International Journal of E-Learning & Distance Education
La Revue internationale de l'apprentissage en ligne et de l'enseignement à distance

ISSN: 2292-8588 **Volume 37, No. 1, 2022**

Towards Safeguarding Users' legitimate rights in Learning Management Systems (LMS): A case study of Blackboard at Sorbonne University Abu Dhabi

Dr. Victor Kabata

Abstract: This paper sought to establish the extent to which users' legitimate rights are safeguarded in Learning Management Systems (LMS); specifically, on the *Blackboard* system used for teaching at Sorbonne University, Abu Dhabi (SUAD). First, the users' legitimate rights that required protection were identified. Second, the security and privacy guarantees afforded by *Blackboard* were assessed. Finally, policy gaps and technological deficiencies that undermine the protection of users' legitimate rights were identified. The study adopted a qualitative research approach and a case study research design. Data was collected through content analysis, document review and interviews. The research revealed that to a large extent the *Blackboard* LMS safeguarded most of the users' legitimate rights. However, the system is silent on some legitimate rights, such as storage limitation and data sharing arrangements. Further, information emerged that revealed *Blackboard*'s privacy practices are largely informed by educational institutions using its products. The study concluded that safeguarding user's legitimate rights is a collective responsibility between the learning management services providers and the educational institutions. As such, there is need for educational institutions using *Blackboard* and other learning management systems to craft robust data protection regimes.

Keywords: Learning Management Systems, Privacy, Users' legitimate rights

Résumé: Cet article a cherché à déterminer dans quelle mesure les droits légitimes des utilisateurs sont sauvegardés dans les plateformes de gestion de l'apprentissage (LMS) et, plus précisément, dans la plateforme Blackboard utilisée pour l'enseignement à l'Université Sorbonne, Abu Dhabi (SUAD). Tout d'abord, les droits légitimes des utilisateurs qui doivent être protégés ont été identifiés. Ensuite, les garanties de sécurité et de confidentialité offertes par Blackboard ont été évaluées. Enfin, les lacunes politiques et les déficiences technologiques qui compromettent la protection des droits légitimes des utilisateurs ont été identifiées. L'étude a été réalisée selon une approche qualitative d'étude de cas. Les données ont été recueillies par le biais d'une analyse de contenu, d'un examen des documents et d'entretiens. La recherche a révélé que, dans une large mesure, la plateforme Blackboard protège la plupart des droits légitimes des utilisateurs. Cependant, la plateforme ne donne pas d'indication concernant certains droits légitimes, tels que la limitation du stockage et les accords de partage des données. En outre, des informations ont révélé que les pratiques de Blackboard en matière de confidentialité sont largement influencées par les établissements d'enseignement qui utilisent ses produits. L'étude a conclu que la sauvegarde des droits légitimes des utilisateurs est une responsabilité collective entre les fournisseurs de services de gestion de l'apprentissage et les établissements d'enseignement. Il est donc nécessaire que les établissements d'enseignement qui utilisent Blackboard et d'autres plateformes de gestion de l'apprentissage élaborent de solides régimes de protection des données.

Mots-clés: Plateformes de gestion de l'apprentissage, Vie privée, Droits légitimes des utilisateurs

Introduction

In the last decade, many higher education institutions have adopted learning management systems (LMSs) as their preferred platform for teaching. This shift towards e-learning is attributed to advances in digital technologies that have made distance learning more widely accepted. The demand for remote learning and use of LMSs has further been intensified by the Covid-19 pandemic. While the adoption of LMSs for teaching and learning is considered convenient and efficient, there are numerous legal and ethical challenges associated with their deployment. For instance, there are questions relating to confidentiality, accuracy, and the retention period of personal data created and uploaded on LMSs. Further, there are concerns relating to intellectual property, particularly regarding ownership of content uploaded on LMSs, and how this content can be shared while adhering to copyright requirements. Moreover, it is unclear if LMSs have put in place security arrangements to safeguard users' data.

There is consensus on the need to uphold ethics in the information society. The World Summit on Information (2005), Action line 10, outlines the ethical dimensions of the information Society. Specifically, Action line 10 advocates the need for information communication technologies (ICTs) to be underpinned by values of common good and human rights as well as preventing abusive use (WSIS, 2005). Likewise, the European Union's (EU), General Data Protection Regulations (GDPR) echo the need to protect fundamental rights and freedoms of natural persons, particularly when processing personal data by automated means (EU, 2016).

Blackboard is among the most popular LMSs in the world, with wide usage among schools and institutions of higher learning. As of July 2014, the system served approximately 20,000 schools and organizations, had more than 20 million users, and the

highest share of the education market with 75% of colleges and universities in the United States using its products and services (Subramanian et al., 2014).

Despite, the widespread adoption and usage of the Blackboard LMS, empirical information relating to its ability to safeguard users' legitimate rights remains scant. This study seeks to fill this research gap by assessing the extent to which the Blackboard LMS safeguards users' legitimate rights.

Research Problem

The use of LMSs for teaching means that a lot of content is created and uploaded onto the system to facilitate learning. However, many LMSs have not prioritized adequate policy and technological guarantees to safeguard the privacy, security, and intellectual property of users' data that is created and shared on these platforms. A literature review revealed that the majority of LMS systems have focused on course development and delivery with little or no consideration to privacy and security as required elements (El-Khatib et al., 2003).

