5th International Conference on Higher Education Advances (HEAd'19)
Universitat Politècnica de València, València, 2019
DOI: http://dx.doi.org/10.4995/HEAd19.2019.9063

Compliance of MOOCs and OERs with the new privacy and security EU regulations

Katerina Zdravkova
Faculty of Computer Science and Engineering, University Sts Cyril and Methodius, Skopje, Macedonia.

Abstract

Since their appearance in the early 2000s, Massive Open Online Courses (MOOCs) and Open Educational Resources (OERs) arose among the most important educational priorities. Many top universities worldwide have been involved in the research and direct implementation of this innovative pedagogical approach. Simultaneously with the development and massive deployment of the new learning and teaching method, European regulations responsible for data privacy and information security protection have significantly evolved. This paper assesses the compliance of the ten most popular MOOCs and OERs with the General Data Protection Regulation (GDPR) and the Directive on security of network and information systems (NIS Directive). In order to systematically examine their online platforms, a few privacy indicators were outlined and thoroughly observed. Alongside this, the involvement of the open education providers in the NIS Directive was examined. Research findings are presented and elaborated in a way that it makes easy to generate recommendations on how to anticipate the future of open education as a reasonable reaction to global change in the era of rapid technological growth, and at the same time to obey the crucial ethical principles defined by this development.

Keywords: *GDPR; ISO Standardisation; NIS Directive; Privacy obliteration; Security attacks.*

1. Introduction

The internet and its considerable popularity enabled the birth of open learning, initiating dramatic changes in education by enabling access to all the learners and teachers (Bonk, 2009). The UNESCO forum on the impact of open courseware held in 2002 defined Open Education Resources (OERs) as "technology-enabled, open provision of educational resource for consultation, use and adaptation by the community of users for non-commercial purposes". It promoted the idea of full and open access to learning objects. This initiative formally recognized the open coursewares (OCW), which were founded in 1999 with the recorded and online published video lectures by the University of Tübingen (https://timms.uni-tuebingen.de/), but became widely appreciated in 2001, when Massachusetts Institute of Technology (MIT) started making their educational materials publicly available, online and for free,, as part of the MIT OpenCourseWare (MIT OCW) (https://ocw.mit.edu/index.htm). Since 2002, OER and OCW are used interchangeably.

Learning objects were introduced in 1994 by Wayne Hodgins (Hodgins, 2006). According to Hodgins (2006), taking into consideration their role of core elements for content creation and distribution, learning objects will "increase and improve the effectiveness of learning and human performance". His optimistic expectations were embodied in the Massive Open Online Courses (MOOCs), which were first mentioned by Cormier (2008), who coined the term to label the distributed online course "Connectivism and Connective Knowledge", created by Stephen Downes and George Siemens (2008). Apart from contributing to the first MOOC and authoring the corresponding online book (Downes, 2012), Downes believed that the new approach was more creative and dynamic in comparison to the existing ones, which according to him resembled "television shows or digital textbooks" (Ossiannilsson, 2014). For less than 10 years, MOOCs became immensely popular, enabling millions of learners to extend their knowledge and competences in various topics at different educational levels, and by providing a certain fee, they can obtain a verified certificate in the area.

There is not a strict distinction between MOOCs and OERs. The timeline published by Yuan and Powell (2013) suggests that all MOOCs are influenced or directly related to open education, making them successors of OERs. The UNESCO guide suggests that OERs are resource-based, with openly licensed content, usually under Creative Commons copyright licenses (https://creativecommons.org/), and not necessarily shareable in digital format (Butcher, 2015). MOOCs can have flexible design and resources (Lambert, 2015), they are neither massive nor free (Kilgore and Lowenthal, 2015), and as the second 'O' in their acronym indicates, all the communication and content sharing is online. Nevertheless, MOOCs and OERs are usually jointly presented, such as in the topics of interest of HEAd'19. Consistently, ten popular MOOCs / OERs, which will be examined in the rest of the paper are also jointly presented. They include: Alison, Coursera, CourseSites, edX, FutureLearn, Khan Academy, LearningSpace, MIT OpenLearn, OpenCourseWare, and Udacity.

