International Working Group
on Data Protection
in Telecommunications

675.54.9

Working Paper on E-Learning Platforms[1]

61st Meeting, 24-25 April 2017, Washington D.C. (USA)

Introduction

1. In many countries, the use of e-learning platforms has become increasingly popular. E-learning platforms typically enable the creation of "virtual classrooms" where teachers can distribute learning materials and conduct tests. Additionally, many of these platforms facilitate collaborative learning and allow students and teachers to communicate with each other. As these platforms become embedded in the curriculum, their use is becoming commonplace.

2. Until recently, student performance assessment and related data collection was mostly limited to test results and attendance. The use of e-learning platforms, however, has led to an increase in the amount of personal data available about students. These data range from information about the way electronic teaching materials are used and how tasks are fulfilled (e.g., the time invested or needed for viewing and reading them), to class participation and other educational activities (e.g., grading). The more the teaching is based on virtual classrooms or electronic devices, the more specific and detailed digitized data about students and their behavior and performance will be generated. In addition, detailed digitized data about pupils and students and their behavior may drive the demand for increased use of data within education, including the use of so-called "learning analytics"[2].

3. At the university level, already many institutions – often in partnership with private enterprises – have started to offer "Massive Open Online Courses" ("MOOCs"), which enable students to enroll in university classes over the Internet. These courses are not provided in traditional classrooms and often involve the collection

[1] The Office of the Privacy Commissioner of Canada abstains from the adoption of this Working Paper, which relates to matters outside of its jurisdiction.

[2] Learning analytics can be described as "the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs". Learning and Academic Analytics, Siemens, G., 5 August 2011, http://www.learninganalytics.net/?p=131

Secretariat
Berliner Beauftragte für
Datenschutz und Informationsfreiheit
Friedrichstr. 219
D-10969 Berlin
Phone +49 / 30 / 13889 0
Fax: +49 / 30 / 215 5050

E-Mail:
IWGDPT@datenschutz-berlin.de

Internet:
http://www.berlin-privacy-group.org

of personal student data across national borders[3]. The digital platforms record every single interaction between the student, the teacher, and the learning environment. It may be unclear to both students and teachers what becomes of the data gathered.

4. The sensitivity of digitized pupil and student data should not be underestimated. Personal data about learning behavior may be viewed as particularly sensitive, as these data contain information about the interests and abilities of students, how well they memorize facts, how quickly they can solve exercises of all kinds, and how willing they are to learn something new. Combined with data analytics, they might also be used to predict professional future and career opportunities[4]. For example, in the U.S., some states link data about primary and secondary education ("K-12 education data") with workforce data[5]. Certain e-learning platforms use the data they process on students for new forms of analysis (e.g. to predict dyslexia) and, in some instances, for their own commercial purposes[6]. The increasing digitization of pupil and student records, coupled with the rise of new analytic techniques, make students subject to pervasive monitoring that could threaten fundamental privacy and intellectual freedom rights.

5. In many cases, the data processed in the context of e-learning platforms are not stored with the school administrator. Many educational institutions rely on external, cloud-based providers to store and process pupil and student data. Cloud-based platforms create additional privacy and security risks[7]. A matter of particular concern is the distribution of control between educational institutions and the providers of e-learning platforms[8]. Providers may impose standard terms and conditions that give the provider considerable leeway and may result in situations where the provider uses the data for their own purposes. These purposes may be incompatible with the educational mission of the institution. In addition, certain providers may not be willing to assume key responsibilities (e.g. relating to data security) or adhere to restrictions (e.g. relating to international transfers) which are necessary to ensure an appropriate level of protection.

---

[3] Steve Kolowich, *Are MOOC-Takers 'Students'? Not When It Comes to the Feds Protecting Their Data,* THE CHRONICLE OF HIGHER EDUCATION, Dec. 3, 2014, http://chronicle.com/article/Are-MOOC-Takers-Students-/150325.