This paper seeks to address this research gap by highlighting the privacy, security and copyright requirements for learning management systems, with a particular focus on the Blackboard system that is used for teaching at Sorbonne University Abu Dhabi (SUAD). Specifically, the researcher will use classical and contemporary ethical traditions as well as European Union's General Data Protection Regulations (GDPR) and data protection principles to map out the users' rights that must be protected when using an LMS for teaching and learning. Subsequently, the researcher will investigate the security and privacy guarantees afforded by the Blackboard LMS in adherence to the identified users' legitimate rights. Lastly, the study will identify the policy gaps and technological

deficiencies that undermine the protection of users' legitimate rights in the Blackboard system.

Research Questions

The objective of this study was to establish whether users' legitimate rights are safeguarded in the Blackboard LMS. This objective was achieved by answering the following research questions:

1. What are the users' legitimate rights that should be protected while using Blackboard and other Learning Management Systems?
2. Which among the users' legitimate rights are safeguarded in the Blackboard LMS?
3. What policy gaps and technological deficiencies are undermining users' legitimate rights in the Blackboard LMS?

Theoretical Framework

This study uses both classical and contemporary theoretical perspectives as orienting lenses in analysing the concept of legitimate rights. The classical perspective focuses only on privacy, confidentiality, contextual integrity, and freedom (Kaplan & Haenlein, 2010; Mutula, 2013). A holistic approach to the concept of legitimate rights is informed by concern among researchers that the classical perspective of legitimate rights does not adequately illuminate the ethical implications of emerging information technologies.

Contemporary ethical model provide a broader perspective of the concept of "legitimate rights" by defining the ethical standards in technological environments. It draws from computer ethics and philosophy of technology (Kaplan & Haenlein, 2010; Giles, 2006; Boyd, 2007). The contemporary ethical traditions encompass a broad range of issues such

as disclosure ethics, global information ethics, pragmatism, virtual ethics, feminism and care ethics, and intercultural information ethics (Capurro, 2010).

The ethical issues in technological environments as espoused by the contemporary ethical traditions are access and accessibility, accuracy, security, trust, illegal surveillance, identity, theft, intellectual property, and copyright (World Summit on the Information Society, 2005; Kaplan & Haenlein 2010; Mason, 1986).

Accordingly, the contemporary ethical traditions will complement the classical tradition as an orienting lens for this study as it provides a broader understanding of the legitimate rights (privacy, security, and intellectual property) that should be safeguarded when using the Blackboard LMS (henceforth referred to simply as Blackboard).

The relevance of both classical and contemporary ethical traditions as underpinning conceptual models for this study is further underscored by the fact that the ethical issues articulated by the models are consistent with the principles of data protection outlined in Article 5 of the European Union's (EU) General Data Protection Regulations (GDPR). As an education institution (data controller), domiciled in France and United Arab Emirates (UAE), SUAD is obliged to manage its users' data in compliance with provisions of EU's GDPR and the UAE Data Protection law, Federal Decree-Law No. 45 of 2021, announced on November 27, 2021. Notably, EU's GDPR is regarded as the global standard for protecting personal data. As such, UAE Data Protection Law largely mirrors provisions of the EU's GDPR.

El-Khatib et al. (2003) reinforce the idea of using EU's GDPR as an additional orienting lens for studies of this nature by noting that use of privacy principles would assist in establishing how well an application meets privacy requirements. The authors further

noted that the privacy principles offer a means of critiquing the appropriateness of different technologies (El-Khatib et al., 2003).

Literature Review

As mentioned earlier, the users' legitimate rights articulated in the classical and contemporary ethical traditions are embodied in the EU's GDPR data protection principles. In view of this, review of literature on research question one of this study—requiring the identification of users' legitimate rights to be protected in Blackboard—will be discussed under three broad themes: privacy, security, and intellectual property.

Below is a discussion of each of these broad themes, and how each of them will be assessed in the context of Blackboard.

Users' Legitimate Rights that Require Protection in Blackboard

1. Privacy Rights

According to Banisar and Davies (1999), privacy is a fundamental right essential to the autonomy and the protection of human dignity, serving as the foundation upon which other human rights are founded. Internationally, privacy is regarded as a fundamental human right that is recognised in international conventions and treaties. Specifically, Article 12 of the United Nations Declaration on Human Rights (1948) recognises privacy by stating:

> *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks (p.4).*

Similarly, Article 17 of the International Convention of Civil and Political Rights (ICCPR) recognises privacy in the same wording as the UNDHR.

In the context of data management systems, the right to protection of personal data is considered an important element of privacy. Specifically, EU's GDPR describes privacy in the context of protection of personal data as the right to protection of natural persons in relation to processing activities and to ensure the free flow of personal data between member states (EU, 2016).

As far as LMSs are concerned, privacy refers to the learner's ability to maintain a 'personal space' within which they can control the conditions under which personal information is shared with others (El-khatib et al, 2003). As mentioned earlier, there are several users' legitimate rights embodied within the aspect of privacy. Below is a discussion of the rights of a data subject that embody the aspect of privacy as outlined in Article 5 of EU's GDPR.

