

# Learner Privacy, a pending assignment

Marc Alier<sup>†</sup>, María José Casany  
Service Engineering Dept.  
Universitat Politècnica de Catalunya  
Barcelona Spain  
{[marc.alier.ma.jose.casan@upc.edu](mailto:marc.alier.ma.jose.casan@upc.edu)}

Charles Severance  
School of Information  
University of Michigan  
Michigan EEU  
[csev@umich.edu](mailto:csev@umich.edu)

Daniel Amo  
La Salle  
Universitat Ramon Llull  
Barcelona Spain  
[daniel.amo@salle.url.edu](mailto:daniel.amo@salle.url.edu)

## CCS CONCEPTS

• Security and privacy • Human and societal aspects of security and privacy • Social Aspects of Security and Privacy • Social and professional topics • Surveillance

## KEYWORDS

Technologies for education, Student's privacy, Learning Management Systems, Surveillance.-<sup>†</sup>

## ABSTRACT

In 2020 the data about learners is escaping the premises of the learning institutions. The personal information about students and their activity while they interact with Learning Management Systems and Online Learning Tools is in custody of cloud computing providers, and Learning Tools vendors. The model of Software As A Service allows service providers to control all the information about the students. There are an increasing number of cases in which we know that this information has leaked, or has been used in a shady way. This paper analyzes how this situation came to pass, why this is wrong and goes through examples where data and metadata about learners is being gathered in shady conditions. Finally, we conclude that this problem has several dimensions: legal, organizational, cultural and technical, how any solution needs to address these four dimensions, and that we should better get started working on it.

---

\*Article Title Footnote needs to be captured as Title Note

<sup>†</sup>Author Footnote to be captured as Author Note

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

TEEM 2020, Salamanca, Spain

© 2020 Copyright held by the owner/author(s).

## 1 Introduction. When privacy became an issue

In 2016 the issue of privacy entered the radar of social awareness because the public outrage caused by the news about Cambridge Analytica. News outlets reported how the company used personal data leaked from Facebook and other platforms to influence the 2016 political campaigns of Brexit in the UK, and the presidential election in the USA [1]. Almost in sync with these events, some rising voices started to warn us about the real depth of the issue and its impact.

Tristan Harris, a former design ethicist at Google where he first worked on user experience design and then studied ethics of human persuasion, gave a popular TED Talk in 2017 [2] titled "How a handful of tech companies controls billions of minds every day". Harris described how tech companies use data about the user's interactions to "improve" the design and interfaces of apps and websites. The purpose of this "improvement" is to influence the behavior of millions of users and get leverage to push the companies own goals. Just like the B.F. Skinner behaviorist experiments, but conducted at an unprecedented scale on unsuspecting subjects, without their consent and with great unforeseen consequences.

Professor Soshana Zuboff published in 2014 her essay "A Digital Declaration: Big Data as Surveillance Capitalism" [3], outlined the concept of Surveillance Capitalism as a "radically disembodied and extractive variant of information capitalism" based on the commodification of "reality" and its transformation into behavioral data for analysis and sales. According to Zuboff collecting and processing data in the context of capitalism's core profit-making motive might present a danger to human liberty, autonomy, and wellbeing. Surveillance capitalists have become focused on expanding the proportion of social life that is open to data collection and data processing, with significant implications for individual vulnerability, control of society, and for privacy as well. In 2019 Zuboff's work was popularized in the mainstream with her bestseller book "The Age of Surveillance Capitalism" widely discussed in public forums like podcasts, blogs, round tables, and the press worldwide [4].

In addition to that, in the last 3 years, face and voice recognition technologies have reached a level of efficiency, accuracy, and reduction of costs that have propitiated its introduction at scale in public spaces. Countries like China have started to use these technologies in conjunction with social networks and mobile apps to implement a system of social credit. Just like the dystopic TV series "Black Mirror" predicted in the episode "Nosedive" in 2016 [5]. These technologies are readily being used as a social control tool by totalitarian states.

Nowadays in 2020, privacy is a very relevant issue to discuss in all dimensions of social life, in its online and even in analogic public spaces.

This paper first analyzes the technical and organizational causes that have propitiated the current situation of the online learning tools over the last twenty years. Then we take a look at the aims of the current research trends in educational technologies within the framework of surveillance capitalism. Last but not least we go through a series of cases where the privacy of students has ben compromised. At the end we provide some conclusions.