The paper proceeds with Section 2, which examines open education privacy policies, data protection and their compliance with GDPR. Section 3 starts with the security glitches in education, and continues with the direct involvement of Universities and research centres into the NIS Directive, whereas the last section presents the concluding remarks, which are deduced from the previous sections.

2. Data privacy in open education

Student education records contain a lot of sensitive data and confidential documents, including personal data intended for student identification and interaction, like e-mail addresses, but also information about the student's presence at lectures, performance at assignments and exams, facts about the student's behavior and discipline, including the measures against bad performance or misconduct. Learning management systems (LMSs), which are the crucial framework of all the examined MOOCs / OERs have a direct overview of student activity logs. These logs contain additional sensitive information, for example the IP address, login time and duration, as well as indicators of students' mutual communication. All these data and logs are visible to those teachers who are responsible for managing the courses the students are enrolled in (Hew, 2016). Some educational information and records are extracted from LMSs and then presented in a form of student report cards or academic performance certificates to potential internship providers, prospective employers, state institutions or educational institutions offering grants and loans, as well as to foreign institutions and governments, for example for obtaining a visa or a work permit. The awareness of such data collection, and the privacy perception is definitely one of the key predictors for using open education services (Arpaci, Kilicer & Bardakci, 2015).

Many programs and laws protect student privacy. Since 1974, the Family Educational Rights and Privacy Act (FERPA) is regulating the rights of accessing education records in USA (https://www.cde.state.co.us/cdereval/ferpa). In spite of its long history and implementation, first complaints against FERPA have emerged only recently. They cover the improper protection of "information that does not fit into definition of an education record", and the violation of state open record laws, which are additionally controversial due to the loopholes in the federal privacy laws (Elliott, Fatemi, & Wasan, 2014).

Although this paper examines EU regulations, most MOOCs and OERs are registered in the USA, so EU users are complying with US regulations too. This was one of the causes for the EU-US and Swiss-U.S. Privacy Shield (https://www.privacyshield.gov/welcome). Europe has recently started implementing the General Data Protection Regulation (GDPR), which contains the reciprocal EU regulations for the protection of international transfer of personal data outside the EU for commercial purposes (https://ec.europa.eu/info/law/law-topic/data-

protection/data-transfers-outside-eu_en). In parallel with these rules, GDPR regulates privacy in education (https://ec.europa.eu/info/law/law-topic/data-protection_en).

In January 2014, an ambitious European project, called Higher education Online (HOME) was launched (https://home.eadtu.eu/). It unites 23 European educational institutions, whose aim is to create and implement MOOCs "the European way". One of the crucial values of the project is "full privacy for all respondents". The privacy policy of the European Association of Distance Teaching Universities (https://eadtu.eu/), which is responsible for managing this project has been adjusted to "comply with applicable data privacy" and control "personal data under the GDPR" (https://eadtu.eu/privacy-policy). The policy introduces the five areas of concerns: data collection and use; data sharing; retention periods when storing personal data; cookies; and privacy rights and contact. They are all incorporated within HOME.

Is the same approach implemented in the popular MOOCs / OERs worldwide? The major privacy concern reported so far deals with the considerable sharing of learner data (Reich, 2015). To minimize the risks, Reich suggests protection of learners' anonymity and technical solutions that will enable safe data sharing. Another problem is that most learners are non-experts and they don't know how to manage their online privacy (Egelman, Bernd, Friedland & Garcia, 2016).

After examining the age restrictions, the collection of age data, the amount of cookies, provided data dashboards, and the contact information regarding data from Coursera, EdX, and Blackboard's CourseSites MOOCs, Jones and Regner (2015), revealed "inconsistencies among MOOC platform and the level and type of legal uncertainty surrounding them". However, the most worrying is the fact that the student awareness about privacy issues and threats is rather low (Frost & Hamlin, 2017). This fact was confirmed by a survey made with 259 students from 34 nations. After examining many different questions, Frost and Hamlin (2017) concluded that "the responses indicate a lack of basic understanding about Internet security". Privacy was not mentioned at all.

