



AI in education: learner choice and fundamental rights

Bettina Berendt , Allison Littlejohn & Mike Blakemore

To cite this article: Bettina Berendt , Allison Littlejohn & Mike Blakemore (2020): AI in education: learner choice and fundamental rights, Learning, Media and Technology, DOI: [10.1080/17439884.2020.1786399](https://doi.org/10.1080/17439884.2020.1786399)

To link to this article: <https://doi.org/10.1080/17439884.2020.1786399>



Published online: 03 Jul 2020.



Submit your article to this journal [↗](#)



Article views: 11



View related articles [↗](#)



View Crossmark data [↗](#)



AI in education: learner choice and fundamental rights

Bettina Berendt^{a,b}, Allison Littlejohn^c and Mike Blakemore^d

^aFaculty of Electrical Engineering and Computer Science, Technische Universität Berlin, Berlin, Germany;

^bDepartment of Computer Science, KU Leuven, Leuven, Belgium; ^cUCL Knowledge Lab, UCL, London, UK; ^dEcorys UK, Birmingham, UK

ABSTRACT

This article examines benefits and risks of Artificial Intelligence (AI) in education in relation to fundamental human rights. The article is based on an EU scoping study [Berendt, B., A. Littlejohn, P. Kern, P. Mitros, X. Shacklock, and M. Blakemore. 2017. *Big Data for Monitoring Educational Systems*. Luxembourg: Publications Office of the European Union. <https://publications.europa.eu/en/publication-detail/-/publication/94cb5fc8-473e-11e7-aea8-01aa75ed71a1/>]. The study takes into account the potential for AI and 'Big Data' to provide more effective monitoring of the education system in real-time, but also considers the implications for fundamental human rights and freedoms of both teachers and learners. The analysis highlights a need to balance the benefits and risks as AI tools are developed, marketed and deployed. We conclude with a call to embed consideration of the benefits and risks of AI in education as technology tools into the development, marketing and deployment of these tools. There are questions around who – which body or organisation – should take responsibility for regulating AI in education, particularly since AI impacts not only data protection and privacy, but on fundamental rights in general. Given AI's global impact, it should be regulated at a trans-national level, with a global organisation such as the UN taking on this role.

ARTICLE HISTORY

Received 4 April 2019

Accepted 16 June 2020

KEYWORDS

Artificial intelligence; Big Data; predictive analytics; data protection; fundamental rights; education

1. Introduction

'Artificial Intelligence' (AI) applied to the proliferation of real-time data (Big Data) is promoted as a way to improve education in ways that offer more personalised, flexible, inclusive and engaging learning (UNESCO 2017). To realise these benefits, governments, education sectors and technology organisations have been exploring the introduction of AI tools and platforms to deliver educational system monitoring that is more efficient (with less administrative burden) and effective (with timely, accurate, and informative indicators) than in contemporary education.

AI is defined as '*the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings*'.¹ Much of the current attention is on machine learning and data mining: techniques that use a range of statistical-analytic (algorithmic) methods to harvest, structure and analyse computationally large data sets to reveal patterns, trends, and associations and to derive predictions from these. A system is considered 'intelligent' when it 'learns' from the data it is fed.² In theory, new data – if representative of what they are intended to represent – enable the system to make more informed decisions about new, individual cases.

AI scientists have been adapting machine learning, computer modelling and statistics techniques used in the business sector to improve decision making in educational systems (Nistor, Derntl, and

Klamma 2015; HEC Report 2016). The patterns, trends, and associations identified by AI in educational systems tend to relate to complex human behaviour and interactions. These AI systems capitalise on a range of modelling techniques, such as ‘early alert systems’ that use predictive models to forecast the likelihood of a learner falling behind or dropping out of a course; ‘visualisation systems’ that illustrate learner progress in relation to pre-determined learning pathways; ‘recommender systems’ that endorse resources, people or future actions of the learner; and ‘adaptive systems’ that personalise content, presentation, recommendations and other design elements (Long and Siemens 2011; Wolff et al. 2013; Nistor, Derntl, and Klamma 2015; Papamitsiou and Economides 2014). Many of these systems have been subsumed under the term ‘learning analytics’, which represents ‘the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimising learning and the environments in which it occurs’, with ‘analytics’ referring to ‘statistics, visualization, computer/data sciences, artificial intelligence’.³ To emphasise the numerous connections to other fields in which AI is being deployed, and to encompass AI systems that go beyond data and analytics, we will refer to ‘uses of AI in education’ and similar terms throughout this paper.

Many AI systems in education use data about the choices and behaviour of previous learners to support and enhance learning in a number of ways: providing Intelligent Tutoring (cf. Roll, Russell, and Gašević 2018; Chou, Chan, and Lin 2003); predicting each student’s grades, allowing the system to propose remedial action; introducing new forms of assessment (e.g., *International Journal of Artificial Intelligence in Education*, 28(1), 2018); or linking academic performance predictions with university openings or job applications (Berendt et al. 2017).

Predictive systems offer benefits, alerting tutors about students ‘at risk’ of falling behind. However, there are a number of drawbacks associated with the use of these systems. First, there are risks of amplifying the ‘status quo’ in education (West 2017). Algorithms may be designed to conform to existing processes and to be trained on data that includes existing biases (Custer, King, and Atnic 2018). Thus the use of these systems amplifies existing prejudices, such as gender or ethnicity biases, making it more difficult to change educational approaches and systems. Second, using tools continually to monitor individual students can grow into aggressive tracking and potentially can be used for more sinister applications, such as state monitoring of citizens (Sellgren 2018; Jack 2018). Third, AI systems can (inadvertently) exert influence and control through making decisions that have serious and ill-considered risks and drawbacks associated with them. For example, linking academic performance predictions with university or job applications will likely have a serious impact on an individual’s future choices (Berendt et al. 2017). These risks of AI in education are not always apparent because they are unseen, unintended or unanticipated consequences of the use of AI systems in education (Pringle, Michael, and Michael 2016). These issues are highlighted through a growing number of studies of the legal and ethical issues associated with embedding AI systems in education (Prinsloo and Slade 2016, 2017). However, there have been few analyses of the impact of AI in education on individual freedoms and fundamental rights.

There are significant human rights concerns associated with the use of systems that gather large amounts of personal data about learners.⁴ Large-scale collection and analysis of personal data are of concern to human-rights advocates, who continue to call for strong(er) data protection legislation and implementation (e.g., Watters 2018; Williamson 2015). Thus, the benefits of AI have to be considered alongside a proper assessment, critique and questioning of who are the beneficiaries whose goals are being met, whether educators, students, parents, policy makers or technology companies.

