Жамият ва инновациялар –
Общество и инновации –
Society and innovations
Journal home page:
https://inscience.uz/index.php/socinov/index

Privacy consideration in design and use of online admissions software in higher education

Aigul Kantoro Kyzy[1] **Ammar Younas**[2]

University of Alberta, Tashkent State University of Law

ARTICLE INFO

Article history:
Received August 2022
Received in revised form
20 August 2022
Accepted 25 September 2022
Available online
25 October 2022

Keywords:
Online Admission Software, Privacy, Data Protection, Rights, GDPR

ABSTRACT

Higher Education institutes, all over the world are recruiting students by allowing them to apply through online system. The aim is to make admission process easier because there are many students come from other cities, even abroad. Most of higher education institutions believe that students who have grown up using digital technologies ("digital natives") have little concern for privacy of their data. This paper argues that “privacy” and “Right” are well established norms in all major jurisdictions and are keys to ensuring human dignity, safety and self-determination. Therefore, students’ personal data collected via online admission systems and its protection requires a holistic approach to system design and its use that incorporates a combination of legal, administrative, and technical safeguards.

DOI: https://doi.org/10.47689/2181-1415-vol3-iss9/S-pp62-69

Соблюдение конфиденциальности при разработке и использовании программного обеспечения для онлайн-приема в высшее образование

Калит сўзлар:
Программное обеспечение для онлайн-доступа, конфиденциальность, защита данных, права, Генеральный регламент о

АННОТАЦИЯ

Высшие учебные заведения по всему миру набирают студентов, позволяя им подавать заявки через онлайн-систему. Цель состоит в том, чтобы облегчить процесс поступления, потому что многие студенты приезжают из других городов, и даже из-за рубежа. Большинство высших учебных заведений считают, что студенты, выросшие с

[1] MA Student, Department of Media and Technology Studies, University of Alberta, Canada
Email: aigul.kantoro@gmail.com
[2] Lecturer (Highly Qualified Specialist), Department of Business Law, Tashkent State University of Law, Uzbekistan
Email: doctorammaryounas@gmail.com

защите персональных данных (GDPR)	использованием цифровых технологий («цифровые аборигены»), мало заботятся о конфиденциальности своих данных. В этом документе утверждается, что «неприкосновенность частной жизни» и «Право» являются устоявшимися нормами во всех основных юрисдикциях и являются ключом к обеспечению человеческого достоинства, безопасности и самоопределения. Таким образом, персональные данные студентов, собираемые с помощью систем онлайн-приема, и их защита требуют целостного подхода к проектированию системы и ее использованию, который включает в себя сочетание правовых, административных и технических гарантий.

Acknowledgement of the "Privacy" and the "Right"

The Oxford English Dictionary (2022) entry for "privacy" defines the term as "state or condition of being alone, undisturbed, or free from public attention, interference or intrusion". The Dictionary dates the creation of word "privacy" in English in circa 1500s (Oxford English Dictionary, 2022). The etymological roots of the term come from Latin word 'privatus' with its meaning "apart from the State, peculiar to oneself, of or belonging to an individual, private" (Engelhardt, 2000). Within the years scope of terminology have captured numerous aspects including social, political, legal, psychological, philosophical and religious.

The initial acknowledged claim for a "right to privacy" in 1890 lies in an article on *The Right to Privacy* published by Samuel Warren and Louis Brandeis (1890). The article demands legal recognition of "the right to privacy, as a part of more general right to the immunity of the person - the right to one's personality" (Warren & Brandeis, 1890). The work provided encouragement for development of consequences during privacy invasion cases. Two lawyers outlined the necessity of re-defining common principle of law of having full protection in person and property. The work of Warren and Brandeis is a response to underlying changes brought by press and photography, also known as "yellow journalism" (p. 193). The major concern of authors was over impreciseness and ethical issues of the press and its influence on "sacred precincts of private and domestic life" (p. 195). Two authors point to the work of E. L. Godkin (1890) "The Rights of the Citizen: To his Reputation" that demands amendments and reconsiderations to allow "each member in a greater or less degree enjoy the confidence and good opinion of his fellows". The article proposed law as one tool to address privacy issues in the United States. In 1881, the Supreme Court of Michigan recognized a certain level of privacy in a case where a woman giving birth had an unauthorized man enter the room with her doctor (Danielson, 1999). After publication of the article, Supreme Court of Georgia held that unauthorized use of a person's photo for an advertisement constituted it as a breach of privacy (Pavesich, 1905). The law intended to embrace privacy rights in the twentieth century with the 1939 Restatement of Torts including privacy torts, and in 1977 the American Law Institute included four classic privacy cases in its Restatement (Second) of Torts (Park & Kaye, 2020). The Warren and Brandeis article bears historical importance as the forerunner of privacy rights recognition.