## 2. (Lack of) Privacy in technologies for education

### 2.1 A good starting point

LMS started to be developed in the early days of the Web, usually purposely built in house in a language like Perl and plain HTML. In the late 90s started appearing the first commercial products as the use of LMS was spreading to all institutions. The LMS market had appeared.

We could say that by the turn of the millennium LMS were already widespread. In the year 2000 most, if not all, educational institutions used some kind of Learning Management System (LMS). Whether as support of traditional lectures, as a Virtual Learning Environment (VLE), or for online learning (e-learning), and everything in between. The LMS tools and configuration were the same.

And we started inadvertently in a situation where LMS implemented really good privacy for the learner data. And that's because in 2000 everybody had their LMS running on campus hardware and the institutions IT crew maintaining it.

Companies like IBM, Blackboard, and WebCT, developed the LMS and provided it as a licensed software product. Something that the institution run on their own IT infrastructure. All the data submitted by the students and the logs about the student's activity would stay the system, in possession and custody of the institution. Just like before the information revolution, it was kept on paper archives. The digital transformation had not changed how the learner information was managed, hence privacy was not an issue to consider.

### 2.2 The time for switching LMS platform 2000-2007

Back in 2.000, each university and education institution needed to run locally their servers. This was expensive in terms of infrastructure, hardware, storage, and complexity in the software architecture and the skills needed to run it smoothly. There was no other choice.

LMS software was expensive in terms of licensing, but also in terms of maintenance, updating the system every year. The IT department received a bunch of CD-ROMs with the new version of the LMS. Then they had to perform the updates and make sure everything worked well with the installation, nothing broke, and the hardware could handle at scale the new version. No small task. This was especially tricky if some customizations were made to the software. In the end, most installations would not update to the newer versions every year. Needless to say, this was a huge security risk.

So, there was an interesting situation in the early 2000s where the option of getting a new LMS was very attractive in the market. That is because an institution was always competing with the three or four-year-old version of the entrenched LMS that was already at a school. Changing the LMS would be often considered a better and easier choice than upgrading to the new version of the installed LMS. Especially when your new vendor had all the incentives to get the institution as a new customer and thus would offer to help with the migration.

This might explain why in the early 2000s LMS like Moodle (and to a lesser extend Sakai) in the open-source world, and Blackboard (as a private vendor) started gaining market share, with institutions switching to their products from old LMS products, to the point that they got most of the market of LMS in learning institutions by 2010 [6].

Another explanation might lie in one problem with the LMS in the early 2000's systems. Every system in the market had a particular plug-in format. So, if a developer wanted to develop a custom feature she had to build it and maintain it for every system.

The open-source Sakai project started in 2004, with Charles Severance - one of the authors- as one of the founding members. Sakai stated purpose was to provide a solution to the problem of interoperability and allow developers to provide extensions to the features of the main LMS. This attracted people and institutions to the platform between 2004 and 2006.

### 2.3 The rise of Learning Interoperability Standards 2007-2010

That kind of scared the established companies, so they came to the table of the IMS Global Learning Consortium to discuss the issue. Sakai led the way in building standards like IMS Learning Tools Interoperability [7] - implemented for Moodle with the participation of some of the authors [8-9] and IMS Common Cartridge [10].

IMS Common Cartridge is an industry-standard that provides a specification that describes the format for creating and sharing primarily educational digital content. The

specification is developed by IMS Global Learning Consortium and describes in detail the packaging format and infrastructure needed to support it and the methods for presenting it to the end-user.

IMS Learning Tools Interoperability (LTI) is the industry established interoperability standard that allows the integration of web-based applications for learning within the context of one activity in a course of an LMS. The students can seamlessly access the learning web application by clicking on a link, while the LMS provides authentication, authorization, and learning context to the provider of the learning tool [7-8].

LTI is more relevant for the present paper because it sets up the requirements to implement a model of Software As A Service of Learning Tools vendors, providing services to learning institutions.

Sakai never really gained all that much market share but had a lot of influence on the other LMS, and by 2008-2009 IMS Learning Tools Interoperability was implemented by all the relevant actors.