1.1 Right to Opt-in and Opt-out (Consent). Data subjects have a right to choose (opt-in) whether a data controller and data processor can collect their personal data. In essence, the data controller is expected to seek the consent of the data subject before collection, use, or disclosure of their personal data. Article 7 of EU's GDPR makes it an obligation for the data controller to demonstrate that the data subject has consented to processing of his or her personal data (EU, 2016).

In the context of a data management system, a data controller's online system should have an opt-in mechanism that seeks the data subject's consent in the form of a signed certificate to guarantee authentication and non-repudiation (El-khatib et al, 2003).

In the same vein, data subjects have the right to withdraw consent (opt-out) to processing of their personal data. Article 7 of EU's GDPR points out that the data subject has the right to withdraw his or her consent at any time (EU, 2016). As such, a data management system

should have an opt-out mechanism that facilitates the data subject to withdraw consent at will.

This study sought to establish whether Blackboard makes provision for the data subject to opt-in and out.

1.2 Right to Know How Long the Data Controller and Data Processor will Store Personal Data, and Criteria Used for Deciding the Retention Period. Article 5(e) of the EU's GDPR states that personal data shall be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The only personal data that can be kept for longer periods is that which will be processed for archiving purposes in public interest or for scientific or historical research purposes (EU, 2016).

In the context of a LMS, in keeping with this principle, students have the right to know how long the data controller (SUAD) will keep their academic and other records captured on Blackboard after they have finished their studies. Similarly, SUAD's faculty have the right to know how long personal information such as credentials within their Blackboard accounts will be retained by the system.

1.3 Right to Rectification (Correct or Update Information). Data subjects also have the right to have their personal data—in the custody of the data controller, and by extension the data processor—corrected or updated. Article 16 of EU's GDPR states the data controller is obligated to rectify any incomplete or inaccurate personal data relating to the data subject upon the subjects' request and without delay (EU, 2016).

Similarly, Article 5(d) of EU's GDPR reinforces the aspect of accuracy by noting that personal data shall be kept up to date and that every reasonable step shall be taken to ensure that personal data that is inaccurate is erased or rectified without delay (EU, 2016).

Notably, rectification here is being undertaken to ensure accuracy and completeness. This is particularly important for this study as accuracy is one of the legitimate rights identified by the contemporary ethical traditions that underpin this study.

In the context of a learning management system, the data controller and by extension the data processor, should facilitate students and faculty to easily update or correct incomplete personal data. For example, if the marital status of a student or faculty changes while they are still at the institution, their records should be updated accordingly.

El-khatib et al. (2003) identified several ways through which data controllers and processors can adhere to this principle. First, by having a mechanism within the system that requires the data subject to verify the data and sign-off on its accuracy and completeness. Second, by having functionality within the system that periodically requests the data subject to update his/ her information. And last, enabling the system to run rule-based checks on the data to identify inconsistencies.

This study sought to establish if Blackboard has mechanisms that facilitate rectification of data, and whether its privacy notice makes provision for the rectification of personal data.

1.4 Right to Be Forgotten (Erasure). Data subjects also have the right to demand their personal data to be deleted from the system. Article 17 of EU's GDPR provides that the data subject shall have the right to obtain from the controller the erasure of personal data (EU, 2016). Further, EU's GDPR provides the circumstances under which a data subject can demand their personal data be erased. These circumstances may include when the data subject withdraws consent or when data is unlawfully processed (EU, 2016).

However, the right to erasure is not absolute. There are grounds under which the data controller may fail to comply with the request for erasure; for example, if the data controller is exercising freedom of speech or some legal obligation (EU, 2016).

In the context of a LMS, students and faculty have a right to have their personal data deleted from the data systems controlled by the data controller, and by extension the data processor. This is particularly the case after a student has graduated from the learning institution and feels that their personal data should not be retained any longer by the data controller. Likewise, a member of the faculty who has retired may request their personal data to be deleted.

Notably, the right to be forgotten is particularly relevant to this study as it is consistent with other legitimate users' rights, namely the need to protect users from illegal surveillance and identity theft, and maintaining confidentiality of their personal data.

1.5 Right to Restrict Processing of Personal Data. Data subjects have the right to restrict the data controller, and by extension the data processor, from processing their personal data. Article 18 of EU's GDPR outlines the circumstances under which a data subject can restrict the processing of their personal data. This includes when the accuracy is contested as well as when the processing is unlawful (EU, 2016).

The right to restrict processing is relevant to this study as it facilitates protection of other legitimate user's rights identified in the contemporary ethical traditions. In particular, restricting the processing of personal data ensures the privacy and confidentiality of the data subject is protected, and protects the data subject from identity theft and illegal surveillance.

This study sought to establish whether Blackboard's privacy notice makes provision for users to restrict processing of their personal data.

1.6 Right to Data Portability. Data subjects have the right to have their personal data transferred to them, or to a third party of their choice, in a readable format. Article 20

of EU's GDPR provides the data subject the right to receive personal data in the custody of a given controller, and transmit it to another controller without hindrance (EU, 2016).

In the context of a LMS, if a student or faculty member requires that their personal data be transferred to another controller or processor, the learning institution is obligated to do so as long as the transfer of data does not affect the rights and freedoms of others.