In late 1880s, Judge Thomas Cooley (1888) proclaimed that people had a right "to be let alone". Following these developments in 1965 the privacy was enunciated as a

constitutional right in the United States. In Griswold v. Connecticut, Justice William O. Douglas placed a right to privacy in a "penumbra" (shadow) cast by the First, Third, Fourth, Fifth and Ninth Amendments (Clark, 1974). The decision of the Court covered only one dimension of privacy. But Griswold "allowed Americans to imagine more robust applications of the 'right to be let alone'" (Igo, 2018).

In 1948, the United Nations General Assembly adopted the Universal Declaration of Human Rights (UDHR) that guarantees individual rights of everyone (United Nations, 2022). The United Nations (2022) statement accepted as the most relevant to privacy rights determines that:

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of law against such interference or attacks."

The European Union developed more broad privacy protection laws. From the beginning of the 1980s the non-binding OECD (2022) privacy Guidelines, and the first international agreement, the Council of Europe (CoE) data protection Convention (Council of Europe, 1981) established privacy principles. The Directive included stronger protection requirements along with establishment of impartial entity, Data Protection Authority (DPA). The international document sets "the strongest standard for data privacy" (Council of Europe, 1981). In 1995 the European Communities adopted the Data Protection Directive (DPD) (Wolters, 2017) to systematize European data protection system. The DPD required data protection laws for all member states. It also included rules about transfer of information to non-EU countries that put pressure on other countries to create data protection legislation. The latest significant legislation is General Data Protection Regulation (GDPR) adopted in 2016 (GDPR.eu, 2022).

The GDPR covers personal information - name, contact details, computer location, and identification data such as race and sexual orientation. The GDPR requests from organizations lawful justification for holding data and secure storage of it. The companies need to possess individual's consent to store information including name and email address on their system. The potential penalties for failure to comply with GDPR for businesses include up to two percent of a company annual turnover in fines (GDPR.eu, 2022). The GDPR is a significant legislation to protect individuals who give companies their data. The companies need to be considered about manipulative questions while asking for individual's consent to store information. Similarly in case of clients' data being hacked, the company is responsible of notifying clients about incident within three days. The GDPR (2022) ensures "right of access" where people can see what information companies are storing on them. Along with the "right to be forgotten" (GDPR.eu, 2022) in several cases people can demand their data erased. The companies operating in EU countries must bring their practices into compliance with the GDPR along with organisations based outside of Europe who store data of EU citizens.

A new approach in data protection provides an opportunity for companies to rebuild trust with their customers after numerous cases of misuse of data. For instance, the Cambridge Analytica and Facebook's acquisitions of using illegally collected data and its further manipulation that influenced on elections in the USA (Timberg & Romm, 2021). According to Timbers and Romm (2021) Mark Zuckerberg's response to the Cambridge Analytica scandal was - "We did not take a broad enough view of our responsibility, and that was a big mistake. And it was my mistake. And I am sorry."

Recent developments in technology have created information explosion to the society. Nowadays, almost every part of individual's life can be digitized, tracked, and logged - every photo, journey, purchase, and hobbies. This leads to large data collection, more and more data is collected and stored. The privacy concerns go beyond the nineteenth century's privacy comprehension. The privacy is a new realm filled with tensions and trade-offs accompanied with significant consequences for individuals and governments.

Peculiarities of the Online Admission Software

One of the aspects of privacy is privacy of applicants during enrolment and admissions process. The enrolment and admissions process in higher education has shifted into digitalized format accepting submissions from applicants across the globe. Due to unforeseen situation caused by COVID-19 universities had to admit students online using admissions software. The online admissions process approach accompanies strengths and limitations to ensure placement without compromising the privacy of applicants. The process requires submission of personally identifying information in online environment. The educational institutions have to use intrusive software to ensure education integrity and its fair access. The question of privacy has been compromised to provide equal access to education guaranteed by the UN Human Rights Declaration. The Article 26 of it outlines that "Everyone has the right to education. Technical and professional education shall be made generally available and higher education shall be equally accessible to all on the basis of merit" (United Nations, 2022).