[4] For example, Singapore is developing a "Total Online Learning Solution" that combines education data and training data. Every student will be assigned a "Learning Record Store" in kindergarten; cf. Frankfurter Allgemeine Zeitung (FAZ) of 28 January 2016, p. 9:"Fürs Überleben lernen wir. Was Unternehmen aus Lerndaten ableiten können".

[5] See, e.g., National Center for Education Statistics, *SLDS Topical Webinar Summary: Linking K12 Education Data to Workforce*, Aug. 28, 2014: https://nces.ed.gov/programs/slds/pdf/Linking_K12_Education_Data_to_Workforce_August2014.pdf.

[6] Dutch Data Protection Authority (College bescherming persoonsgegevens) case z2013-00795, 14 juli 2014. Report of conclusions: "Onderzoek CBP naar de verwerking van persoonsgegevens door Snappet" (https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/mijn_privacy/rap_2013_snappet.pdf)

[7] Cf. the Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland), p 1-3; https://datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

[8] Ariel Bogle, *What the Failure of inBloom Means for the Student-Data Industry*, SLATE, April 24, 2014, http://www.slate.com/blogs/future_tense/2014/04/24/what_the_failure_of_inbloom_means_for_the_student_data_industry.html.

Scope

6. For the purpose of this paper, “e-learning” is understood as the use of technological tools and media that assist in the communication of knowledge, its development and the interaction among teachers, students and educational institutions. E-learning platforms typically involve a variety of devices (such as computers, tablets and mobile devices), data processing and usage models (in-classroom, online courses…) and actors (students, educational institutions, platform providers, application providers…).

7. This paper outlines the main privacy risks for students associated with e-learning platforms and provides recommendations for educational institutions, e-learning platform providers and data protection authorities. This paper does not deal with possible privacy risks for teachers resulting from their use of e-learning platforms (e.g. teacher performance evaluation). The paper in first instance seeks to address the increasing use of e-learning platforms in primary and secondary education.

Privacy risks for students

Unlawful processing and lack of transparency

8. Legislation covering educational institutions may not adequately address new technological trends in learning processes and the extended scope and purposes of data processing in the context of e-learning and learning analytics. Whether consent could be considered to be a valid base is also questionable. Consent should be freely given, which can hardly be guaranteed in an educational context especially where the use of the e-learning platform is compulsory. Hence, in some jurisdictions the collection and analysis of students' data may take place without the necessary legal grounds when the lawmakers have not safeguarded data protection and privacy rights for data processing related to e-learning platforms and learning analytics.

9. The collection or use of students’ data may take place without the knowledge or awareness of teachers, educational institutions, parents or students. Moreover, students, parents and teachers may not be aware of the identity of the actors involved in the processing of student data. Lack of transparency has a direct impact on respect for the principle of lawfulness and fairness.

Excessive collection

10. Students may be subject to excessive collection of personal data. Such data collection may concern highly personal or sensitive information, including location, health, sleep patterns, social media activity[9]. Physical educators, for example, might employ tracking and assessment tools that also monitor student’s health-related habits and behavior outside of school. Other educational institutions might

[9] Khaliah Barnes, *Student Data Collection Is Out of Control*, N.Y. TIMES (Sept. 25, 2014), http://www.nytimes.com/roomfordebate/2014/09/24/protecting-student-privacy-in-online-learning/student-data-collection-is-out-of-control.

be tempted to monitor students' social media activities in their efforts to address cyberbullying. In doing so, educational institutions may unduly encroach upon the private lives of pupils and students. Within the educational context, it is important to respect the principle of proportionality also extending to activities beyond the educational context.

11. For the purpose of learning analytics, the scope of information that is demanded about the students may be even more excessive. Certain analytics tools employ information about social media activities, logs from online-gaming, online communities and physiological sensor data like eye-tracking or motion capture traces. Datasets of interest could include data about cognitive development, social learning, discourse progression, network interactions, learning paths through courses, competency completion and help-seeking behaviour[10].

Profiling and automated decision-making

12. The type and amount of data collected through e-learning platforms facilitates statistical analysis and profiling. As a result, students may be increasingly measured on the basis of group profiles rather than being assessed in their individual development.