Further, an education institution (data controller) may wish to transition from using one learning management system to another. Such an action would necessitate the movement of data from the old LMS to the new system. In such a case, the data processor of the old LMS is expected to facilitate the data controller's movement to a new LMS.

The aspect of data portability is particularly relevant to this study as it touches on the legitimate users' right of trust as articulated by the contemporary ethical traditions. Indeed, a data subject will only seek to transfer their personal data to a data processor that they trust.

2. Security Rights

Another important overarching legitimate users' right is security. Security embodies most of the users' legitimate rights articulated in both classical and contemporary ethical traditions. Specifically, security of data in a data management system has bearing on the ability of the data subject to access data that is accurate and authentic (trustworthy). Furthermore, appropriate security functionalities in a data management system protect the data subject from identity theft and illegal surveillance, thereby promoting users' trust in the system.

In the context of data management systems, security and privacy are inextricably linked concepts. Solove (2006) contends that in many discussions, privacy is often equated to security. However, in reality, security and privacy are distinct concepts. While you cannot

have privacy without security, you can have security without privacy. A case in point is where an organization secures its information and then makes legal but poor decisions about this information, thereby raising privacy concerns (Solove, 2006).

Understanding the interplay between security and privacy is particularly important for this study since most of the users' legitimate rights related to security have bearing on the data subject's privacy rights discussed earlier. In the context of a LMS, El-Khatib et al. (2003) describes security as ways and means for implementing data integrity and protection policies for organizations involved in e-learning.

In essence, security is considered a key aspect for a LMS to perform effectively and to be trusted by the users. Ali and Zafar (2017) reinforced the need for security in e-learning by noting there was need for institutions offering e-learning programs to adopt robust measures to protect restricted, confidential, or sensitive participant's data against loss or improper use by unauthorised users.

Below is a discussion of users' security rights that must be protected in a learning management system.

2.1 Right to Have Personal Data Processed in a Secure Manner. Data subjects have a right to have their data processed in a secure manner. Specifically, Article 5 of EU's GDPR provides that users' personal data shall be processed in a manner that ensures appropriate security including protection against accidental loss, destruction, and damage (EU, 2006). As such, GDPR obligates data controllers, and by extension data processors, to undertake appropriate technical and organizational measures that guarantee security of their data systems.

These measures include having system design features that:

- Facilitate encryption, pseudonymization and anonymity of data;

- Facilitate the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- Ensure the ongoing confidentiality, integrity, availability, and resilience of the processing system and its services (EU, 2016).

A data management system that is designed with the above-mentioned security guarantees safeguards the users' right to accuracy, security, and trust. Anonymization of data protects its confidentiality and integrity, thereby safeguarding users' privacy rights.

3. Intellectual Property Rights

As previously mentioned, use of a LMS entails the creation of content while using the system, as well as uploading content onto the system. This raises several questions related to the intellectual property rights (i.e., copyright) of the creators of content (faculty/ instructor). Specifically, the learning material created or uploaded into the LMS is a product of the work and expertise of instructors. As such, it is expected that instructors would want to protect their content from illegal use and distribution (Graf, 2002).

The need to safeguard users' intellectual property rights in LMSs is reinforced by Mason (1986) who notes that information systems should strive to protect the sanctity of intellectual property to avoid the indignities of unwittingly transferring control of knowledge from individuals to machines.

Regrettably, content creators have no control over the distribution of content after uploading it onto the LMS. Graf (2002) echoes the aspect of loss of control by noting that once content is uploaded into the system, students have an opportunity to copy and redistribute the content at will. Worse still, the collaborative nature of many LMSs makes it easy for students to share content.

There is also the question of *secondary copyright* which arises when instructors develop content from existing learning materials from other authors that are already copyrighted.

A question in this case relates to the process by which permission is obtained from the original copyright holder to use and/or adapt the material in the course.

Research Methodology

This study adopted a qualitative research approach and a case study research design. Data were collected through content analysis, document review, and interviews. First, the researcher reviewed literature on privacy, security, and intellectual property to obtain background information for the study. Review of the literature enabled the researcher to answer research question #1, which sought to identify the users' legitimate rights that need to be safeguarded in a LMS.

The researcher then conducted content analysis of Blackboard's user privacy policy to understand the various privacy and security guarantees afforded by the system. EU's GDPR "rights of the data subject" checklist was used to assess whether the Blackboard privacy policy has provisions that adequately safeguard users' legitimate rights.

Afterwards, semi-structured interviews were conducted on purposively selected respondents to understand SUAD's underlying technology architecture and its privacy and security offerings—particularly in relation to the Blackboard system. The researcher interviewed an information technology staff member at SUAD who gave insights on the information technology security arrangements that SUAD has put in place to protect users' personal information.

Finally, information obtained from the interviews was used to validate and corroborate data obtained earlier through content analysis of Blackboard's privacy policy. Further, the interviews provided details relevant in answering question three of the study and helped identify the policy gaps and technological deficiencies within the Blackboard LMS that could be undermining the protection of users' legitimate rights.

Findings and Discussion

The study revealed that LMSs are obligated to protect users' legitimate rights as provided in the EU's General Data Protection Regulations (GDPR). The data protection principles outlined in Article 5 of EU's GDPR embody most of the users' legitimate rights articulated in the classical and contemporary ethical traditions. These principles include lawfulness, fairness, and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity, and confidentiality.