Table 1. presents the privacy indicators of the ten MOOCs / OERs, which were announced in the introduction of the paper, as they are available from their sites. After the platform name, its URL and the country of origin, the following privacy indicators are displayed: visitors' consents to obtain and store cookies, visibility of the privacy policy, collection of sensitive data, collection of online habits, and finally, data mining of collected data.

Sensitive data encompass the following information: 1: name, 2: date of birth, 3, gender, 4: country of residence, 5: e-mail, 6: home address, and 7: phone number. Online habits embrace: 1: time of accessing the system, 2: pace of opening and elaborating new lectures, 3: amount of attempts during online assignments, 4: participation in discussions, 5: supporting other colleagues, 6: content of discussion threads, 7: asked assistance from professor, 8: learning habits, 9: reading habits. The suspicion that MOOC / OER perform

data mining of the information collected from their learners is confirmed with the reports published by themselves.

Table 1. Privacy issues of the most popular MOOCs and OERs.

Name of the platform	Country	Cookie consent	Privacy policy	Sensitive data	Online habits	Data mining
Alison alison.com	Ireland	No	GDPR adjusted	1, 5	1, 2, 3, 4, 8, 9	N.A.
Coursera www.coursera.org	US	No	GDPR adjusted	1, 5	1, 2, 3, 4, 5, 6, 7, 8, 9	Yes
CourseSites coursesites.com	US	Yes	Detailed advanced	1, 4, 5	1, 2, 3, 4, 5, 6, 7, 8, 9	Yes
edX www.edx.org	US	No	GDPR adjusted	1, 4, 5	1, 2, 3, 4, 5, 6, 7, 8, 9	Yes
FutureLearn www.futurelearn.com	UK	Yes	Detailed advanced	5	1, 2, 3, 4, 8, 9	Yes
Jisc www.jisc.ac.uk/	UK	No	Short outdated	1, 2, 3, 4, 5, 6, 7	1, 2, 3, 4, 5, 6, 7, 8, 9	Yes
Khan Academy www.khanacademy.org	US	No	GDPR adjusted	1, 2, 5	1, 2, 3, 7, 8, 9	Yes
OpenCourseWare ocw.mit.edu/index.htm	US	No	Short outdated	No regis-tration	None	N.A.
OpenLearn open.edu/openlearn	UK	Yes	Detailed advanced	1, 2, 4, 5, 7	1, 2, 3, 4, 5, 6, 7, 8, 9	Yes
Udacity www.udacity.com/	US	Yes	GDPR adjusted	1, 5	N.A.	N.A.

In spite of EU regulations, only FutureLearn and Open University's OpenLearn require cookie consent from their visitors. Majority of US sites simply ignore this. Apart from Jisc, which is a warehouse of UK higher and further education and MIT's OpenCourseWare, all other MOOCs / OERs have adjusted GDPR privacy policies. CourseSites, FutureLearn and OpenLearn have implemented even more information regarding their GDPR policies. The amount of collected personal data during registration varies from e-mail only, to all the data in Jisc. Although registration is not enabled, learners officially enrol to UK Universities, thus all their data are collected by the corresponding schools. Online habits are closely observed and pass through detailed data mining in Coursera (Mukala et al., 2015), CourseSites

(Holcomb & Buell, 2016), EdX (DeBoer et al, 2013), FutureLearn (Hodge, 2016; (Hone, Kate & Ghada, 2016), and OU OpenLearn (Johnson, 2015). All in all, MOOCs / OERs lightly comply with GDPR. This problem should be resolved as soon as possible.