13. Moreover, the educational institutions are not in control over the algorithms used for learning analytics, and they rely on the providers of the e-learning platform to interpret what the clickstream data of the students says about their knowledge. This means that the teacher will have to make decisions based on interpretations that they cannot validate.

14. Providers of e-learning platforms or other companies use student data to make subjective assessments about, for example, student "sociability" and "enthusiasm"[11]. Intrinsic human biases in both data generation and system design may lead to unfair results for students, especially members of groups that have historically experienced discrimination. Inferences and judgments about students that are unrelated to academic performance may stigmatize them and limit educational opportunities.

15. Parents and students may not have access to the data used to make a decision; to information about the decision-making process (functioning of the analytics) or to the reasoning underlying the determinations made about students (e.g. when grading or identifying potential learning difficulties). This may be especially true for closed-source algorithms whose methodology is inscrutable, or systems that utilize machine-learning, where even the system developers may not know why certain assessments were generated.

---

[10] (2016). Editorial: Datasets for Learning Analytics. *Journal of Learning Analytics*, *3*(3), 307–311. http://dx.doi.org/10.18608/jla.2016.32.15

[11] Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html?pagewanted=all

16. There may not be a mechanism to ensure fairness in the decision-making process or a mechanism for students and parents to challenge the final assessments[12].

Function creep

17. Private companies collecting student information on e-learning platforms might use the information beyond the academic objective for their own data mining purposes[13]. The data might be used to make real world decisions about student future opportunities, including employment, housing, and credit[14].

Inadequate security

18. Educational institutions and providers of e-learning platforms may fail to adequately safeguard the student data they collect[15]. Student data is already the subject of data breaches, regardless of whether the data is stored with the school or transferred to private vendors and public agencies[16]. Such data breaches might result, for example, from use of insecure login mechanism, from poor configuration of the platform or other types of human error. Students, teachers, or administrators might also be motivated to breach the security of their own (or other students') data for illegitimate purposes (e.g. to change grades).

Lack of accountability

19. Absence of a clear allocation of roles and responsibilities among the various actors involved in e-learning platforms may result in a situation where neither educational institutions nor providers undertake necessary measures to adequately protect privacy and data protection risks.

20. Parents and students may not have access to a single point of contact to address privacy and data protection risks.

---

[12] See Marc Rotenberg and Khaliah Barnes, *Student and Data Privacy*, N.Y. TIMES (May 3, 2014), http://www.nytimes.com/2014/05/04/business/students-and-data-privacy.html

[13] Google, for example, admitted to reading student emails the company collected in its popular Google Apps for Education platform. Cf. Benjamin Herold, *Google Under Fire for Data-Mining Student Email Messages*, EDUCATION WEEK (Mar. 26, 2014), http://www.edweek.org/ew/articles/2014/03/13/26google.h33.html.

[14] The U.S., for example, already offers "Good Student Discounts," whereby student grades can be used to calculate auto insurance discounts. See, e.g., STATE FARM, *Coverage Options That Fit You*, https://www.statefarm.com/insurance/auto/discounts.

[15] See, e.g., Natasha Singer, *Uncovering Security Flaws in Digital Education Products for School Children*, N.Y. TIMES, Feb. 8, 2015, at B1, *available at* http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html; *D.C. Special-Education Students' Confidential Info Was Publicly Accessible for Years*, WTOP (Feb. 4, 2015, 5:15 AM), http://wtop.com/dc/2015/02/d-c-special-education-students-confidential-info-publicly-accessible-years/; Benjamin Herold, *Danger Posed by Student-Data Breaches Prompts Action*, EDUCATION WEEK (Jan. 22, 2014), http://www.edweek.org/ew/articles/2014/01/22/18dataharm_ep.h33.html;

[16] Natasha Singer, *Data Security Is a Classroom Worry, Too*, N.Y. TIMES, June 22, 2013, at BU1, *available at* http://www.nytimes.com/2013/06/23/business/data-security-is-a-classroom-worry-too.html.