Some scholars have argued that the main beneficiaries of AI in education are the so-called Tech Giants – global technology companies such as *Facebook*, *Google* and *Microsoft* (Watters 2018). These companies have been proposing and offering practical ‘AI solutions’ that are infiltrating education systems globally. Industry initiatives such as *Facebook for Education* (<https://www.facebook.com/education>), *Google for Education* (<https://edu.google.com>) and *Microsoft Education* (<https://www.microsoft.com/en-gb/education>) have led to a ‘creeping surveillance’ embedded within education sectors.

To make sure use of learners' personal data provides benefits for the learners themselves, some governments and supra-national entities (such as the European Union, EU) have made explicit political choices in favour of protecting individual rights. One notable example is the EU General Data Protection Regulation (GDPR), one of the most ambitious and far-reaching attempts to regulate the use of Big Data, which came into effect as law across all EU countries in May 2018. The GDPR is based on the principle that all individuals should have control over how their personal data is used across different contexts, including AI-based decision making. Although GDPR focuses on data protection and privacy rights, its explicit purpose is to protect the fundamental rights and freedoms that underpin democracy. Thus, the GDPR is an important part of the narrative around examination of the risks to citizens associated with the use of AI.

This article considers the benefits and risks to citizens afforded by the use of AI in education systems. Its contribution is that of a critical review of empirical and theoretical literature, informed by our scholarly and professional expertise in educational technology and policy, AI, and data protection and privacy. The article is structured as follows: in Section 2, we examine the benefits and risks citizens face associated with the use of AI in education, by interrogating the choices learners may have about the use of their data. In Section 3, we describe how the risks identified in Section 2 are reflected in the GDPR framework, how these risks might be addressed, and what challenges remain. In Section 4, we make recommendations on how governments might protect their citizens against issues associated with the use of AI in education.

2. The paradox: learner choice

Education systems face a paradox. In formal education systems, such as schools,⁵ participation is compulsory. Even in colleges and universities, learners have to participate in learning activities and assessments that are considered (by teachers) to be beneficial for them. Paradoxically, obligatory participation may be viewed as a reduction of fundamental human rights, including the right to exercise autonomy and to make choices. This paradox comes into sharp focus where learners have to participate in activities and assessments where their data is gathered. Even in situations where data gathering could be beneficial for learners, if the choice is not made freely and in an informed way, it may restrict the learner's autonomy, choice and fundamental human rights. Learners could be given the right to opt out of data collection. However, large-scale data gathering may be regarded as critical for good data quality which may offer learner benefits. Therefore, consideration of how to balance fundamental human rights with data quality and potential benefits for the learner is vital. This section presents a number of case examples of the use of AI in education and interrogates autonomy, choice and the ability to 'opt out' of data collection as a fundamental human right.

2.1. The ability to 'opt out'

Learners may wish to opt out of data collection (or not 'opt in') for diverse reasons, including political objections to surveillance. However, students who are below the legal age of adulthood are (in many countries) not able to legally 'opt in' or 'out' of monitoring. These decisions usually are made on their behalf by parents or legal guardians who may not be aware of the implications of their choices.

The choice to opt in or out of data collection influences data quality. Data gathered may be biased by over- or under-representing specific groups of learners. This problem is difficult to resolve, because it may not be obvious which groups are mis-represented and in what ways the representation of these groups is inaccurate. If datasets are non-representative and biased, the conclusions drawn from data analysis are not reliable. Analysis of these data may accentuate disadvantage by leading to conclusions that discriminate against under-represented learners (cf. the relationships between Big Data, representation, and discrimination discussed by Barocas and Selbst 2016). It is

important that learners can ‘opt out’ of having their data collected, but the act of ‘opting out’ may skew data representation, accentuating disadvantage.

One example of a system that allows students to opt in or out of data monitoring is *OU Analyse*, an AI system developed by The Open University (UK) to provide early prediction of ‘at-risk’ students (Kuzilek et al. 2015). If the student agrees to have their data collected, the system gathers demographic data, including age, gender, place of residence and prior qualifications, and combines these with observed activity within the university’s Virtual Learning Environment (Moodle). Each individual’s data is analysed in relation to data from prior cohorts of students to predict the likelihood of passing the next assessment. These predictions are visualised as a course overview dashboard where the tutor who will mark the assessment can view the progress of each student using a ‘traffic light’ system. The system uses the data to make a decision whether remedial action is needed and recommends to the learner what to study next. While this type of system can be useful in helping a student progress, the use of the system raises fundamental questions such as: who does the system benefit (the student or the organisation)? Is it intended to support learning or to enable the organisation to gain more revenue income? Can the data gathered be used to influence what type of staff are hired? Does the system, which is based on the idea of regular, traditional assessment, impede innovation? Does the system benefit the learners or systems designers who create the analytics to diagnose learning outcomes? Can the system be manipulated?

Systems that focus on supporting students to pass an assessment can be manipulated for all kinds of reasons. For example, the system may make sure students achieve the grades they need to ensure sufficient income stream for the organisation; tutors might focus on preparing students for the exams, rather than on learning specific concepts. There is evidence (Daly et al. 2012) that this already happens in some UK schools in more advantaged areas, where teachers sometimes focus on preparing pupils for university entrance exams, rather than on the broader goal of learning, a strategy sometimes termed ‘teaching to the test’. ‘Gaming the system’ is not a new strategy in educational organisations. There is evidence that educational testing systems have been based on inherent bias. Advantaged students tend to have access to greater support to improve their grades, which means that grades are not a measure of ability, but a measure of what students have achieved with a high degree of supports they have access to. If improvement is rewarded, there is an incentive to downplay performance in the first measurement (Hargreaves and Shirley 2009). These action-related inequities may exacerbate unfairness in educational testing, and this has been the subject of descriptive and remedial research for fifty years (Hutchinson and Mitchell 2019).

Goodhart’s Law states: ‘*When a measure becomes a target, it ceases to be a good measure*’, and this general observation applies in educational settings as much as in the business field where it was conceptualised. The temptation is to try to counter this phenomenon by measuring more, which creates a self-reinforcing dynamic of surveillance (Wright and Kreis 2014, 191). Systems that invite ‘gaming’ behaviour, where people tend to act in ways that they believe will offer them benefits, rather than behaving naturally, affect data quality. Poor quality data will negatively impact equity, which, in turn, may lead to unwarranted surveillance of ‘poorly performing’ students. Surveillance is a major problem of large-scale data collection and analysis, and data protection laws aim at eliminating unnecessary data collection and processing.