Although some users' legitimate rights such as intellectual property are not articulated in the EU's GDPR data protection principles, this study ensured that they were accommodated by using contemporary ethical traditions as a complementary underpinning framework for the study. As such, users' legitimate rights that must be protected while using Blackboard include: access and accessibility, accuracy, security, trust, protection against illegal surveillance, protection against identity theft, intellectual property and copyright (World Summit on the Information Society, 2005; Kaplan & Haenlein, 2010; Mason, 1986). Furthermore, these rights are interdependent and inextricably linked to each other, and to ensure coherent analysis, they have been discussed under the broad themes of privacy, security, and intellectual property.

Below, Table 1 summarises the various users' legitimate rights that should be integrated into a learning management system. The table ranks the level of integration of the rights within Blackboard on a scale of 0–5:

- 0 No effort in integrating a particular right within Blackboard
- 1-2 Limited activity undertaken to integrate rights within Blackboard
- 3-Considerable effort towards integrating the right
- 4 Right fully integrated but with restriction
- 5- Right fully integrated without restriction

Table 1

Blackboard Scorecard for Rights that Should be Integrated into a Learning Management System

User Rights	Score 0–5*	Comments
Privacy		
Opt-in/Opt-out	5	The system has several product functionalities that allow users to opt-in or out.
Retention period and criteria	4	Data retention within Blackboard is based on SUAD retention policy as well international standards such as National Institute of standards Technology, NIST800-88 guidelines as well as Department of Defence, DOD 5220.22-M standards.
Rectify info	4	In the profile section, Blackboard allows users to edit their biodata as well as update their passwords. Rectification of certain data is based on privileges assigned by the system administrator.
Erasure	4	In the profile section, Blackboard allows users to edit or erase information on their biodata. Erasure of certain data is based on privileges assigned by the system administrator.
Restriction on processing	2	Restriction on processing of personal data only applies to users within European Union
Data portability	1	The system lacks explicit provisions on the rights of the data subject during transfer of data to another data processor or system.
Security		
Encryption, pseudonymization, anonymity of data	5	System anonymises users' personal data by removing or hashing direct identifiers such as student's name and email address. System leverages a default encryption functionality that protects against insecure storage of data.
Access to personal data in a timely manner	5	Blackboard leverages high availability cloud infrastructure that guarantees a monthly availability of 99.9%.
Intellectual Property Rights		
Safeguard users' (esp. instructors') intellectual property	2	Intention to introduce a functionality that allows learners to only read without downloading or sharing instructors' content
Safeguard subsequent use of previously copyrighted material	0	The system is silent on whether the intellectual property of the first copyright holder extend to the entire lifetime of the digital data.

*Scorecard ratings: 0 - No effort in integrating a particular right within Blackboard; 1-2 - Limited activity undertaken to integrate rights within Blackboard; 3 - Considerable effort towards integrating the right; 4 - Right fully integrated but with restriction; 5 - Right fully integrated without restriction.

Below is a detailed discussion of the users' legitimate rights and provisions within Blackboard's privacy policy that incorporate these rights.

1. Privacy Rights

1.1. Right to Opt-in and Opt-out (Consent). An analysis of Blackboard's privacy statement revealed that the LMS recognised the need for data subjects to make a choice on whether to opt-in or out of the system. The privacy statement states:

> *We offer individuals the opportunity to opt-out of personal information or to provide explicit opt-in consent for sensitive personal information being disclosed to a third party or being used for a purpose that is materially different from the purpose for which it was originally collected (Blackboard, 2020).*

The privacy statement underscores the fact that data subjects using Blackboard have the right to opt-out at any time if they feel that their personal information is being used for direct marketing purposes. Specifically, the privacy statement outlines procedures to be followed by data subjects wishing to (opt-out) unsubscribe from the system: "To exercise this right, log into your account through the services and use the designated functionality" (Blackboard, 2020).

Blackboard's mechanism for allowing users to opt in and out is particularly relevant to this study since it is consistent with Article 32 of EU's GDPR which specifies the condition of consent. Specifically, Article 32 outlines that the mechanism for consent may include:

> *A data subject ticking a box when visiting an internal website, choosing technical settings for information society services or another statement or conduct which clearly indicates the data subject's acceptance of the proposed processing of their personal data (EU, 2016).*

For example, Blackboard's privacy settings provide an option to users' to give permission on the visibility of their personal data. Specifically, users' can enable or disable the visibility of their mobile number, email address, profile picture, emergency contact and date of birth.

Likewise, students using Blackboard*'s Mobile Learn App*, now just *Blackboard App*, version 6.12.0 are required to grant the system permission to access the contacts list on their mobile device. This enables the system to match the students' contacts to users in *Blackboard Learn* and display their photo from the users' contact list in discussion boards.

In the same vein, users using *Blackboard Mobile App* are required to give consent by asking them to enable location data to enable the system to collect information relating to their location from their device.

To maintain evidence of consent granted, the system maintains logs that cannot be modified. This guarantees authentication and non-repudiation.

1.2 Right to Know How Long the Data Controller and Data Processor will Store Personal Data, and Criteria Used for Deciding the Retention Period. Besides knowing the personal information that is in the custody of the learning management system and how it is being used, students and faculty members also have the right to know how long the data processor will store their data, and the criteria that informs the retention period.