Chilling effect

21. Student awareness of constant tracking paired with doubt about future misuse or exposure may have a chilling effect on creativity and expression during a child's intellectual development. Students may feel compelled to adhere to traditional norms and may be deterred from articulating novel ideas out of concern that documentation of unorthodox ideas could be held against them in the future.

Recommendations for educational institutions and providers of e-learning platforms

22. Despite the privacy challenges that surround the use of e-learning platforms, it is possible to use these types of platforms without infringing key privacy principles. The Working Group makes the following recommendations to educational institutions and providers of e-learning platforms with the aim of mitigating the privacy and security risks described above.

23. Educational institutions should engage providers of e-learning platforms that offer sufficient guarantees to ensure that the privacy and data protection rights of students are adequately protected.

24. Educational institutions and providers of e-learning platforms should educate themselves about the existing legal framework on privacy in their jurisdiction, and about any existing guidance, e.g. by Data Protection Authorities[17].

25. Educational institutions must obtain parental consent whenever necessary.

26. Educational institutions and providers of e-learning platforms should collect only as much pupil or student data as they need to complete specified purposes.

27. Educational institutions and providers of e-learning platforms should ensure the purposes for which they are collecting information are clearly defined. For example, "educational purposes" and "educational quality" are vague terms that permit overly broad collection. A more focused collection would, for example, specify that the collection is necessary to "improve fifth grade reading skills" or "enhance college-level physics courses."

28. Educational institutions and providers of e-learning platforms should clearly allocate their respective roles, responsibilities and rights. Educational institutions should ensure that the agreement with the provider of an e-learning platforms stipulates that the provider may only processes student data in accordance with the instructions of the educational institution. Due consideration should also be

---

[17] For example, the Spanish DPA has recently published a report about the results of an of an ex-officio inspection on cloud services in educational services with a set of recommendations to be followed by all interested stakeholders, covering issues like security, data location, contractual clauses, controller-processor relationship, information to users, cloud services, mobile apps and others. Cf. http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Inspeccion_cloud_educacion.pdf (in Spanish). The German National Conference of Data Protection Commissioners has also recently published guidance on the application of online learning platforms in schools; cf. https://datenschutz-berlin.de/attachments/1220/OH_Lernplattform_neu.pdf (in German).

given to issues of data security, geographic location data and the possibility of independent auditing[18].

29. Providers of e-learning platforms should only collect, use, or disclose pupil or student data for purposes which have been explicitly authorized by the educational institution. Providers should not retain pupil or student data for longer than is necessary to support the authorized educational purposes[19].

30. Students and parents have the right to accessible and clear information on privacy and security practices. Educational institutions and providers of e-learning platforms should publish information regarding the categories of information collected, the purposes for which the information will be used, the identity of the actors involved in the processing, for how long the data will be kept, and the security practices in place.

31. Educational institutions must ensure that they retain full control over any determinations or evaluations made about students, especially in case of automated decision-making.

32. Educational institutions and providers of e-learning platform and other companies should ensure utmost transparency regarding the use of algorithms and profiles that may influence decision-making. Any associated automated decision-making or other rule-based systems and the reasoning underlying the determinations made with the systems must be explained to students and parents.

33. Algorithms, protocols, designs and implementations should be open for external review and/or testing. Open audits, or audits by trusted entities, can help to provide assurance that the e-learning technology in fact has all claimed properties and will not generate unfair or discriminatory outcomes.

34. Educational institutions and providers of e-learning platforms should implement Privacy Enhancing Techniques ("PETs") that minimize or eliminate the collection of students' personal data. Where possible, data should be de-identified or deleted, consistent with the principles of data minimization, privacy by design and privacy by default. Institutions should consider allowing the use the platform under a pseudonym only and not disclosing the real names of students to provider of the platform.

35. When student data is collected, controllers should clearly define retention periods for the different categories of student data and apply these to safeguard that they are not retained longer than necessary.

