



COVID-19 Education Response Roundtable

Protecting learner data, privacy and security

Friday 29 May 2020

13h00 – 14h30 GMT+2

Concept note and agenda

Introduction

The global shift to distance learning in response to COVID-19 school closures has propelled longstanding discussions about learners’ data privacy and security to the forefront of national and international agendas.

Before the pandemic and depending on national contexts, many student records, whether test scores, homework assignments, or attendance information, were digitalized and bundled into easily searchable portfolios. The abrupt transition to distance learning has accelerated this process dramatically: more educational data is being digitized and stored than ever before and at an unprecedented scale. The information collected is routinely stored on servers that are located across the globe and controlled by corporations, some of them specialists in the monetization of personal data. In this changed educational context, learner data is being processed and sold for commercial purposes, and learners themselves are regularly subjected to market forces, such as targeted advertisements.

The internet technologies that are currently mediating teaching and learning as a result of COVID-19 routinely capture dizzying quantities of information ranging from administrative data (name, gender, attendance information, examination scores), to data about learning processes (as varied as thinking characteristics, learning trajectory, engagement score, response times, pages read, videos viewed). Furthermore, new learning technologies sometimes collect and process biometric information (for

example, fingerprints or eye scans used to access and complete an examination), and lines between the personal realms and academic realms are blurring. Images of the interiors of students' homes are often visible in video classes, and instructional hours, once structured around a fixed class schedule, have, in many instances, become asynchronous and irregular.

Recent incidents, such as widespread hacking of lectures held on video-conferencing platforms and privacy intrusions associated with online assessments have forced the education sector to confront the challenge of maintaining privacy and security in online learning spaces.

Questions about who owns digital learning data, how it can be collected, used and shared, and by whom have also taken on greater urgency because of the sudden and largely unplanned transition to distance education. The data is valuable to a variety of entities, whether advertising juggernauts, data brokers, social scientists, corporations, political parties and, of course, governments and educators. It is particularly valuable to employers. Just as human resource departments regularly ask to see the academic transcripts of job seekers, it is not hard to imagine a near future in which employers might ask to see *every* available record.

Already complex analytic technology, often powered by artificial intelligence, can pour over messy learning portfolios to make assumptions about learner performance at the level of systems as well as at the level of individual learners. This technology can aggregate and integrate data to venture far-reaching inferences about learners and their capacities and limitations. Today a poor grades in secondary school can hurt a student's chance to attend higher education, tomorrow a student's test score on a single assignment in primary school might carry lifelong repercussions if it is found to closely correlate to, say, job performance in a particular field.

Adding further challenges, the technologies used to capture, store and make sense of learner data are often opaque and controlled by multiple parties, and this can make accountability difficult to ascribe. Analytics that generate faulty, biased or discriminatory conclusions can carry significant consequences for learners. The threats are particularly acute for women who are often disadvantaged by data scanning systems that undervalue their learning and accomplishments.

Finally, even when learning data is responsibly collected and used, its security can be compromised and this exposes learners to a variety of risks, ranging from identity theft to bullying and blackmail. Very few digital systems—at least thus far—have proven to be fail-proof.

The collection and use of learner data involves complex tradeoffs, and governments and other organizations are trying to strike a balance to maximize the considerable opportunities offered by this data to improve the quality and equity of learning, while also mitigating the risks posed to privacy. Governments and international community should develop appropriate policies, strategies and regulatory frameworks to mitigate such risks while optimizing the many benefits of online learning solutions.

This webinar, the eleventh in an ongoing UNESCO series, will dive into this timely debate and ask if we have, as a result of COVID-19 and regardless of intentionality, entered an era of learning surveillance and, if so, what actions we should take to protect privacy without losing the educational opportunities offered by digitalization?

Discussion questions

The discussion will feature a presentation by Borhene Chakroun, Director for Policy and Lifelong Learning Systems at UNESCO, and interventions from high-level representatives of national authorities and international agencies reflecting different constituencies. Speakers will address the following questions:

1. How has the massive shift to online learning in response to COVID-19 impacted the privacy and security of learners and their data?
2. Many educators seem to have turned to social media and general-purpose video-conferencing platforms during lockdown, instead of (or in addition to) online tools specifically developed and designed for teaching, learning or the management of education. What privacy and security challenges have arisen from this? What guidance is being provided to guide and support educators?
3. What have been the most innovative and effective approaches to ensuring the protection and security of learners' data in the context of online learning and datafication of education? What measures have accounted for the special risks of women and girls?
4. What frameworks exist to help monitor and understand learners' digital security and safety?
5. What is the future of learner privacy in our rapidly digitalizing world? What further developments are expected over the next several years? How can educational authorities, international organizations and data protection and privacy enforcement authorities join forces together to protect learners in this context?

Audience

The webinar is designed for online learning and ICT in education policy-makers and stakeholders: ministries of education, ministries of employment, data protection and privacy enforcement authorities, school boards, school administrators, school ICT managers, online educational institutions, ed-tech representatives, privacy watchdogs, teachers, as well as learners and their families.