Predictive modelling systems were originally developed to help companies with financial planning. These origins raise fundamental questions about who benefits from the use of AI systems in education: learners, teachers, parents, institutions or the technology companies that create the systems. There are questions around whether the data is used to alert education administrators to a potential reduction in the number of students who progress to the next stage, which could lead to a loss of revenue for the organisation. To make accurate financial projections, it is also important for the organisation to predict the level of resources needed to support each student. These data help organisations predict how many students will progress, forecast their likely fee income and predict outlay costs for student support. In the future these data could be used to hire teaching staff on a casual basis, depending on the numbers of students predicted for each cohort and the likely level of

support they need. Therefore, the introduction of AI systems bring closer a consideration of economic concerns associated with the cost of education, the conditions under which teaching staff are employed and the ways students are supported.

Rather than supporting innovation, the use of AI systems can (inadvertently) reproduce and magnify traditional approaches to education. Algorithms that analyse and convert unstructured, institutional data into ‘insights’ are trained on near-real-time data used to support traditional approaches to teaching and learning, where students are guided through a sequential set of content, then engage in an assessment to mark the progress to the next stage (Knight, Buckingham Shum, and Littleton 2013). These data may not be in a form needed to evidence learning progress. There is general agreement that traditional assessment is not an effective means of measuring learning and progress (Brown and Knight 2012), yet assessment data are used in many predictive analytics systems. This arguably makes it more difficult for schools, colleges and universities to change assessment models to more authentic and reliable forms of assessment (Hood and Littlejohn 2018). This problem becomes even more acute where AI systems do not allow students to ‘opt out’ of data collection.

2.2. Systems with limited ‘opt out’

A number of systems are being trialled in schools to monitor children’s progress through continual surveillance and data gathering. A system trialled in schools in China used robots located in classrooms and data chips embedded in each child’s uniform to gather facial recognition and locational data and analyse these to monitor engagement and interaction (Shelton and Xiao 2018). The parent is given the option to opt out the monitoring on behalf of the child. However, as there is strong social pressure not to opt out, parents may consent. Parents may believe it is in their child’s best interest to focus at school and trust that data will be used by the government to help improve education.

Another system trialled in China deployed headsets to detect and monitor brain activity (Jing and Soo 2019) – technology normally used for brain scans in hospitals. Each student wears a headband with small electrodes to measure the brain’s electrical signals to monitor each student’s level of concentration. A red light displayed on the headband when the student is focused turns blue when the student becomes distracted. The information can be sent directly (in real time) to the teacher and parents. While students engage in problem solving activities, the teacher can identify those not ‘paying attention’. At the end of each class the teacher receives a report detailing the overall concentration and variations in concentration levels of each student. However, data quality may be compromised if the headset is not positioned carefully or the student is moving. These headbands are being used to force students to focus on their lessons and it is reported they achieve higher scores (Jing and Soo 2019). However, the stress placed on children through this form of constant monitoring has not been measured. There is pressure on teachers too, since the reports generated could mistakenly be used as a measure of teaching quality. The government receives non-anonymised data which it is free to use. Moreover, the use of these data may not be obvious to the students, parents or teachers (Wall Street Journal 2019). AI systems use that subjects cannot opt out of lead to a reduction of human rights, especially where data legally ‘belongs’ to the data controller and where processing is not transparent.⁶

Data ‘ownership’ and control are a form of power differential. Student data can be highly detailed and distributed across educational administrative systems and commercial platforms, raising complex questions around ownership and control (House of Commons 2014). Learning management systems increasingly store learners’ data in systems that are outside an educational institution. While systems may be intuitively easy to use (for example, clear menus and effective user training), their software design and hardware configuration adds a high degree of complexity. Teaching staff may focus on the teaching and learning functions, rather than understanding the underlying data storage and security functionalities. This can lead to various problems, for example use of a proprietary system such as Dropbox for student work may breach privacy rules, because it stores data ‘in the cloud’ (Kelion 2015). These platforms do not provide teachers and learners sufficient access to their

own data, undermining the individual's ability to self-determine how their data will be used and making teaching processes inscrutable (for an argument involving Coursera, see Dehaye 2016).

Transparency and accountability often are reduced where algorithms and software are proprietary. Even if these systems are open to inspection, the algorithms may be 'non-interpretable' (Lipton 2018). Lack of transparency and non-interpretability can have specific effects, such as 'undetected representation biases' or 'undetected algorithmic biases' (Williamson 2015), increasing the difficulty with which algorithmic systems and power structures can be challenged. This focus on algorithms obscures another problem: the availability and integration of multiple sources of data.

Current trends in computing towards service-oriented architectures (McLellan 2016) and industry concentration (Lynn 2017) make it more likely that large vendors (so-called Tech Giants) control both the algorithmic software and data, opening up opportunities for further linkage and profiling.⁷ This increases the risks of large-scale security breaches⁸ and power differentials and reduces the likelihood of transparency for the user, and of their trust in the data system (Gürses and van Hoboken 2017).

In theory each individual's right to data protection can reduce the power imbalance between the individual and those who control the data (Gutwirth and De Hert 2006), and this form of individual empowerment is one of the main goals of the GDPR (Tsormpatzoudi, Berendt, and Coudert 2016). However, embedding AI systems into education may exacerbate power imbalances and create new, unforeseen disparities. AI systems may shift the locus of expertise and power from teachers and school administrators towards programmers or systems designers who create the analytics to diagnose learning outcomes, predict future educational achievement and to determine who gets recommended for what. These shifts in decision-making pose a range of risks including de-skilling (known from other domains; see Condliffe 2016; Economist 2014) and transfers of public responsibilities and powers to private actors not subject to democratic control (Taekke 2011).

Data-related challenges extend beyond data 'ownership' to embrace effective data control and usage rights. The spirit of the EU GDPR data protection is not concerned with who owns personal data, but focuses on how these data are being protected (no matter who owns them) by enabling individuals to exert control over data about them. Treating personal data as a property allows people to sell their data and data rights, an option that is likely to be chosen by poorer or less well educated people. Thus, the possibility for individuals to sell their own personal data could increase social divides (see De Wolf et al. 2017).