---

[18] For more information see also the Working Paper on Cloud Computing - Privacy and data protection issues - "Sopot Memorandum" - 51st meeting, 23-24 April 2012, Sopot (Poland), p. 3-6; https://datenschutz-berlin.de/attachments/875/Sopot_Memorandum.12.6.12.pdf

[19] See also Student Privacy Pledge, "K-12 School Service Provider Pledge to Safeguard Student Privacy", https://studentprivacypledge.org/wp-content/uploads/2014/09/Student-Privacy-Pledge-V1.pdf.

36. Students and parents have the right to access and correct educational records and any other personal data (e.g. behavioural information) stored, regardless of who collects or maintains the information.

37. In cases of automated individual decisions, students should have access to the decision and its reasoning. There should be specific procedures that lead to a human evaluation of decisions in cases where a different point of view is submitted, counter-arguments presented, or where the decisions are challenged.

38. Educational institutions should avoid 'lock-in' situations where personal data of students is tied in a black-box processing platform with poor transparency and control. Providers of e-learning platforms should allow portability of data in a structured, machine readable and open formats (e.g. when a pupil changes school).

39. Students may on occasion make poorly informed decisions that could affect them in their adult life. The notion of the right to be forgotten has been introduced in some legislative frameworks in order to ensure that the negative consequences of poor decisions are minimized. Educational institutions should inform students about their rights and raise awareness of mindful publishing and sharing of personal data. Providers of e-learning platforms should embed tools that enable effective exercise of the right to be forgotten.

40. Educational institutions and providers of e-learning platforms should collect, use, and disclose student information solely in ways that are consistent with the context in which students provide data. Data related to students' use of the e-learning platform should not be used or made available for any other incompatible secondary purposes.

41. Educational institutions should conduct a privacy impact assessment and a risk analysis before using an e-learning platform, and should implement the necessary technical and organizational measures according to the analysis before and while using the services of an e-learning platform. Technological and organizational measures for data security should be continuously monitored and improved.

42. Educational institutions and providers of e-learning platforms should use a two-factor authentication mechanism for administrators and teachers to log in to the e-learning platform to prevent misuse through stolen passwords. Access controls and logging policies need to be in place and enforced to ensure that access to personal data is properly managed and supervised. Access to personal data should follow the 'need-to-know' principle.

43. Providers of e-learning platforms should notify educational institutions, students or their parents, and appropriate supervisory authorities in the event of a breach according to the local legal requirements for data breach notification[20].

[20] See for example OECD work on breach notification in The OECD Privacy Framework, OECD 201, available at: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Recommendations for Data Protection Authorities

44. Data protection and privacy authorities should strengthen their awareness raising activities by providing guidance to schools. This could include promoting the application of privacy by design principles with e-learning providers, while also strengthening their supervisory activities (e.g., with privacy sweeps).

45. Data protection authorities should support the implementation of codes of conduct, data protection and privacy certification schemes, as well as the development of suitable data protection and privacy impact assessment frameworks and tools, in order to foster the development of privacy friendly solutions.

Recommendations for policymakers

46. Where clear legal rules do not exist for the collection, processing and use of student data, such rules should be established.

47. Where current laws do not adequately address new technological trends in learning processes, the extended scope, purposes and decisions adopted by means of data processing in the context of e-learning, such laws should be updated[21].

48. Finally, policymakers should promote data protection and privacy education in study programmes and curricula[22].

---

[21] EPIC has proposed a framework, the Student Privacy Bill of Rights, modeled after the structure of traditional privacy laws. Cf. EPIC, *Student Privacy Bill of Rights*, https://epic.org/privacy/student/bill-of-rights.html. The Student Privacy Bill of Rights incorporates several provisions in from EU Directive 95/46 and the Council of Europe Convention 108, including purpose specification, requirements that those keeping student data maintain accurate data, and data security requirements. See Khaliah Barnes, *Why a 'Student Privacy Bill of Rights' is Desperately Needed*, WASHINGTON POST, Mar. 6, 2014, https://www.washingtonpost.com/blogs/answer-sheet/wp/2014/03/06/why-a-student-privacy-bill-of-rights-is-desperately-needed.

[22] ICDPPC 38, "Resolution for the Adoption of an International Competency Framework on Privacy Education" (Marrakech 2016), https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf.