal Space, Territory, and Crowding. Brooks/Cole Pub.

Anwar, M.M. (2008). An identity-and trust-based computational model for privacy (Doctoral dissertation, PhD thesis, Department of Computer Science University of Saskatchewan, Saskatoon, Canada.

Anwar, M., & Greer, J. (2006). Reputation management in privacy-enhanced e-learning. In *Proceedings of the 3rd Annual Scientific Conference of the LORNET Research Network (i2LOR-06), Montreal, Canada*.

Anwar, M., & Greer, J. (2008a). Role-and relationship-based identity management for private yet accountable e-learning. In *IFIP International Conference on Trust Management* (pp. 343–358). Boston: Springer.

Anwar, M., & Greer, J. (2008b). Enabling reputation-based trust in privacy-enhanced learning systems. In *International Conference on Intelligent Tutoring Systems* (pp. 681–683). Berlin: Springer.

Anwar, M., & Greer, J. (2009). Implementing role-and relationship-based identity management in e-learning environments. In *Proceedings of the 2009 conference on Artificial Intelligence in Education* (pp. 608–610). Netherlands: IOS Press.

Anwar, M., & Greer, J. (2011). Facilitating trust in privacy-preserving e-learning environments. *IEEE Transactions on Learning Technologies*, *5*(1), 62–73.

Anwar, M., & Greer, J. (2012). Role-and relationship-based identity management for privacy-enhanced e-learning. *International Journal of Artificial Intelligence in Education*, *21*(3), 191–213.

Anwar, M., Greer, J., Brooks, C.A. (2006). Privacy enhanced personalization in e-learning. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services* (p. 42): ACM.

Bates, E.T., & Wiest, L.R. (2004). Impact of personalization of mathematical word problems on student performance. The Mathematics Educator, 14(2).

Bernd, J., Gordo, B., Choi, J., Morgan, B., Henderson, N., Egelman, S., Friedland, G. (2015). Teaching privacy: Multimedia making a difference. *IEEE MultiMedia*, *22*(1), 12–19.

Bol, N., Dienlin, T., Kruikemeier, S., Sax, M., Boerman, S.C., de Vreese, C.H. (2018). Understanding the effects of personalization as a privacy calculus: Analyzing self-disclosure across health, news, and commerce contexts. *Journal of Computer-Mediated Communication*, *23*(6), 370–388.

Brooks, C., Greer, J., Gutwin, C. (2014). The data-assisted approach to building intelligent technology-enhanced learning environments. In Larusson, J.A., & White, B. (Eds.) *Learning analytics: From Research to Practice* (pp. 123–156). New York: Springer.

Chernev, B. (2019). 21 Astonishing E-Learning Statistics For 2019. Retrieved from https://techjury.net/stats-about/elearning/#gref.

Drachsler, H., & Greller, W. (2016). Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In *Proceedings of the sixth international conference on learning analytics & knowledge* (pp. 89–98).

Goffman, E. (1978). The presentation of self in everyday life (p. 56). London: Harmondsworth.

Golbeck, J., & Hendler, J. (2004). Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In *International conference on knowledge engineering and knowledge management* (pp. 116–131). Berlin: Springer.

Haythornthwaite, C. (2006). Facilitating collaboration in online learning. *Journal of Asynchronous Learning Networks*, *10*(1), 7–24.

Huang, J., & Nicol, D. (2010). A formal-semantics-based calculus of trust. *IEEE Internet Computing*, *14*(5), 38–46.

Ivanova, M., Marín, V.I., Tur, G., Buchem, I. (2019). Towards Privacy Issues in Personal Learning environments: A Conceptual Model of PLE Privacy. European Journal of Open, Distance and E-learning, 22(1).

Karat, C.M., Blom, J.O., Karat, J. (Eds.) (2004). *Designing personalized user experiences in eCommerce*, Vol. 5. Berlin: Springer Science & Business Media.