Technical specifications

The webinars will use Zoom as a technical platform. Participants will have the opportunity to ask questions, make comments and share relevant information and material through a chat function.

Agenda

Friday, 22 May 2020	
13:00 – 13:15	Opening remarks: <ul style="list-style-type: none">Mr. Borhene Chakroun, Director of the Division for Policy and Lifelong Learning Systems, UNESCO
13:15 – 14:00	Panelists: <ul style="list-style-type: none">Hon. Claudette Irere, Minister of State for Education and TVET, RwandaLeandro Folgar, President, Plan Ceibal, UruguayMs. Amelia Vance, Director of Youth and Education, Future of Privacy ForumMr. Martin Dougiamas, CEO, MoodleMs. Liz Sproat, Head of Education for Europe, the Middle East and Africa, Google
14:00-14:20	Questions and answers
14:20-14:30	Closing and future directions: <ul style="list-style-type: none">Ms. Pascale Raulin-Serrier, CNIL, France

Panellists

Borhene Chakroun is the Director of the Division of Policies and Lifelong Learning Systems at UNESCO. His work focuses on global trends in reforming education and training systems for skills development in the context of the 2030 Sustainable Development Agenda. He has conducted a range of policy reviews and skills systems diagnosis and authored various articles and books on skills development and lifelong learning. Previously he worked as a consultant for the EU, the World Bank and other international organizations and the European Training Foundation (ETF).



Hon. Claudette Irere was appointed Minister of Education and TVET of the Republic of Rwanda in February 2020. This position has been reinstated as the government moves to streamline and strengthen TVET, laying out pillars of the country's new development blueprint, Vision 2020. Prior to her current position, she was the Permanent Secretary in the Ministry of ICT and Innovation. Hon. Claudette Irere, who co-founded FabLab Rwanda and served as its general-manager, previously also served as project manager at PSF-ICT Chamber, general-manager at Klab, and manager ICT projects at Transform Africa. Hon. Claudette Irere acquired her master's degree in Computer Engineering from Oklahoma Christian University in 2013 a year after graduating from the former National University of Rwanda with a Bachelor's in Computer Science in 2012.



Leading the edtech national strategy of Uruguay during COVID-19 crisis, Leandro Folgar is the president of Plan Ceibal. He has a degree in Education (Catholic University of Uruguay, UCU) and a Master's degree in Technology, Innovation and Education from Harvard University. He is a Fulbright alumnus, entrepreneur, and consultant for the corporate sector. He worked as a researcher and teacher at the Human Sciences and Business Sciences departments of UCU. Learning environments of the 21st century is his line of research. He also specializes in Active Teaching Methods and Adult Development. He is also a professor at UCU Business School and UCU Education Department.



Amelia Vance is Director of Youth and Education Privacy at the Future of Privacy Forum. Amelia advises policymakers, academics, companies, districts, and states on child and student privacy law and best practices; oversees the education privacy resource center website, FERPA|Sherpa, and the review of applicants to the Student Privacy Pledge; and convenes stakeholders to ensure the responsible use of student data and education technology in schools. Prior to FPF, Amelia was the Director of the Education Data & Technology Project at the National Association of State Boards of Education (NASBE).



Dr Martin Dougiamas is best known as the founder of the open-source Moodle LMS (used by over 60% of all higher education in the world). He is now the CEO of the Moodle project, which produces Moodle Apps, MoodleCloud, Moodle Educator Certifications, Moodle Workplace and more.

Martin has a mixed academic background with multiple post-graduate degrees in Computer Science and Education and two honorary doctorates (from Spain and Belgium). He continues to focus on researching how technology can support teaching and learning in open and human ways, especially when it supports the UN's sustainable development goals.



Liz Sproat is Google's Head of Education for Europe: Middle East and Africa. With more than 15 years' experience in education, Liz is responsible for working with universities and schools to bring technology into the classroom. Prior to moving to Google, Liz was based in Dubai working as Vice President for K12 for Pearson Education. In that role Liz collaborated with Ministries in the UAE, Saudi and Nigeria to develop national professional development and digital programmes.



After joining the French Data Protection Authority (CNIL) in 2005 and serving in European and international Affairs for 8 years, Pascale Raulin-Serrier has been developing national and international expertise for the French Commission in promoting collaborative projects in digital education targeted towards all types of audience. Pascale is currently addressing awareness workshops and face-to-face training activities aimed to teachers, schools and educators at large on privacy best practices. On behalf of CNIL leading an international working group in Digital Privacy Education, she has been facilitating sharing of pedagogical resources and projects among 50 Data Protection Authorities globally and has worked on successful adoption of 2013, 2016 & 2018 international Resolutions in Digital Privacy Education including a Personal Data Protection Competency framework for school students which is being promoted for implementation in national curricula in close cooperation with Ministries of National Education.



Stay in touch

UNESCO's COVID-19 Education Response



COVID19taskforce@unesco.org



<https://en.unesco.org/covid19/educationresponse>



[@UNESCO](https://twitter.com/UNESCO)