3. Data protection

The most recent report on Distributed Denial of Service (DDoS) attacks from October 2018 revealed that the peak period of their occurrence was September, and that "the primary target, year after year, is the education system, attacks being directed at the web resources of schools, universities and testing centers" (Kupreev, Badovskaya, Gutnikov, 2018). The target of the great DDoS attack in September 2018 was University of Edinburgh, which is part of the UK MOOC Jisc (McLachlan, 2018). In the statement about the severe security glitch, McLachlan (2008) said that it was "a cyber attack on their network and against other UK Universities". Jisc's security operations centre head Chapman (2018) revealed that the pick of such attacks coincided with the beginning of the academic year, with in average 10 DDoS attacks daily, while the holiday periods were usually idle. Additionally, the discovered attack pattern indicated that attackers were usually students who sometimes purchased the DDoS packages from so called "booter" or "stresser" sites (Whittaker, 2018). If there is a doubt that Udacity was hit by a massive DDoS attack (https://twitter.com/udacity/status/869222317787717633), it is explicitly acknowledged that the developer platform GitHub was a DDoS victim (https://githubengineering.com/ddos-incident-report/). Universities are sometimes infected by ransomwares. University of Calgary experienced a ransomware attack in 2016 (https://www.ucalgary.ca/risk/node/30), while University College London was a victim of a similar vulnerability in 2017 (https://www.bbc.com/news/education-40288548).

All the security weaknesses mentioned in the previous paragraph were promptly removed mainly because the greatest security experts are associated with Universities and research centres. Accordingly, they "have a decisive role to play in spurring research, development and innovation in those areas" (https://eur-lex.europa.eu/eli/dir/2016/1148/oj). The European Union Agency for Network and Information Security (ENISA), as a centre of expertise for cyber security in Europe, established its own MOOC, which embraces 535 courses from 28 European countries. Apart from this MOOC, Jisc endorses the Directive (https://community.jisc.ac.uk/taxonomy/term/nis-directive), while US based Coursera is providing training materials "for implementing the EC roadmap NIS education" (https://www.enisa.europa.eu/publications/roadmap-for-nis-education-programmes-in-europe). Others have no visible signs to cooperate or implement the Directive. One of the ENISA's goals is NIS Standardisation (https://www.enisa.europa.eu/events/enisa-cscg-2017/presentations/purser), which suggests: ISO SC27 for privacy, ISO 15408 for security assurance and ISO 2700 series for organisational management for secure operations. To the best of the authors' knowledge, none of the examined MOOCs / OERs are unambiguously indicating the fulfilment of any of

these standards. On the other hand, all of them (N.B. except Knan Academy) offer courses about ISO standardisation, which proves their awareness about them. Consequently, if they are not already, they can easily become fully ISO complaint, which will immediately trigger their compliance with the new EU security regulations.

4. Conclusion

Coursera, edX and Udacity were launched after 2011. Jointly, in less than 8 years, they have reached more than 50 million students and offered more than 5000 advanced education courses. Fascinated by the openness and social interactions of the open educational model, together with the possibility to obtain a valuable certificate of course completion or a recognized University degree, many learners have actively participated and completed the MOOCs. Their success stories trigger new prospective learners to experience open education.

The greatest responsibility for sustainable MOOCs / OERs falls on their providers. Together with the attractive courses, good learning resources, and experienced educators, who are motivated to innovate the learning process, the MOOC platforms should protect students' human rights and values. However, every year, the data privacy and security risks increase. To protect learners from these escalating hazards, the regulations should be carefully obeyed.

The study of the most popular and influential MOOCs and OERs has shown that, despite that the awareness of the new EU regulations is high, very few steps have been made to implement data protection rules and to protect learners' privacy. In short term, it will not affect the popularity of open education, but gradually, as learners seek greater protection from any privacy threats (Lorenz et al, 2013), if the protection is not equally offered, this education model might collapse.

References

Arpaci, I., Kilicer, K., & Bardakci, S. (2015). Effects of security and privacy concerns on educational use of cloud services. *Computers in Human Behavior*, *45*, 93-98.

Bonk, C. J. (2009). The world is open: How web technology is revolutionizing education. In *EdMedia: World Conference on Educational Media and Technology* (pp. 3371-3380). Association for the Advancement of Computing in Education (AACE).

Butcher, N. (2015). *A basic guide to open educational resources (OER)*. Commonwealth of Learning (COL).