2.3. Lifelong data measurement

Having a lifelong 'record of achievement' has been viewed by governments, education policy makers, teachers and learners themselves as a valuable way to demonstrate their ability to enter educational programmes or gain employment. One problem is that the record may only include formal assessment records. In domains such as computer programming or the design disciplines, achievement is better demonstrated through analysis of day-to-day activity and outcomes, rather than through assessment *per se* (Deno 1985). These activities often are distributed over different sites, such as work, an online forum and social media, rather than in one educational institution or learning system. Therefore, there is a need to gather and analyse data related to achievement distributed across different sites.

There are different techniques for collecting and storing lifelong learner profiles. A common example is the e-Portfolio, where students '*document their learning, deposit and share collections of work, reflect on their learning and showcase their learning and achievements*'.⁹ These e-portfolios allow an audit trail of activity that is useful for documenting learning progress (Kamentez 2015). Blockchain technologies have been proposed as a way to ensure 'authenticity of data' stored in e-portfolios. A blockchain is a distributed record of online activities, or digital events, which has a consensus method to agree whether a new 'block' is legitimate (Sharples and Domingue 2016). This system allows formation of a permanent, distributed record of intellectual effort and reputational

reward. A central claim is that blockchain ‘democratises’ education by opening up records of achievement beyond traditional forms of certification in ways that allow employers to view a wide range of achievements (e.g., Kaplan and Garcia 2019). In reality, blockchain is probably just ‘less insecure’ than existing data security methodologies (Orcutt 2018), and by requiring a shift of trust from institutions to technology (Schneier 2019), it may actually undermine attitudes that are necessary for a democracy to function.

Despite the potential benefits of e-portfolios and blockchain, there are a range of associated risks. The first is the validity of the data and how records of achievement are interpreted by employers. There are many reasons why an individual may demonstrate a sudden dip in performance, but how might periods of low performance be interpreted by future employers? Ideally, when all records of achievement at every point of a student’s journey are recorded, data have to be interpreted in context. However, most analytics systems do not harvest data that takes into consideration the learner’s context and consequences for their learning decisions (Morozov 2014). These systems tend to use quantitative data but there are fundamental questions around the assumptions that make it inevitable to use data that can be quantified, rather than qualitative, contextual data. These contextual data – learner motivations, goals, self-regulation and agency – are difficult to measure but are, nevertheless, critically important to learning (Littlejohn and Hood 2018, 82).

Concerns about context and agency illustrate a further problem associated with data ownership: students need to be able to control their own data and decide whether or not they wish all records of achievement at every point in their lives to be included. Ensuring students are able to make choices about when and how their data is used is an important consideration, to ensure individuals are not disadvantaged. However, the least advantaged are less likely to have access to support and advice to help them decide how to include their data in the system in ways that advantage them. Those learners who already are advantaged are more likely to have support networks to help them manage their own data.

There also questions surrounding who decides to retain or delete data. If data about learning ‘follow’ learners throughout their lives, who stores it, who is the data ‘steward’, can data be selectively deleted? The internet is a massive archive, but often it does not support and allow agency of those the data represent (Lynch 2017).

Educational e-portfolios provide more information about achievement than traditional educational certificates. They offer the convenience of having all certification in one place alongside supplementary information, which allows for more detailed data analysis. However, long-term data, collection can morph into unhelpful surveillance capitalising on the association of learners with ever-more detailed life-long data dossiers. Another issue is that these data, aggregated differently, form detailed life-long data trails that can be associated with teachers and others involved in education. These longitudinal data collections pose challenges which we will address next.

Lifelong, aggregated data represent people as ‘objects’ with ‘measured characteristics’ that are used to predict their futures. However, all humans experience different phases of lifelong development, so, rather than supporting their development, lifelong data could deprive learners of the right to have details about them forgotten. Educational systems tend to focus on recording specific phases, such as childhood or adolescence. However, for some learners these may not be phases of rapid development and data from these phases may not accurately illustrate attainment. There are well-defined moments in time that can become opportunities to forget, for example when data is transferred from one institution to another. These points in time provide learner’s opportunity to shape how their progress is documented.

Another problem is that data collection may undermine the idea of the ‘school as a protected space’. Educational institutions are not simply locations where teaching takes place, but also serve as protected spaces where learners are (in theory) free from social, political and economic pressures.¹⁰ The continuous assessment of student performance, as opposed to being tested at milestone intervals, places learners under continuous stress, emulates a business environment, and may give undue influence to contextual factors such as economic pressures. This means that learners who

are advantaged by having skilled support networks and resources will find ways of maintaining long-term portfolios that benefit them in their future careers. Thus, lifelong portfolios may reduce equity.

3. Approaches towards better governance of AI and Big Data: the case of the European Union's general data protection regulation

Governments are facing challenges in terms of how they provide quality education for increasing numbers of learners while, at the same time, safeguarding fundamental rights of their citizens. The issues discussed in Section 2 raise questions about how education systems should be governed. The European Union's data protection law GDPR is one approach being used by the EU countries to address human rights issues. The GDPR expressly aims to protect the 'fundamental rights and freedoms' of individuals in relation to data protection and privacy (Article 1 (2); see Gutwirth and De Hert 2006, for the relationship between data protection, privacy and fundamental rights, and ICO, n.d., for an overview of GDPR principles).

In terms of learners being able to opt out of data collection (see Sections 2.1 and 2.2), the GDPR requires that personal data be processed only if one of several conditions are met (Article 6). One of these conditions is *consent* (Article 7, Article 4 11.), which has to be freely given and in an informed way. There have been intense debates as to whether users give consent in an informed way (Schiffner et al. 2018).

A second issue is data quality. Section 2.1 illustrated how differential accuracy in the ways different people are represented may lead to poor data quality: data from some groups may be missing, while others may be represented in more advantageous ways. These differentials in data quality may result from inequality, and, through AI and analytics, may reinforce disadvantage. The GDPR recognises data quality as a foundational principles underpinning the processing of personal data ('accuracy', Article 5 (1) d.) of the individuals represented in a dataset. The accuracy with which populations are represented, is indirectly addressed, through Recital 71 which requires procedures that prevent '*discriminatory effects on natural persons*'. At the same time, the need for informed consent outweighs compulsory 'opt-in', even at the expense of data quality.