The right to know the retention period is relevant to this study since it is consistent with the principle of storage limitation that is articulated in Article 5 of EU's GDPR. The aspect of storage limitation is critical in the protection of other legitimate rights such as right against predatory practices; e.g., illegal surveillance. In this case, when personal information is stored more than is necessary, it is prone to misuse and may be used for tracking and monitoring data subjects.

The study revealed that there is no clause within Blackboard's privacy statement that explicitly addresses the aspect of storage limitation. Perhaps the expectation from Blackboard is that users' can obtain this information from their respective educational institutions or data controllers as the privacy policy has an overriding statement that advises users', "Contact your institution to exercise your rights" (Blackboard, 2020).

A follow-up with the IT staff from SUAD on this issue revealed that SUAD's IT system keeps student information for up to eight semesters after which the data can be destroyed (Alabsi, Khader, personal communication, June 2021).

Further, on the question of the retention period, the IT staff noted that Blackboard has granted SUAD freedom to destroy any data on request based on National Institute of standards Technology, NIST800-88 Guidelines for Media Sanitization (http://dx.doi.org/10.6028/NIST.SP.800-88r1) as well as the Department of Defense, DOD 5220.22-M wipe standard.

1.3 Right to Rectification (Correct or Update Incorrect or Incomplete Information). In the context of a LMS, some of the personal information that may need to be corrected or updated includes a student's name (e.g., after marriage), or a student's contact details such as phone number and postal address. Analysis of Blackboard's privacy statement revealed that the privacy notice acknowledges that users of the LMS have the right to rectify their personal data held by the system. The privacy statement states: "In many of our products, you have the right to rectification of personal information we hold about you…You will be able to change some of the information yourself by logging into your account" (Blackboard, 2020).

Blackboard has a functionality that allows the user to update their password when need arises.

Likewise, in the profile section, Blackboard allows users to edit their biodata. This includes information relating to their email address, mobile number, nationality, gender, date of birth, and education. However, the privileges on what information a user is allowed to rectify lies with the system administrator.

1.4 Right to Be Forgotten (Erasure). Users of learning management systems also have the right to have their personal information held by the system erased or deleted, particularly when it is no longer needed. For instance, students that have completed their studies in a given educational institution may prefer to have their personal details deleted or erased from the institution's data management systems. Similarly, an instructor or faculty member that has retired or left the educational institution may wish to have any personal information held by the institution deleted or erased from the institution's databases.

Analysis of the privacy statement revealed that Blackboard recognises that its users have the right to be forgotten or to have their personal information erased from its databases.

Specifically, Blackboard's privacy statement states that:

> *In many jurisdictions, you may have the right to erasure of personal information we hold about you…In many of our products, you will be able to delete some of the information yourself by logging into your account (Blackboard, 2020).*

As mentioned earlier, within the profile section, the system has a functionality that allows users to edit or erase their biodata. However, users' have no absolute control on the erasure of their data from the system. The privilege on what data users can erase from the system is assigned by the system administrator.

The privacy statement explains what a data subject should do if they are unable to delete their personal information held in Blackboard's databases. Essentially, the notice advises users of Blackboard's products and services to contact their respective educational institution (data controller) to exercise their rights (Blackboard, 2020).

1.5 Right to Restrict Processing of Personal Data. An analysis of the privacy notice revealed that Blackboard recognises that its users have the right to restrict the processing of their data held in the system. Specifically, the privacy notice states: "In the European Union, you also may have the right to object to or restrict certain types of use of your personal information" (Blackboard, 2020). This implies that students at SUAD may not have the privilege to restrict the processing of their personal information as they are not within the European Union. Accordingly, there is need for SUAD's privacy policy to elaborate on the mechanisms put in place to safeguard students' right to restrict processing of their personal data.

1.6 Right to Data Portability. On the right to portability, it emerged that Blackboard's privacy notice has not explicitly addressed the right of the data subject to transfer his or her personal data to another data processor or system. Instead, the privacy notice lays emphasis on transfer of personal data to locations outside the data subject's country. In particular, the privacy notice provides assurances that users' data will be protected while being transferred from one location to another. In terms of system technical capabilities, the study revealed that Blackboard supports both big bang and phased approaches to data migration. Specifically, the system allows archiving of all courses and their contents after which it permits them to be exported to the new system.

2. Security Rights

2.1 Right to Have Personal Data Processed in a Secure Manner. The study found that Blackboard's privacy notice acknowledged the need for users' data to be secured. In particular, the notice states:

> *We employ a variety of physical, administrative, and technological safeguards designed to protect personal information against loss, misuse and unauthorised access or disclosure. We have dedicated information security programs and work hard to continuously enhance our technical and operational security measures (Blackboard, 2020).*

The study found that some of the technical measures within Blackboard that are meant to guarantee security of personal information include data encryption, firewalls, data use and access limitations, as well as physical access controls (Blackboard, 2020). This information was corroborated by SUAD IT staff who noted that: "The system is secure; it is able to undertake vulnerability assessments to identify any potential security threats."

Notably, Blackboard has also undertaken technical and organizational measures to adhere to the principle of data minimisation. Specifically, the system maintains secure logs of its data collection that acts as evidence of its data collection patterns. In essence, the system limits itself to only collecting data that is required to fulfil its purpose.