Admissions and enrollment management software is a tool that assists universities to manage student admissions and enrollment process including accepting applications and processing application fees. Admissions software include marketing features providing ability to maintain communication with potential applicants. In other words, admissions software replicates customer relationship management software (CRM) software (Salesforce.org, 2022). The CRM records interactions between business and its potential and existing customers. The integrated admissions software contains marketing outreach, online forms design, application, and payment processing along with campus tour and interview scheduling functionalities. Some software also includes analytics and data integration tools. The admissions software integrates with student information systems to streamline the sharing of student data collected during admissions process with tools used during their tenure at school. In order to qualify for inclusion in admission management, the admissions software must meet the following criteria:

- Be modelled with a particular purpose for school admissions use
- Include student application management
- Have email marketing, scheduling, and application progress tracking functions
- Accept and process application payments

The Salesforce.org Education Cloud is one of the CRM platforms used by universities including USC, Stanford, Purdue, Rutgers, Michigan State, UPenn, and Notre Dame (Belland, 2021). It was developed in 1999 by four people in San Francisco as the cloud CRM with all software hosted on the Internet and subscription services for its clients (Salesforce.org). Within education cloud it offers admissions and enrollment product. Admissions Connect was developed in partnership with Education Data Architecture (EDA), data architecture aimed to configure Salesforce.org for education. EDA is a standardized and dependable framework for admissions and enrollment, education history and test scores

(Salesforce.org). Salesforce.org claims to store data in “All in one trusted place”. It displays the TrustArc (2022) Privacy Verified seal. It proves that company meets requirements of EU-U.S. Privacy Shield and/ or Swiss-U.S. Privacy Shield (TrustArc, 2022).

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were developed by the U.S. Department of Commerce and the European Union Commission and Swiss Administration to establish compliance system with data protection requirements during personal data transfer from European Union and Switzerland to the United States. It is voluntary to join the Privacy Shield Framework. The commitment to act in accordance with the Privacy Shield Framework is enforceable under U.S. law. The Federal Trade Commission (Privacy Shield Framework), the Department of Transportation or another statutory body control the organization compliance with the Privacy Shield Framework (p. 2). The Department of Commerce maintains and announces an authoritative list of U.S. organizations and their commitment to follow Principles (Privacy Shield Framework). The Department has authority:

“To remove an organization from the Privacy Shield List if it withdraws voluntarily from the Privacy Shield of if it fails to complete its annual re-certification to the Department. An organization removal from the Privacy Shield List means it may no longer benefit from the adequacy decision of European Commission to receive personal information from the EU. The organization must continue to apply the principles to personal information it received while it participated in Privacy Shield and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide “adequate” protection for information by another authorized means. The Department will also remove from the Privacy Shield List those organization that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete personal information they received under the Privacy Shield.” (Privacy Shield Framework).

The platform collects personal data including name and surname, year of birth, country of birth, government issued passport data, mailing address, information about parents/ guardians (name and surname, age, and their occupation along with phone number), contact information. The data collected and stored within platform with further usage in analytics. The Salesforce.org collects all this and other university program related information in a form of submissions within platform. The application process is maintained only by submission of documents including motivation and reference letters along with language and subject test scores. In other words, the application process does not include synchronous video-streaming examination part. However, there are universities that contain examination part that is managed by admissions software with synchronous video-streaming tools. The Eklavvya is one of the admissions software used for synchronous video-streaming examination. It helps educational institutions with managing all administrative and academic tasks in integrated system. The software was developed and managed by IT company from India, Splashgain Technology Solutions in 2009. The company serves across fifteen countries with its headquarters located in India, United States of America, and United Arab Emirates. The focus areas of expertise include education technology in remote proctoring, AI proctoring and digital assessments.