The law requires and encourages the development and deployment of (often novel) methods to ensure data quality is as good as possible. It is only through the collection of good quality data that equity and fundamental rights can be achieved. These requirements have triggered new areas of research in computer science, AI and related fields. These research areas include investigations of anonymous data collection and processing, de-identification, and fairness, particularly in terms of non-discrimination (e.g., Schiffner et al. 2018; <https://www.facctconference.org/>). Future uses of AI in Education should draw on these developments.

A third issue is the intentional or incidental re-purposing of data (see Section 2.1). One of the GDPR's key principles is purpose limitation (Article 5 (1) b.): to ensure data is not used for purposes other than those specifically named and (in the case of consent-based processing) agreed at the outset. This principle conflicts with the exploratory nature of AI analyses; illustrations include the complex phrasing of consent forms, along with the notion of 'compatible purpose' as well as the general problem of 'mission creep'. These remain major problems in AI research and development which should be controlled.

A fourth issue is associated with 'profiling'. The GDPR highlights a number of risks associated with extensive and fine-grained profiling of people (Article 22 and Recital 71). Profiles (such as e-portfolio profiling described in Section 2.3) are collections of data about individuals that are gathered over an extended period of time. The GDPR mandates that profiling should not lead to discriminatory outcomes. These legal provisions have contributed substantially to computer science and interdisciplinary efforts to develop 'fair, accountable' and 'non-discriminatory' algorithms and systems (cf. <https://www.facctconference.org/>). The GDPR has also introduced a 'right to be forgotten' (primary name: right to erasure, Article 17). However, this right does not include the micro-

management of one's own data. Exercising this right involves careful balancing of the rights of the individual with the rights of the collective.

A fifth issue is transparency, which is related to data 'ownership' (the sixth issue). The GDPR recognises these challenges (highlighted in Section 2.2) and mandates for transparency and fairness as key principles that underpin the processing of personal data (Article 5 (1)). It also requires processors to provide various forms of information that form an 'explanation' of how and why data are processed, including the AI methods deployed (cf. Selbst and Powles 2017 or Schiffner et al. 2018). Arguably the GDPR also makes it impossible to treat personal data as 'owned' in the same sense as other 'objects' can be owned, since data remain 'protected' throughout business or other transactions (Purtova 2017). These legal provisions have contributed substantially to the efforts of computer scientists to develop 'Explainable AI', aimed at making it easier to interpret AI processing (Guidotti et al. 2019). It remains an ongoing challenge to balance the interests of the public in transparency through, for example, code being made open-source (and scrutable) and data subjects being afforded information and explanation rights, with the interests of companies to protect their trade secrets and competitive advantage (e.g., Schiffner et al. 2018). Certainly, the legal mandate of the GDPR to consider data protection from the start and throughout product life cycles ('data protection by design', Schiffner et al. 2018, also known as 'privacy by design', Tsormpatzoudi, Berendt, and Coudert 2016), is a step in the right direction.

There remains a fundamental question around the extent to which AI in education maintains the status quo, instead of facilitating innovation (see Section 2.1). Basing the future on past data is inherently conservative and is predisposed to reproducing the status quo. This issue is at odds with the idea of AI leading to 'innovation' (e.g., Barabas et al. 2018; D'Ignazio and Klein 2018/in press). This issue makes it even important to investigate AI systems critically.

The GDPR is influential beyond the EU countries in which it has been implemented. First, its implementation across the EU regulates the behaviour of entities outside the EU. This includes technology companies that process the personal data of EU citizens. Second, the implementation of GDPR has influenced some non-EU countries to reconsider their own laws (Kpadonou 2019). Third, the implementation of the GDPR is driving research on data and human rights. Despite these positive outcomes, there are serious limitations of GDPR. First, as a *general data protection* regulation, GDPR is not tailored towards any particular domain, such as education. Second, rapid digitalisation is mediated through a number of factors, such as social norms, industry power and industry self-regulation. This makes it difficult for regulation to keep in-step with other influences. Approaches to governance such as the EU's Ethics Guidelines on Trustworthy AI¹¹, are one of the many complementary forms of regulation available. However, these tend to be *general* (in this case for AI¹²) and are limited (in this case being about ethics, which is not legally enforceable).

In summary, laws such as GDPR offer important ways to address the issues associated with the use of AI in education. However, these laws are not sufficient in themselves to solve major issues. A long-term vision is to co-design 'the next GDPR' as a comprehensive regulation of AI.

4. A way forward: promoting learner choice and agency

This article has analysed issues of AI in education, placing emphasis on human rights and the importance of learners 'owning' and 'controlling' their data. Enabling ownership and control requires support that enables individual agency of learners and teachers. Learners should not simply be considered 'data subjects' and should be enabled to exert autonomy over their own data. This is also important for teachers, about whom big personal data are collected and whose expertise and actions may be constrained and undermined by data surveillance.

It is important to strike a balance between enabling autonomy and burdening individuals with the need to manage their data as their data footprint expands (see Shamir 2008). There is a danger that, rather than supporting agency, giving learners options around their data provide the illusion of 'consumer choice' (Jones, Pykett, and Whitehead 2013, 153). A pervasive, digital environment may

encourage learners to behave as passive consumers, rather than engendering democratic behaviour and choice (Björklund 2016). These tendencies towards passive compliance are illustrated in the idea of AI systems as enabling ‘personalised learning’, moving away from the philosophy of learning as a collective action and civic activity. It is important to consider how governments are introducing AI into national education systems. Nations that view education as primarily as an investment in future employability, such as the US and UK, will likely introduce different forms of regulation around AI in education compared with countries that view education primarily as a benefit for society.

In summary, through consideration of the effects of AI in education on individual freedoms and fundamental rights, this article concludes with a call to action to foreground fundamental human rights as a starting point for implementation of AI in educational systems. There is an urgent need to make sure learners and teachers, rather than technology companies and organisations, are the main beneficiaries as AI tools are developed, marketed and embedded in education. However, it remains unclear who – which body or organisation – will take responsibility and how. AI in education extends beyond data privacy and impacts fundamental human rights. Educational institutions are too narrowly focussed to take on this role, because of their inability to influence broader impact beyond educational policy into labour law, consumer protection law and so on. At a national, governmental level, the consideration of human rights will include different perspectives, depending on each country and its associated culture. While laws, such as the European Union’s data protection law GDPR, begin to address some key challenges, these are not sufficient to solve the problems associated with AI in education. Issues raised by the use of AI in education are of global proportion, and provisions are needed at a trans-national level, overseen by (for example) the UN, to monitor and regulate AI systems development across different sections of society, including education. The sooner regulation is implemented, the faster learners, teachers and all citizens can avoid the risks of AI in education undermining their fundamental human rights.