But Sakai and Moodle were also imitating blackboard and WebC (later acquired by Blackboard) in that their product was just about providing a piece of software that the customer had to run on its own.

So by 2009, we had LTI plus two major high-quality open-source LMS (Moodle and Sakai), and we had high privacy and reasonably good interoperability.

#### **2.4 The LMS goes to the cloud or becomes a service 2010-2020**

In 2006 Amazon launched its cloud computing platform Amazon Web Services (AWS). AWS with the EC2 service started offering Linux servers (2006), file storage with the S3 (2006), ElastiCache (2011) [11].

AWS and other Cloud Computing platforms that came later solved the problem of hardware scalability and availability. One can launch huge servers to run your software, instantly at a low hourly cost. And then when the workload goes down, give back to the cloud those servers and resources and stop paying for that.

Cloud computing solved the problem of hardware availability but did not solve the problem of managing, maintaining, and updating the software. IT departments were stuck with the same software architectures of the LMS and having to deal with juggernauts like the ORACLE Database and all the complexity it entails.

In addition to that, using AWS before was hard. To use AWS at scale before 2017, which is pretty recent, required a very particular set of technical skills difficult to acquire. Technicians had to be students of AWS to be able to use AWS effectively.

However, this is no longer true. Since 2018 a developer, like the authors, can run servers at production at scale as a side project. That is because the management of the servers has become simpler to manage, to the point that the tasks are almost fully automated. But to do this before 2018 and certainly, before 2015 was impossible.

Then things started to change. Two trends happened in the late 2000s and early 2010s. Universities got tired of running their hardware and they got tired of upgrading their software. Moving servers to the cloud started to be considered a best practice, and an even more attractive option was to have the LMS as a Service.

Canvas was born in the age of the cloud. Canvas implemented good interoperability and simplicity to outsource everything.

Because of LTI and other interoperability standards, it became possible to move the LMS to a Canvas based LMS as a Service in the cloud, while keep on using the preferred Learning Tools from Blackboard or Sakai or Moodle.

Companies like Blackboard, Desire2learn, Moodle, and Sakai didn't react to the emergence of Cloud Computing nearly as fast as canvas did. So Canvas a tremendous advantage that helped to capture about 40% of market share [12].

The proposal of LMS as a Service that proposes Canvas, and then the other vendors run to implement, its equivalent to the mantra "Hakuna Matata" featured in Disney's Lion King: "it means no worries for the rest of your days". It meant that University IT didn't need to have any skills to run the LMS, since it was provided as a Service.

But the outsourcing of in campus online services does not stop here. Google and Microsoft have been offering to education institutions for free for all the staff and students their software as a services suites with integrated email, calendar, cloud drive storage, office apps, online conferencing and LMS like features. We repeat, for free. They just want the data.

As is often said, "When the service is free, the user is the product."

Just like in the movie, the consequences of the carelessness of the "Hakuna Matata" attitude manifested just when the song ended. The outsourcing of the operations, maintenance, and improvement of the LMS to a Software As A Service cloud provider led to a loss of IT developer talent. They didn't have interesting things to do. They lost the ability to affect the LMS to meet faculty needs.

To sum up, we started in the early 2000s where the learning institution operated and kept the information about learners in their infrastructure, just like when everything where stored in paper files. The situation did not present any problem regarding privacy. Over the last 20 years, three technical innovations have transformed the LMS design, architecture, business model, and operations. These innovations are Interoperability standards for learning tools and contents, cloud computing, and Software As A Service.

As a consequence, in 2020, there are universities where there's not a single bit of learner data stored in servers that belong to the institution. The learner data and metadata has escaped the control of the institution. And this creates a lot of potential for issues with learner data privacy.

The situation has changed, and we become aware of this just when privacy has become an issue. Like we exposed in the previous section of this paper.

### 3. Towards surveillance in education

The aim to get and analyze as much data as possible of the user's activity in order to gain the ability to influence their behavior is not an exclusive thing from the usual suspects from big tech (Google, Amazon, Microsoft, Facebook, Apple, Tencent, Alibaba, and Palantir). We find this exact purpose in the big trends in research and innovation in education: Learning Analytics, Gamification, Adaptive learning, and Proctoring [13].