Similarly, Blackboard anonymises users' personal data by removing or hashing direct identifiers such as student's name and email address, and devise identity from the data set prior to using it to carry out research and analysis (Blackboard, 2020).

Further, a review of literature revealed that users of e-learning management systems are susceptible to numerous security risks associated with the architecture of the system.

These include:

- Broken authentication and session management;
- Interception of their data while on transit over an unsecured network;
- Inability to access the system due to denial of service;
- Breach of confidentiality due to insecure cryptographic storage and insecure direct object reference;
- Leakage of information;
- Attack on the integrity of data prompted by buffer overflow, cross site request forgery, cross site scripting, injection flaws and malicious file execution (Dutta et al, 2011; Stapić et al, 2008).

The findings show that Blackboard guarantees the security of personal data against the above-mentioned risks through:

- An authentication framework that ensures users can only access the system using their username and password;
- Role-based access controls based on a "least privilege default deny access control" policy; This means restricting access rights for users to only those resources absolutely required to perform routine and lawful activities.
- Default encryption functionality that protects against insecure data storage;
- Compliance with international security standards such as ISO 9001 and ISO 27001;
- Use of a single sign on method that leverages token authentication to ensure users credentials and data are not shared;
- Permission/ entitlement checking that ensures that users can only make changes to data based on the permissions assigned to them;
- Session expiration capability where sessions automatically expire after a user has been idle beyond a programmed duration;
- Session fingerprinting which can detect when a user session has been hijacked by a malicious attacker.

3. Intellectual Property Rights

While Blackboard's privacy notice acknowledges that content is uploaded on to the system and created through chat messages, the notice is silent on how distribution of the uploaded content can be controlled to protect the intellectual property rights of the creators. Similarly, and regrettably, SUAD lacks a privacy policy that stipulates how previously copyrighted material should be adapted into a course. However, an interview with SUAD's IT staff revealed that: "We are in the process of coming up with a functionality that will ensure that content created and uploaded on Blackboard is in encrypted form such that students can only read it but cannot download or share it."

A common way of safeguarding Intellectual property within LMSs is extending the control of the copyright holder to the entire lifetime of the digital data (Graf 2002).

This entails the use of encryption technology known as CIPRESS (Cryptographic Intellectual Property Rights Enforcement System). The defining feature of this technology is that it prevents illegal distribution of downloaded material and allows monitoring of the usage of documents. In essence, all data is stored in encrypted form on a storage device of a client computer. This means that whenever a document is accessed it must be decrypted. However, this technology ensures that this decryption is only temporary such that the decrypted data of a document only exists in the virtual memory section of the computer. Once the document is saved to a storage device, it is encrypted again. The main point here is that CIPRESS does not reuse the encryption key but creates a new personalized key specific to the document whenever the document is written (Graf 2002).

In the context of an LMS, the student can access learning material only if he/she has authenticated themselves against the CIPRESS system and been provided with the key required to decrypt the learning material. Notably, this key retrieval is not a one-off affair

but a feature that is performed every time the learning material is being delivered to the student, that is, with every access to the learning material. This means that in a CIPRESS environment, students cannot manipulate the Key centre ensuring that only legitimate users are able to use the learning material. This allows instructors to safely include sensitive or confidential learning material.

Similarly, if an intruder happens to steal the learning material or the disk containing the learning material all he gets is encrypted data. To view the content, he/she would need a key from the key centre.

In terms of preventing illicit re-distribution of learning material, if a legitimate student forwards learning material to a different student, the data will be in encrypted form meaning that the other student will only be able to view the content if the Key centre delivers the appropriate keys. As such, in a CIPRESS environment, redistribution of learning material is controlled since the keys used are specific for every combination of document and a student cannot re-use the keys of another student. This combination of re-encryption and watermarking ensures that access control does not end once the material is distributed to the student. Instead, CIPRESS technology ensures access control is extended to the entire lifespan of the learning material (Graf 2002).

Conclusion

The study revealed that to a large extent Blackboard's privacy notice makes provisions for the fulfilment of most of user's legitimate rights outlined in the classical and contemporary ethical traditions as well as EU's GDPR. However, the privacy notice is silent on key users' legitimate rights such as data subjects' right to data portability, storage limitation, and intellectual property rights of the content creators.

More importantly, the issue emerged that as a data processor, Blackboard's privacy practices are largely informed by the privacy practices of the educational institution (data controller) in this case, SUAD. As such, Blackboard manages students' and faculty members' personal information based on the privacy agreement stipulated to it by the data controller. This means that SUAD has to formulate a robust privacy policy as a first step towards effective protection of users' legitimate rights on Blackboard LMS. Accordingly, this study concludes that safeguarding user legitimate rights is a joint responsibility between data controllers (educational institutions) and data processors (LMS service providers). On one hand, data controllers are obliged to formulate robust data protection regimes that will underpin the privacy practices adopted by LMS service providers. Likewise, data processors are obliged to adopt privacy practices that embody all the data protection principles as outlined in the global data protection standard, GDPR.