Notes

1. <https://www.britannica.com/technology/artificial-intelligence>.
2. <https://www.britannica.com/technology/machine-learning>.
3. <https://www.solaresearch.org/about/what-is-learning-analytics/>.
4. For our argument, the following three terms can and are used mostly interchangeably: *human rights* in the sense of the Universal Declaration of Human Rights, *fundamental rights* as legally protected human rights, in particular the *freedoms* such as privacy, protection of personal data, expression and education (see Charter of Fundamental Rights of the European Union).
5. Education is not monolithic and children have specific needs and rights (e.g., Livingstone and O’Neill 2014; Lupton and Williamson 2017; Berendt et al. 2017). However, we focus on issues and arguments that hold across different ages and educational contexts.
6. A data controller is “*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*” (GDPR Article 4, 7.). Thus, it is responsible for, and often also performs, data collection and processing tasks.
7. For example, two common platforms integrate *Microsoft Office 365* (EUFolio) resp. *Microsoft Office Online* (Smartschool).
8. Cf. the purchase of Lynda.com by LinkedIn and the subsequent data breach (Barbaschow 2016).
9. Cited from <http://eufolio.eu/>, see also projects such as <http://europortfolio.org/>.
10. <http://www.etymonline.com/index.php?term=school>.
11. <https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>.
12. See the University of Buckingham’s Institute for Ethical AI in Education (IEAIED) position on EU Guidelines (<http://instituteforethicalaiineducation.org/#mission>).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Bettina Berendt is Professor for Internet and Society at the Faculty of Electrical Engineering and Computer Science at Technische Universität Berlin, Germany, Director of the Weizenbaum Institute for the Networked Society, Germany, and guest professor at KU Leuven, Belgium. She previously held positions as professor in the Artificial Intelligence group (Department of Computer Science at KU Leuven) and in the Information Systems group (School of Business and Economics at Humboldt-Universität zu Berlin). Her research centres on data science and critical data science, including privacy/data protection, discrimination and fairness, and ethics and AI, with a focus on textual and web-related data.

Professor Allison Littlejohn is Director of the UCL Knowledge Lab, a centre exploring the future of education with technology in the UCL Institute of Education. She previously held positions as Dean (Learning & Teaching) (University of Glasgow), Academic Director of Digital Innovation (Open University), Founding Director (Caledonian Academy at Glasgow Caledonian University) and Senior Researcher (Royal Dutch Shell). Allison's research focuses on the role of professional and digital learning in addressing global challenges and her work has made contributions to the understanding of how people learn for work in diverse contexts and cultures across the Energy, Finance, Health, Education and International Development sectors.

Michael Blakemore is a Director of Ecorys UK, Emeritus Professor of Geography at Durham University and an Honorary Research Fellow at Durham Business School. He has been a UK EHEA (European Higher Education Area) expert and a UK Bologna Expert. He was Chair for the European Commission of the Marie Skłodowska-Curie Individual Fellowships, Economics and Social Science Evaluation Panel, and joint lead scientist in establishing the 'Digital Transformation - Governance of Human Societies' project at the Joint Research Centre (Ispra) Centre for Advanced Studies. He also served as executive director of Nomis. His recent work has been at the interface between education and employment/business and focussed on the ongoing developments in digital society.

References

- Barabas, C., M. Virza, K. Dinakar, J. Ito, and J. Zittrain. 2018. Interventions Over Predictions: Reframing the Ethical Debate for Actuarial Risk Assessment. *Proceedings of Machine Learning Research* 81, PMLR 2018, 62–76.
- Barbaschow, A. 2016. LinkedIn's Lynda.com Suffers Database Breach. *ZDNet*, Dec. 18. Accessed 25 May 2020. <https://www.zdnet.com/article/linkedin-lynda-com-suffers-database-breach/>.
- Barocas, S., and A. Selbst. 2016. Big Data's Disparate Impact. *104 California Law Review* 671.
- Berendt, B., A. Littlejohn, P. Kern, P. Mitros, X. Shacklock, and M. Blakemore. 2017. *Big Data for Monitoring Educational Systems*. Luxembourg: Publications Office of the European Union. <https://publications.europa.eu/en/publication-detail/-/publication/94cb5fc8-473e-11e7-aea8-01aa75ed71a1/>.
- Björklund, F. 2016. "E-government and Moral Citizenship: The Case of Estonia." *Citizenship Studies* 20 (6-7): 914–931. doi:10.1080/13621025.2016.1213222.
- Brown, S., and P. Knight. 2012. *Assessing Learners in Higher Education*. London: RoutledgeFalmer.
- Chou, C.-Y., T.-W. Chan, and C.-J. Lin. 2003. "Redefining the Learning Companion: The Past, Present, and Future of Educational Agents." *Computers & Education* 40 (3): 255–269.
- Condliffe, J. 2016. DeepMind Will Use AI to Streamline Targeted Cancer Treatment. *Technology Review*, August 31, 2016. Accessed 25 May 2020. <https://www.technologyreview.com/s/602277/deepmind-will-use-ai-to-streamline-targeted-cancer-treatment/?set=602270>.
- Custer, S., E. M. King, and T. M. Atnic. 2018. *Toward Data-Driven Education Systems: Insights into Using Information to Measure Results and Manage Change*. Brookings Institution. Accessed 25 May 2020. <https://www.brookings.edu/research/toward-data-driven-education-systems-insights-into-using-information-to-measure-results-and-manage-change/0>.
- Daly, A. L., J. A. Baird, S. Chamberlain, and M. Meadows. 2012. "Assessment Reform: Students' and Teachers' Responses to the Introduction of Stretch and Challenge at A-Level." *Curriculum Journal* 23 (2): 139–155.
- Dehay, P.-O. 2016. Investigation by Zurich Data Protection Authority of Data Transfers Between the Local University and MOOC Startup Coursera. *Medium*, Apr 1, 2016. Accessed 25 May 2020. <https://higheredrevolution.com/investigation-by-zurich-data-protection-authority-of-data-transfers-between-the-local-university-36b22757361b>.
- Deno, S. L. 1985. "Curriculum-Based Measurement: The Emerging Alternative." *Exceptional Children* 52 (3): 219–232.
- De Wolf, R., E. Vanderhoven, B. Berendt, J. Pierson, and T. Schellens. 2017. "Self-Reflection on Privacy Research in Social Networking Sites." *Behaviour & Information Technology* 36 (5): 459–469.
- D'Ignazio, C., and L. F. Klein. 2018. *in press*. *Data Feminism*. Boston, MA: MIT Press. Accessed 25 May 2020. <https://bookbook.pubpub.org/data-feminism>.
- Economist. 2014. Eyes on the Classroom. *The Economist*. Jul 26, 2014. Accessed 25 May 2020. <http://www.economist.com/news/americas/21608640-close-education-gap-latin-america-must-produce-better-teachers-eyes-classroom>.
- Guidotti, R., A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi. 2019. "A Survey of Methods for Explaining Black Box Models." *ACM Computing Surveys* 51 (5): 93:1–93:42.