In 2013 the company has been certified for Information Security Management System - ISO/IEC 27001: 2013. ISO (2022) 27001 is an international standard that proves

company's management of information security. It defines requirements for an Information Security Management System (ISMS). According to the Certification Europe (2022) outlines the standard procedure for "establishing, implementing, operating, monitoring, maintaining, and improving company's ISMS". The ISO 27001 standard and ISMS present framework for information security management to assist organizations with:

- Secure storage of confidential information
- Effective risk management of information security and potential security threats including cybercrime, personal data breaches, vandalism/ terrorism, misuse/ theft, viral attack, etc.
- Legal compliance with other regulations such as European Union General Data Protection Regulation (EU GDPR)

The Eklavvya collects personal information about applicants like the Salesforce.org. Although applicants submit all required information, the software requires to showcase government issued identification card during the synchronous video-streaming examination to prove identity. For proctored exams the software collects video/ audio streaming, screen sharing, geolocation data, audio/ visual and biometric information (Eklavvya, 2022). For online video-streaming examination Eklavvya requires exam takers to download its secured browser that will be used during the test. Applicants provided with username and password to log into the system. Once applicants log into the system of Eklavvya, they can review details of online examination developed by the university. To proceed with taking exam, applicants are expected to verify identity by giving permission to access web camera. Then the system requires to present identification card in front of screen for web camera. To prevent cheating and plagiarism, the system will record identification card. In the next step the system requires applicants to capture photograph of the applicant. Once identity verification is completed, the applicant may begin the examination. The exam taker's activities are recorded and remote exam invigilator monitors activities throughout the whole examination time using AI based auto proctoring (Eklavvya, 2022). AI proctor checks whether computer camera is at eye-level. It detects background noises including human voice, music, environmental sounds. AI proctor controls whether applicant's face within middle of the computer screen throughout the examination period. After three instances of the system not detecting applicant's face or hearing background noises the examination will automatically end.

Summary

Having investigated couple of admissions software, we may conclude that online enrolment process can be one of the methods to leverage technology. There are 31.097 universities in the world (Ranking Web of Universities, 2021). The higher education benefits not only an individual but society in general. It provides adequate job skills and prepares individuals to be active members of their communities and societies. There are around 220 million students in the world (The World Bank, 2021). The World Bank reports economic returns for higher education graduates are the highest in entire educational system – 17 % increase in earnings while with 10 % for primary and 7 % for secondary education (Montenegro & Patrinos, 2014). According to Montenegro and Patrinos (2014) these high returns are even greater in Sub-Saharan Africa, 21 % increase in earnings for higher education graduates.

The enrolment and admissions process must happen in lawful, transparent, and fair manner that ensures security and data collection that is reduced to minimum necessary in relation to processing purpose. To ensure data privacy of applicants and maintain institution status and compliance with regional and local legislation universities are using admissions software with data privacy protection. Similarly, enrolment and admissions software developing companies are focusing on data privacy and attempting to comply with legislation and secure personal information management. The higher education is facing new developments along with public policy that must keep abreast of new concerns in digital world. Data privacy is one of aspects that has emerged with the spread of internet, technology, and innovation. It encompasses all aspects of society activities and entails related vital consequences. The admissions process had plagiarism and cheating cases in smaller cases earlier during paper-based admissions. Now we observe entangled data entry points that create our personal profile in financial and educational institutions, our job places and service organizations. The data is new value that must be stored and managed securely to ensure individual's digital security.

References

1. Belland, J. (2021, June 25). *Colleges & Universities choose Salesforce to accelerate advancement roi*. Salesforce.org. Retrieved September 2, 2022, from http://www.salesforce.org/blog/higher-ed-advancement/

2. Certification Europe. (2022, July 28). *ISO 27001*. Certification Europe. Retrieved September 23, 2022, from http://www.certificationeurope.com/certification/iso-27001-information-security/

3. Clark, R. H. (1974). Constitutional sources of the penumbral right to privacy. *Villanova Law Review*, 19, 833–884

4. Cooley, T. M. (1888). *A treatise on the law of torts, or, the wrongs which arise independent of contract* (2nd ed.). Callaghan

5. Council of Europe: Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. (1981). *International Legal Materials*, 20(2), 317-325. doi:10.1017/S0020782900032873

6. Danielson, C. (1999). The Gender of Privacy and the Embodied Self: Examining the Origins of the Right to Privacy in U.S. Law. *Feminist Studies*, *25*(2), 311–344. https://doi.org/10.2307/3178682

7. Eklavvya. (2022, September 22). *Highly reputed online assessment tool*. Eklavvya. Retrieved September 23, 2022, from http://www.eklavvya.com/