According to Siemens Learning Analytics is the use of intelligent data, learner produced data, and analysis models to discover information and social connections for predicting and advising people's learning [14]. While this definition has been debated, criticized, and modified by the research community the elements of getting as much data about the users, now students and learners often minors, to gain the ability to modify their behavior, now advising people's learning. We have to acknowledge that this definition is not precise enough because teachers are also under scrutiny and managers have, of course at the best heart, the intentions of advising the teachers teaching.

Gamification is the application of game-design elements and game principles in non-game contexts. Gamification involves the design of a set of activities and processes to solve problems to improve user engagement, organizational productivity, learning, knowledge retention, exercise, employee recruitment and evaluation, and more [15]. Gamification is being researched and used in educational contexts and presented as a nice tool of educational innovation for teachers [16]. Again we have the elements of environmental design to nudge users, now students, to behave in the way the designer desires.

Adaptive learning or Adaptive teaching uses computer algorithms and machine learning - fed by data, of course, to orchestrate the interaction with the learner and deliver customized resources and learning activities to address the unique needs of each learner. In professional learning contexts, individuals may "test out" of some training to ensure they engage with novel instruction. Computers adapt the presentation of educational material according to students' learning needs, as indicated by their responses to questions, tasks, and experiences. The technology encompasses aspects derived from various fields of study including computer science, AI, psychometrics, education, psychology, and brain science [17].

In a conference in 2020, a presenter gave a talk about a research about how to determine the student's emotions while working on an online learning platform by analyzing several streams of data, including video from the students. One of the authors asked about the ethics implications of the research. The presenter explained quite proud that the research had been approved the ethics commission of their institution.

It is obvious that the current culture in the community that does research in topics like learning analytics, gamification, adaptive learning, proctoring, and - to much horror for the authors - emotional analysis of the students does not consider that using personal data of the students represents an ethical problem.

But, when set in the framework of surveillance capitalism, education innovation research about Learning Analytics,

Gamification, Adaptive Learning, and other emerging trends seem to fit right in. All this research is about getting as much data about the users, creating models of behavior, and changing the environment to influence the behavior of the users with increasing leverage, without considering the consequences this research might have.

### 4. Examples of surveillance in education

It does not matter what are the goals driving the machine: maximizing profit, influencing an election, pushing a cultural change, or learn better. The possibilities for unintended consequences and bad uses of these technologies if applied on a scale, provide enough ideas for a spinoff series of Black Mirror just devoted to education-related dystopias.

What is certain is that there are incentives in place to get as much data as possible about students and their interactions with learning tools. Just consider the following examples:

The "nonprofit foundation" inBloom who operated a free Software As A Service application to manage student data for public school districts across the EUA, created a database with more than 400 different data fields about students that school administrators could fill in. Some schools administrators collected sensible data such as family relationships and reasons for enrollment changes [18]. The inBloom analytics system was closed down in April 2014, after parents and pressure groups expressed sincere concerns about the misuse of data, the repurposing of data for commercial interests, as well as general safety from cyber-attack [19].

Another case of misuse of students' data is the practice of some colleges or universities to track students [20-21]. Pressures for admissions officers to meet target enrollment numbers have led some HEIs to consider Big Data as their solution. According to Rivard's reporting on the use of data analytics in admissions, recruiters are stratifying and analyzing personal information of potential applicants in order to "target them for certain traits," including income and ethnicity. Further, admissions professionals purchase and analyze datasets sold by the National Research Center for College and University Admissions, the College Board, or by ACT in order to develop predictive algorithms to score whether or not a specific student is likely to enroll given her profile information. In aggregate, the datasets include millions of student names and identifiable information [22].

For example, Houston Baptist University discovered that its models successfully predicted which students would enroll, regardless of whether or not they received costly viewbooks and mailers—the traditional way of marketing to students [23].

In the COVID-19 tracking systems there is Albion's, an attempt to mitigate the potential spread of COVID-19. A college in Michigan is requiring all students to install the app that will track student's live locations at all times. Unfortunately, researchers have already found two major vulnerabilities in the app that can expose students' personal and health data [24].

The Duke Study (from the Duke University) recorded thousands of student's faces. In 2014, thousands of students were walking around campus, going to and from their classes, minding their own business. What they might not have known is that on this particular day, Duke researchers were recording them and putting their likenesses into a data set. This data set would be placed on a public website, and it would be downloaded by academics, security contractors, and military researchers around the globe [25].