- Gürses, S., J. V. J. van Hoboken, et al. 2017. "Privacy After the Agile Turn." In *The Cambridge Handbook of Consumer Privacy*, edited by E. Selinger, 579–601. Cambridge: Cambridge University Press.
- Gutwirth, S., and P. De Hert. 2006. "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency and Power." In *Privacy and the Criminal Law*, edited by E. Claes, A. Duff, and S. Gutwirth, 61–104. Antwerp/Oxford: Intersentia.
- Hargreaves, A., and D. Shirley. 2009. *The Fourth Way: The Inspiring Future for Educational Change*. Thousand Oaks, CA: Corwin Press.
- HEC Report. 2016. *From Bricks to Clicks, Higher Education Commission Report*. Accessed 25 May 2020. http://www.policyconnect.org.uk/hec/sites/site_hec/files/report/419/fieldreportdownload/frombrickstoclicks-hecreportforweb.pdf.
- Hood, N., and A. Littlejohn. 2018. "Disruptive Democratisers? The Complexities and Incongruities of Scale, Diversity and Personalisation in MOOCs." In *Ubiquitous Inclusive Learning in a Digital Era*, edited by E. Ossianilsson, 1–28. Hershey, PA: IGI Global.
- House of Commons. 2014. *Responsible Use of Data*. House of Commons, Science and Technology Select Committee. Accessed 25 May 2020. <https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf>.
- Hutchinson, B., and M. Mitchell. 2019. 50 Years of Test (Un)fairness: Lessons for Machine Learning. In Proceedings of the Conference on Fairness, Accountability, and Transparency, FAT* 2019, Atlanta, GA, USA, January 29–31, 2019 (pp. 49–58). ACM.
- ICO (Information Commissioner's Office). n.d. *Guide to the General Data Protection Regulation (GDPR)*. Accessed 25 May 2020. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>.
- Jack, K. 2018. How AI Can Spot Exam Cheats and Raise Standards. *Financial Times* (London). 20 Aug 2018. Accessed 25 May 2020. <https://www.ft.com/content/540e77fa-9fe2-11e8-85da-eeb7a9ce36e4>.
- Jing, M., and Z. Soo. 2019. Brainwave-Tracking Start-Up BrainCo in Controversy Over Tests on Chinese Schoolchildren. *South China Morning Post*, 10 Apr 2019. Accessed 25 May 2020. <https://www.scmp.com/tech/start-ups/article/3005448/brainwave-tracking-start-china-schoolchildren-controversy-working>.
- Jones, R., J. Pykett, and M. Whitehead. 2013. *Changing Behaviours. On the Rise of the Psychological State*. Cheltenham: Edward Elgar Publishing.
- Kamantez, A. 2015. Nonacademic Skills Are Key To Success. But What Should We Call Them? *nprED*. May 28, 2015. Accessed 25 May 2020. <http://www.npr.org/sections/ed/2015/05/28/404684712/non-academic-skills-are-key-to-success-but-what-should-we-call-them>.
- Kaplan, A., and F. Garcia. 2019. Blockchain is the Next Step in Democratizing Education. *IBM Blockchain Blog*. Accessed 25 May 2020. <https://www.ibm.com/blogs/blockchain/2019/09/blockchain-is-the-next-step-in-democratizing-education/>.
- Kelion, L. 2015. Schools Given Dropbox Guidance After Safe Harbour Warning. *BBC News*, Oct 28, 2015. Accessed 25 May 2020. <http://www.bbc.co.uk/news/technology-34646146>.
- Knight, S., S. Buckingham Shum, and K. Littleton. 2013. Epistemology, Pedagogy, Assessment and Learning Analytics. In *Proceedings of the Third International Conference on Learning Analytics and Knowledge* (pp. 75–84). ACM.
- Kpadonou, M. 2019. With the GDPR, Europe Shows the World the Way. *Leaders' League*, 11 Apr 2019. <https://www.leadersleague.com/en/news/with-the-gdpr-europe-shows-the-world-the-way>.
- Kuzilek, J., M. Hlosta, D. Herrmannova, Z. Zdrahal, and A. Wolff. 2015. "OU Analyse: Analysing at-Risk Students at The Open University." *Learning Analytics Review, LAK15-1*, 1–16.
- Lipton, Z. C. 2018. "The Mythos of Model Interpretability." *Queue* 16 (3): 30–56. doi:10.1145/3236386.3241340.
- Littlejohn, A., and N. Hood. 2018. *Reconceptualising Learning in the Digital Age. The [Un]Democratising Potential of MOOCs*. Springer Briefs in Open and Distance Education. Singapore: Springer.
- Livingstone, S., and B. O'Neill. 2014. "Children's Rights Online: Challenges, Dilemmas and Emerging Directions." In *Minding Minors Wandering the Web: Regulating Online Child Safety*, edited by S. van der Hof, B. van den Berg, and B. Schermer, 19–38. Berlin: Springer.
- Long, P., and G. Siemens. 2011. "Penetrating the Fog: Analytics in Learning and Education." *EDUCAUSE Review* 46 (5): 30–40. (September/October 2011). Accessed 25 May 2020. http://er.educause.edu/articles/2012/7/~link.aspx?_id=82AE6F528BDC4EBFBC17FCD75B3E3E5C&_z=z.
- Lupton, D., and B. Williamson. 2017. "The Datafied Child: The Dataveillance of Children and Implications for Their Rights." *New Media & Society* 19 (5): 780–794.
- Lynch, C. 2017. "Stewardship in the 'Age of Algorithms'." *First Monday* 22 (12), doi:10.5210/fm.v22i12.8097.
- Lynn, B. C. 2017. America's Monopolies Are Holding Back the Economy. *The Atlantic*. Feb 22, 2017. Accessed 25 May 2020. <https://www.theatlantic.com/business/archive/2017/02/antimonopoly-big-business/514358/>.
- McLellan, C. 2016. SaaS in 2016: The key trends. *ZDNet*. Aug 1, 2016. Accessed 25 May 2020. <http://www.zdnet.com/article/saas-in-2016-the-key-trends/>.
- Morozov, E. 2014. The planning machine. *The New Yorker*. Oct 13, 2014. Accessed 25 May 2020. <http://www.newyorker.com/magazine/2014/10/13/planning-machine>.