Overall, the study has demonstrated that achieving a robust privacy and security-preserving LMS calls for a multi-pronged approach. First, a policy-based approach where the LMS vendor displays a clear and elaborate privacy notice with easily accessible links thereby complying with the principle of transparency. Second, a privacy-by-design approach where privacy and security aspects such as storage limitation and data minimization are realised by embedding privacy and security through design functionalities on LMSs. Third, a trust and audit approach that entails developing LMSs that generate digital certificates and data logs, thereby ensuring existence of a secured record of transactions thus complying with principles of accountability and purpose limitation.

References

Alabsi, K. (2021) Personal communication.

Ali, R. & Zafar, H. (2017). A security and privacy framework for e-Learning. *International Journal for e-learning security (IJeLS), 7*(2). https://digitalcommons.kennesaw.edu/facpubs/4137

Banisar, D. & Davies, S. (1999). Global trends in privacy protection: An international survey of privacy, data protection and surveillance laws and developments. *John Marshall Journal of Computer and Information Law, 18*(1). https://repository.law.uic.edu/jitpl/vol18/iss1/1/

Blackboard Corporation (2020). Blackboard privacy policy; Blackboard terms of use | Blackboard Help. https://help.blackboard.com/Terms_of_Use

Boyd, D. (2007). Why youth (heart) social networking sites: The role of networked publics in teenage social life. In D. Buckingham (Ed.). *Youth, identity and social media* (pp. 119–142). MIT Press.

Capurro, R. (2010). Global intercultural information ethics from an African perspective. Keynote address presented at the Second African Information Ethics Conference, University of Botswana, Gaborone, 6–7 September.

Dutta, A. K., Mosley, A. A., & Akhtar, M. M. (2011). E-learning in higher education: Design and implementation. *International Journal of Computer Science Issues (IJCSI), 8*(4), 509. http://www.ijcsi.org/articles/E-learning-in-Higher-Education-Design-and-Implementation.php

El-Khatib, K., Korba, L., Xu, Y. & Yee, G. (2003). Privacy and security in e-learning. *International Journal of Distant Education, 1*(4), 1–19. http://doi.org/10.4018/jdet.2003100101

European Union (EU). (2016). General Data Protection Regulations: Art. 5 GDPR - Principles relating to processing of personal data. Proton Technologies AG. https://gdpr.eu/article-5-how-to-process-personal-data/

Giles, D. (2006). Constructing identities in cyberspace: The case of eating disorders. *British Journal of Social Psychology 45*(3), 463–477. https://doi.org/10.1348/014466605X53596

Graf, F. (2002). Providing security for eLearning. *Computers & Graphics, 26*(2), 355–365. https://doi.org/10.1016/S0097-8493(02)00062-6

International Organisation Standard (ISO) 9000. (2015). Quality Management Systems. Available at: https://www.iso.org/iso-9001-quality-management.html

International Organisation Standard, ISO/IEC 27001. (2018). Information Security Management. Available at: https://www.iso.org/isoiec-27001-information-security.html

Kaplan, A. & Haenlein, M. (2010). Users of the world unite: The challenges and opportunities of social media. *Business Horizons, 53*(1), 59–68. https://doi.org/10.1016/j.bushor.2009.09.003

Mason, R. (1986). Four ethical issues of the information age. *Management Information Systems (MIS) Quarterly, 10*(1), 5–12. https://doi.org/10.2307/248873

Mutula, S. (2013). Policy gaps and technological deficiencies in social networking environments: Implications for information sharing. *South Africa Journal of Information Management 15*(1). https://doi.org/10.4102/sajim.v15i1.542

Office of the High Commissioner for Human Rights (OHCHR). (1966). International covenant on civil and political rights (ICCPR). United Nations. http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

Solove, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review, 154*(3), 477 https://scholarship.law.upenn.edu/penn_law_review/vol154/iss3/1

Stapić, Z., Orehovacki, T. & Danié, M. (2008). Determination of optimal security settings for LMS Moodle. Proceedings of 31st MIPRO International Convention on Information Systems Security, *vol. 5*, Opatija, 2008, 84–89. https://www.researchgate.net/publication/224930654_Determination_of_optimal_security_settings_for_LMS_Moodle

Subramanian, P., Zainuddin, N., Alatawi, S., Jarabdeh, T. & Che Hussin, A. (2014). A study of comparison between Moodle and Blackboard based on case studies for better LMS. *Journal of Information Systems Research and Innovation (6)*. https://seminar.utmspace.edu.my/jisri/Volume6.html

United Nations General Assembly. (1948, 10 December). Resolution adopted by the General Assembly, 217 (III). International Bill of Human Rights. 183rd Plenary Meeting (Geneva: United Nations, 71–9. http://www.un-documents.net/a3r217.htm

World Summit on the Information Society (WSIS) (2005). Plan of action: C10. Ethical dimensions of the information society. International Telecommunication Union (ITU). http://www.itu.int/wsis/docs/geneva/official/poa.html#c10

Author

Victor Kabata is a post-doctoral researcher at Sorbonne University, Abu Dhabi.

He is currently engaged in teaching and mentoring Master's and Bachelor's students in the records management and Archival science program within the Department of History. He is also engaged in research aimed at improving the status of public records and archives management in the United Arab Emirates. In this regard, his research interests include records and archives management; information for development; data protection and privacy. He can be reached at victor.kabata@sorbonne.ae.