8. Engelhardt, H. (2000). Privacy and Limited Democracy: The Moral Centrality of Persons. *Social Philosophy and Policy, 17*(2), 120-140. doi:10.1017/S0265052500002132

9. GDPR.eu. (2022). *GDPR Archives*. GDPR.eu. Retrieved September 22, 2022, from https://gdpr.eu/tag/gdpr/

10. Godkin, E. L. (1890). The Rights of the Citizen, IV—To His Own Reputation. *Scribner's Magazine*, 8(1), 58-67

11. Igo, S. E. (2018). *The Known Citizen: A History of Privacy in Modern America*. Harvard University Press. http://www.jstor.org/stable/j.ctv24w653v

12. ISO. (2022, May 30). *ISO/IEC 27001:2013*. ISO. Retrieved September 23, 2022, from http://www.iso.org/standard/54534.html

13. McStay, A. (2017). *Privacy and the media* (First edition.). SAGE Publications

14. Montenegro, C. E., & Patrinos, H. A. (2014). Comparable estimates of returns to schooling around the world. *World Bank policy research working paper*, (7020)

15. Myers, C. (2020). Warren, Samuel & Louis Brandeis. The Right to Privacy, 4 Harv. L. Rev. 193 (1890). *Communication Law and Policy*, 25(4), 519–522

16. OECD. (2022). OECD. Retrieved September 22, 2022, from https://www.oecd.org/

17. Oxford English Dictionary. (2022). *Discover the story of English more than 600,000 words, over a thousand years*. Home: Oxford English Dictionary. Retrieved August 22, 2022, from https://www.oed.com/

18. Park, C. S., & Kaye, B. K. (2020). What's This? Incidental Exposure to News on Social Media, News-Finds-Me Perception, News Efficacy, and News Consumption. *Mass Communication & Society, 23(2)*, 157–180. https://doi-org.login.ezproxy.library.ualberta.ca/10.1080/15205436.2019.1702216

19. Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905)

20. Privacy Shield Framework. (n.d.). *Privacy shield overview*. Privacy Shield Program Overview | Privacy Shield. Retrieved September 23, 2022, from https://www.privacyshield.gov/Program-Overview

21. Ranking Web of Universities. (2021). *Countries arranged by number of universities in top ranks*. Countries arranged by Number of Universities in Top Ranks | Ranking Web of Universities: Webometrics ranks 30000 institutions. Retrieved September 23, 2022, from http://www.webometrics.info/en/distribution_by_country

22. *Restatement of torts: tentative draft.* (1925). American Law Institute

23. Salesforce.org. (n.d.). *Our story*. Salesforce.com. Retrieved September 23, 2022, from http://www.salesforce.com/company/our-story/?d=70130000000i80N

24. Salesforce.org. (2022, August 10). *What is a CRM?* Salesforce.org. Retrieved September 2, 2022, from https://www.salesforce.org/blog/what-is-a-crm/

25. The World Bank. (2021). *Tertiary education*. World Bank. Retrieved September 23, 2022, from http://www.worldbank.org/en/topic/tertiaryeducation#1

26. Timberg, C., & Romm, T. (2021, December 5). *Facebook CEO Mark Zuckerberg to Capitol Hill: 'it was my mistake, and I'm sorry.'*. The Washington Post. Retrieved September 22, 2022, from https://www.washingtonpost.com/news/the-switch/wp/2018/04/09/facebook-chief-executive-mark-zuckerberg-to-captiol-hill-it-was-my-mistake-and-im-sorry/

27. TrustArc. (2022, September 20). *TRUSTARC the leader in privacy management software*. TrustArc The Leader in Privacy Management Software. Retrieved September 23, 2022, from https://trustarc.com/

28. United Nations. (2022). *Universal declaration of human rights*. United Nations. Retrieved September 22, 2022, from http://www.un.org/en/about-us/universal-declaration-of-human-rights

29. Warren, S., & Brandeis, L. (1890). *Warren, Samuel & Louis Brandeis. the right to privacy, 4 Harv. L. rev. 193 (1890)*. Taylor & Francis. Retrieved August 22, 2022, from https://www.tandfonline.com/doi/abs/10.1080/10811680.2020.1805984

30. Wolters, P. T. J. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility? *International Data Privacy Law*, 7(3), 165-178