- Nistor, N., M. Derntl, and R. Klamma. 2015. "Learning Analytics: Trends and Issues of the Empirical Research of the Years 2011–2014." In *Design for Teaching and Learning in a Networked World. EC-TEL 2015*, edited by G. Conole, T. Klobucar, C. Rensing, J. Konert, and É Lavoué, 453–459. Berlin etc.: Springer. LNCS 9307.
- Orcutt, M. 2018. How Secure is Blockchain Really MIT *Technology Review*. Accessed 25 May 2020. <https://www.technologyreview.com/2018/04/25/143246/how-secure-is-blockchain-really/>.
- Papamitsiou, Z., and A. A. Economides. 2014. "Learning Analytics and Educational Data Mining in Practice: A Systematic Literature Review of Empirical Evidence." *Journal of Educational Technology & Society* 17 (4): 49–64.
- Pringle, R., K. Michael, and M. G. Michael. 2016. "Unintended Consequences of Living with AI." *IEEE Technology and Society Magazine* 35 (4): 17–21.
- Prinsloo, P., and S. Slade. 2016. "Student Vulnerability and Agency in Networked, Digital Learning." *European Journal of Open, Distance and E-Learning* 19 (2): 14–34.
- Prinsloo, P., and S. Slade. 2017. An Elephant in the Learning Analytics Room: The Obligation to Act. In *Proceedings of the Seventh International Learning Analytics & Knowledge Conference* (pp. 46–55). ACM.
- Purtova, N. 2017. "Do Property Rights in Personal Data Make Sense After the Big Data Turn? Individual Control and Transparency." *Journal of Law and Economic Regulation* 10 (2): 64–78. <https://ssrn.com/abstract=3070228>.
- Roll, I., D. M. Russell, and D. Gašević. 2018. "Learning at Scale." *International Journal of Artificial Intelligence in Education* 28 (4): 471–477.
- Schiffner, S., B. Berendt, T. Siil, M. Degeling, R. Riemann, F. Schaub, K. Wuyts, et al. 2018. Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative. In *Proc. APF 2018*. Springer LNCS.
- Schneier, B. 2019. There's no Good Reason to Trust Blockchain Technology. *Wired*. Accessed 25 May 2020. <https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/>.
- Selbst, A. D., and J. Powles. 2017. "Meaningful Information and the Right to Explanation." *International Data Privacy Law* 7 (4): 233–242. Available at SSRN: <https://ssrn.com/abstract=3039125>.
- Sellgren, K. 2018. Exam Boards Police Social Media in Cheating Crackdown. *British Broadcasting Corporation (BBC)*. 26 Jul 2018. Accessed 25 May 2020. <https://www.bbc.com/news/education-44965465>.
- Shamir, R. 2008. "The Age of Responsibilization: On Market-Embedded Morality." *Economy and Society* 37 (1): 1–19. doi:10.1080/03085140701760833.
- Sharples, M., and J. Domingue. 2016. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward. In *European Conference on Technology Enhanced Learning* (pp. 490–496). Springer, Cham.
- Shelton, T., and B. Xiao. 2018. "Chinese Schools Enforce 'Smart Uniforms' with GPS Tracking System to Monitor Students." *Australian Broadcasting Corporation*, 28 Dec. 2018. Accessed 25 May 2020. <https://www.abc.net.au/news/2018-12-28/microchipped-school-uniforms-monitor-students-in-china/10671604>.
- Taekke, J. 2011. "Digital Panopticism and Organizational Power." *Surveillance and Society* 8 (4): 441–454. Accessed 25 May 2020. <http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/luhmann/luhmann>.
- Tsormpatzoudi, P., B. Berendt, and F. Coudert. 2016. "Privacy by Design: From Research and Policy to Practice - the Challenge of Multi-Disciplinarity." In *Privacy Technologies and Policy. Proc. APF 2015*, edited by B. Berendt, T. Engel, D. Ikonomou, D. Le Métayer, and S. Schiffner, 199–212. Berlin: Springer. LNCS 9484.
- UNESCO. 2017. *Data Revolution to Measure Equity in Education for SDGs #CIES2017*. 3 Mar 2017. Accessed 25 May 2020. <http://www.iiep.unesco.org/en/data-revolution-measure-equity-education-sdgs-cies2017-3886>.
- Wall Street Journal. 2019. China's Efforts to Lead the Way in AI Start in Its Classrooms. Accessed 25 May 2020. <https://www.wsj.com/articles/chinas-efforts-to-lead-the-way-in-ai-start-in-its-classrooms-11571958181>.
- Watters, A. 2018. *The Stories We Were Told about Education Technology* (2018). Blogentry in Hack Education. Accessed 25 May 2020. <http://hackededucation.com/2018/12/18/top-ed-tech-trends-stories>.
- West, J. 2017. "Data, Democracy and School Accountability: Controversy Over School Evaluation in the Case of DeVasco High School." *Big Data and Society* 4 (1): 1–16. <https://journals.sagepub.com/doi/full/10.1177/2053951717702408>.
- Williamson, B. 2015. Cognitive computing and data analytics in the classroom. *British Sociological Association*. April 2015. Accessed 25 May 2020. http://www.academia.edu/11968853/Cognitive_computing_and_data_analytics_in_the_classroom/.
- Wolff, A., Z. Zdrahal, A. Nikolov, and M. Pantucek. 2013. Improving Retention: Predicting At-Risk Students by Analysing Clicking Behaviour in a Virtual Learning Environment. In *Proceedings of the Third International Conference on Learning Analytics and Knowledge* (pp. 145–149). ACM.
- Wright, D., and R. Kreis, eds. 2014. *Surveillance in Europe*. London: Routledge.