In another similar example, a 2014 project by Stanford researchers called "Brainwash," used a camera to take more than 10,000 images over three days of students. The data from Brainwash was then shared by the researchers with others, including academics in China associated with the National University of Defense Technology, and surveillance technology firm Megvii [26].

#### 4. Conclusions

Our globalized society is experimenting with new technologies that have a great impact on itself. A lot of this impact is positive, the authors are no Luddites, but there are a lot of unintended consequences. Just like 20 years ago we were embracing new technologies and their promises we should now pay close attention to the problems. Make no mistake, information technologies are transforming our society, our economy, and our lives. And when we speak of information technologies in education the stakes are even higher.

The current situation is one where the student's data is outside the control of the learning institution. The new learning technologies researched and developed crave this data to create the perfect learning environment, where the students and teachers to what they are kindly enticed to do by subtle manipulation of the digital environments and systems of incentives. Meanwhile, we remain clueless about what should be the right objectives of education, so a perfect learning enforcement system would be a disaster of unprecedented social proportions.

This paper leaves out the aspects of the legal frameworks that affect information systems in education and shall be discussed in a follow-up paper.

We have to start thinking about our Learning Management Systems and interoperability standards, and to consider the ethics of working with personal information of students that can be used for a number of unforeseen purposes and consequences that might extend to the far future. What information they use, for what purpose and for how long, who has the custody, how is protected, and how can we track and control it. We need to develop solutions at a legal, technical, and organizational level, propose best practices and analyze the possible flaws to improve it. This debate is not happening and it is about time.