Chapman, J. (2018). Cyber attacks on colleges and universities: who, when and why?, from https://www.jisc.ac.uk/blog/cyber-attacks-on-colleges-and-universities-who-when-and-why-14-sep-2018

Cormier, D. (2008). The CCK08 MOOC–Connectivism course, 1/4 way.

DeBoer, J., Stump, G. S., Seaton, D., Ho, A., Pritchard, D. E., & Breslow, L. (2013). Bringing student backgrounds online: MOOC user demographics, site usage, and online learning. In *Educational Data Mining 2013*.

Downes, S. (2012). Connectivism and connective knowledge: Essays on meaning and learning networks.

Downes, S. & Siemens, G. (2008). Connectivism 2008, from https://sites.google.com/site/themoocguide/3-cck08---the-distributed-course

Egelman, S., Bernd, J., Friedland, G., & Garcia, D. (2016). The Teaching Privacy Curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education* (pp. 591-596). ACM.

Elliott, T. L., Fatemi, D., & Wasan, S. (2014). Student Privacy Rights--History, Owasso, and FERPA. *Journal of Higher Education Theory & Practice*, *14*(4).

Frost, J., & Hamlin, A. (2017). Internet security and privacy threats, as perceived by American and int'l business students. *Global Journal of Business Disciplines*, *1*(1), 36.

Hew, K. F. 2016. Promoting engagement in online courses: what strategies can we learn from three highly rated MOOCs. *British Journal of Educational Technology*, *47*(2), 320-341.

Hodge, R. (2016). Adapting a MOOC for Research: Lessons Learned from the First Presentation of "Literature and Mental Health: Reading for Wellbeing". *Journal of Interactive Media in Education*, *2016*(1).

Hodgins, H.W., 2006. The future of learning objects. *Educational Technology*, pp.49-54.

Holcomb, C., & Buell, D. (2016). First-Year Composition as" Big Data": Examining Student Revisions at Scale. In *EDM (Workshops)*.

Hone, K. S., & El Said, G. R. (2016). Exploring the factors affecting MOOC retention: A survey study. *Computers & Education*, *98*, 157-168.

Johnson, G. M. (2015). On-campus and fully-online university students: Comparing demographics, digital technology use and learning characteristics. *Journal of University Teaching & Learning Practice*, *12*(1), 4.

Jones, M. L., & Regner, L. (2016). Users or students? Privacy in university MOOCS. *Science and engineering ethics*, *22*(5), 1473-1496.

Kilgore, W., & Lowenthal, P. R. (2015). The Human Element MOOC. In *Student-teacher interaction in online learning environments* (pp. 373-391). IGI Global.

Kupreev, O., Badovskaya, E., Gutnikov, A. (2018). DDoS Attacks in Q3 2018, from https://securelist.com/ddos-report-in-q3-2018/88617/

Lambert, S. R. (2015). Reluctant mathematician: Skills-based MOOC scaffolds wide range of learners.

Lorenz, B., Sousa, S., & Tomberg, V. (2013). Privacy awareness of students and its impact on online learning participation–a case study. In *Open and social technologies for networked learning* (pp. 189-192). Springer, Berlin, Heidelberg.

McLachlan, G. I. (2018). DDoS Attack 10th September 2018, from https://www.ed.ac.uk/infosec/information-security-updates/ddos-attack-10th-september-2018

Mukala, P., Buijs, J. C., Leemans, M., & van der Aalst, W. M. (2015). Learning Analytics on Coursera Event Data: A Process Mining Approach. In *SIMPDA* (pp. 18-32).

Ossiannilsson, E. (2014). Lessons learned from the European eMOOCs 2014 Stakeholders Summit. *Changing the Trajectory: Quality for Opening up Education*, *109*.

Reich, J. (2015). Rebooting MOOC research. *Science*, *347*(6217), 34-35.

Whittaker, Z. (2018). FBI kicks some of the worst 'DDos for hire' sites off the Internet, from https://techcrunch.com/2018/12/20/fbi-ddos-booter-sites-offline/

Yuan, L., Powell, S., & CETIS, J. (2013). MOOCs and open education: Implications for higher education.