Kettel, L., Brooks, C.A., Greer, J.E. (2004). Supporting Privacy in E-Learning with Semantic Streams. In *PST* (pp. 59–67).

Kobsa, A., & Schreck, J. (2003). Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology (TOIT)*, *3*(2), 149–183.

Kobsa, A., & Schreck, J. (2003). Privacy through pseudonymity in user-adaptive systems. *ACM Transactions on Internet Technology (TOIT)*, *3*(2), 149–183.

Lawani, O., Aïmeur, E., Dalkir, K. (2015). Improving users' trust through friendly privacy policies: an empirical study. In *International Conference on Risks and Security of Internet and Systems* (pp. 55–70). Cham: Springer.

Mason, J., & Lefrere, P. (2003). Trust, collaboration, e-learning and organisational transformation. *International Journal of Training and Development*, *7*(4), 259–270.

McCue, T.J. (2018). E Learning Climbing To $325 Billion By 2025. Forbes. Retrieved from https://www.forbes.com/sites/tjmccue/2018/07/31/e-learning-climbing-to-325-billion-by-2025-uf-canvas-absorb-schoology-moodle/.

Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. Stanford University Press.

O'Keeffe, I., Staikopoulos, A., Rafter, R., Walsh, E., Yousuf, B., Conlan, O., Wade, V. (2012). Personalized activity based eLearning. In *Proceedings of the 12th International Conference on Knowledge Management and Knowledge Technologies* (pp. 1–8).

Pardo, A., & Siemens, G. (2014). Ethical and privacy principles for learning analytics. *British Journal of Educational Technology*, *45*(3), 438–450.

Patil, S., & Kobsa, A. (2005). Privacy in collaboration: Managing impression. In *The First International Conference on Online Communities and Social Computing*.

Potts, B.A., Khosravi, H., Reidsema, C., Bakharia, A., Belonogoff, M., Fleming, M. (2018). Reciprocal peer recommendation for learning purposes. In *Proceedings of the 8th International Conference on Learning Analytics and Knowledge* (pp. 226–235).

Prinsloo, P., & Slade, S. (2016). Student vulnerability, agency, and learning analytics: An exploration. *Journal of Learning Analytics*, *3*(1), 159–182.

Rainie, L., Kiesler, S., Kang, R., Madden, M. (2013). Anonymity, privacy, and security online. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

Richardson, B.R. (2005). An architecture for identity management (Master's Thesis) University of Saskatchewan, Saskatoon, Canada.

Schaub, F., Balebako, R., Cranor, L.F. (2017). Designing effective privacy notices and controls. IEEE Internet Computing.

Slade, S., Prinsloo, P., Khalil, M. (2019). Learning analytics at the intersections of student trust, disclosure and benefit. In *Proceedings of the 9th International Conference on Learning Analytics & Knowledge* (pp. 235–244). New York: ACM.

Troussas, C., Krouska, A., Virvou, M. (2020). Using a multi module model for learning analytics to predict learners? cognitive states and provide tailored learning pathways and assessment. In *Machine Learning Paradigms* (pp. 9–22). Cham: Springer.

US Department of Education (2014). Protecting student privacy while using online educational services: Requirements and best practices.

Verhagen, J., Dalibert, L., Lucivero, F., Timan, T. (2016). Designing values in an adaptive learning platform 2nd workshop on Ethics & Privacy in Learning Analytic during the 6th International Learning Analytics & Knowledge Conference, Apr 2016, Edinburgh, United Kingdom.

Voigt, P., & Von dem Bussche, A. (2017). *The eu general data protection regulation (gdpr). A Practical Guide*, 1st edn. Cham: Springer International Publishing.

Wang, Y.D. (2014). Building student trust in online learning environments. *Distance Education*, *35*(3), 345–359.

Warren, S.D., & Brandeis, L.D. (1890). Right to privacy. *Harv. L. Rev.*, *4*, 193.