#### REFERENCES

- [1] The Cambridge Analytica files. The Guardian. Retrieved September 10, 2020 from: <https://www.theguardian.com/news/series/cambridge-analytica-files>
- [2] Tristan Harris. 2017. How a handful of tech companies control billions of minds every day. (April 2017). Retrieved September 10, 2020 from: [https://www.ted.com/talks/tristan\\_harris\\_how\\_a\\_handful\\_of\\_tech\\_companies\\_control\\_billions\\_of\\_minds\\_every\\_day](https://www.ted.com/talks/tristan_harris_how_a_handful_of_tech_companies_control_billions_of_minds_every_day).
- [3] Shoshana Zuboff. 2014. A Digital declaration. Frankfurter Allgemeine. (September 2014). Retrieved September, 10, 2020 from: <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-on-big-data-as-surveillance-capitalism-13152525.html>
- [4] Shoshana Zuboff. 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, 30(1), (April 2015) 75-89.
- [5] Nosedive. 2016. Black Mirror, season 3, episode 1. (October 2016). Retrieved September 10, 2020 from: <https://www.imdb.com/title/tt5497778/>
- [6] Phill Hill. 2016. State of Higher Ed LMS Market for US and Canada: Spring 2016 Edition. In eLiterate. (April 2016). Retrieved September 10, 2020 from: <https://eliterate.us/state-higher-ed-lms-market-spring-2016/>
- [7] Learning Tool Interoperability: IMS LTI 1.3 and LTI advantage. (September 2020). Retrieved September 10, 2020 from: <http://www.imsglobal.org/activity/learning-tools-interoperability>
- [8] M. Alier, M.J. Casany, M.A. Conde, F.J. García-Peñalvo, & C. Severance. 2010. Interoperability for LMS: the missing piece to become the common place for e-learning innovation. *International Journal of Knowledge and Learning*, 6(2-3), (August 2010) 130-141.
- [9] M.J. Casany, M. Alier & F.J. García-Peñalvo. 2009. SOA initiatives for eLearning. A Moodle case. A Moodle case 23rd International Conference on Advanced Information Networking and Applications, AINA 2009, Workshops Proceedings. The International Symposium on Mining and Web (MAW 2009) (pp. 750-755). Los Alamitos, California, USA: IEEE Computer Society.
- [10] Common Cartridge: How Common Cartridge Benefits K-20 Institutions. (September 2020). Retrieved September 10, 2020 from: <https://www.imsglobal.org/activity/common-cartridge>
- [11] Timeline Amazon web Services. (2020). In wikipedia (September 2020). Retrieved September 10, 2020 from: [https://en.wikipedia.org/wiki/Timeline\\_of\\_Amazon\\_Web\\_Services](https://en.wikipedia.org/wiki/Timeline_of_Amazon_Web_Services)
- [12] LMS Market Share For US & Canadian Higher Ed. Institutions. (2018). Online Learning and Distance Education Resources. (2018). Retrieved September 10, 2020 from: <https://tonybates.wpengine.com/wp-content/uploads/LMS-market-trends-2.jpg>
- [13] De Bruyckere, P. (2016). Gartner Hype Cycle for Education. The Economy of Meaning. (2016). Retrieved September 10, 2020 from: <https://theeconomyofmeaning.com/2016/08/09/gartners-hype-cycle-for-education-2016/>
- [14] George Siemens. 2010. What Are Learning Analytics?. Elearnspace. (August 2010). Retrieved September 10, 2020 from: <https://web.archive.org/web/20180628142047/http://www.elearnspace.org/blog/2010/08/25/what-are-learning-analytics/>
- [15] K. Huotari, & J. Hamari. 2012. "Defining Gamification – A Service Marketing Perspective". *Proceedings of the 16th International Academic MindTrek Conference 2012, Tampere, Finland, October 3-5*.
- [16] Linda Casteneda. 2014. Gamificación, que podría haber más allá de microestímulos. February 2014. Retrieved September 10, 2020 from: <https://www.lindacastaneda.com/es/mushware/gamificacionesytic1314/>.
- [17] Adaptive Learning Wikipedia. (2020). Retrieved September 10, 2020 from: [https://en.wikipedia.org/wiki/Adaptive\\_learning#cite\\_note-1](https://en.wikipedia.org/wiki/Adaptive_learning#cite_note-1)
- [18] Natasha Singer. 2014. InBloom Student Data Repository to Close. In Business, Innovation, technology, Society. (April 2014). Retrieved September 10, 2020 from: [https://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?\\_r=0](https://bits.blogs.nytimes.com/2014/04/21/inbloom-student-data-repository-to-close/?_r=0)
- [19] Drachler, H., & Greller, W. 2016. Privacy and analytics: it's a DELICATE issue a checklist for trusted learning analytics. In *Proceedings of the sixth international conference on learning analytics & knowledge* (pp. 89-98).
- [20] Douglas MacMillan, and Nick Anderson. 2020. Student tracking, secret scores: How college admissions offices rank prospects before they apply. The Washington Post (September 2020). Retrieved September 10, 2020 from: <https://www.washingtonpost.com/business/2019/10/14/colleges-quietly-rank-prospective-students-based-their-personal-data/>
- [21] Douglas MacMillan. 2019. Some colleges are tracking students before they even apply. The Washington Post (October 2019). Retrieved September 10, 2020 from: <https://www.washingtonpost.com/podcasts/post-reports/some-colleges-are-tracking-students-before-they-even-apply/>
- [22] W. Kent Barns. 2013. Does Big Data Know Best? NSA and College Admissions. The Huffington Post (June 2013). Retrieved September 10, 2020 from: [http://www.huffingtonpost.com/w-kent-barns/does-big-data-know-best\\_n\\_3460096.html](http://www.huffingtonpost.com/w-kent-barns/does-big-data-know-best_n_3460096.html)
- [23] Rubel, A., & Jones, K. 2017. Data analytics in higher education: Key concerns and open questions. *U. St. Thomas JL & Pub. Pol'y*, 11, 25.

- [24] Kate Cox. 2020. College contact-tracing app readily leaked personal data, report finds. ArsTechnica (August 2020). Retrieved September 10, 2020 from: <https://arstechnica.com/tech-policy/2020/08/college-contact-tracing-app-readily-leaked-personal-data-report-finds/>
- [25] Jake Satsky (2019). A Duke study recorded thousands of students' faces. Now they're being used all over the world. The Chronicle. (June 2019). Retrieved September 10, 2020 from: <https://www.dukechronicle.com/article/2019/06/duke-university-facial-recognition-data-set-study-surveillance-video-students-china-uyghur>
- [26] Malcom Owen. 2019. Facial recognition bolstered by mass database scraping, but not from Apple . Apple Insider. (Juliol 2019). Retrieved September 10, 2020 from: <https://appleinsider.com/articles/19/07/13/facial-recognition-bolstered-by-mass-database-scraping-but-not-from-apple>