11 September 2019 T-PD(2019)06

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

(Convention 108)

Report on Data in Education

Children's Data Protection in Education Systems: Challenges and Possible Remedies

Directorate General of Human Rights and Rule of Law

Report by Jen Persson, Director of defenddigitalme. The document is an expression of the author's personal viewpoint.

Contents

I. Context

I.1 Introduction

The sensitivity of digitized pupil and student data should not be underestimated. (The International Working Group on Data Protection in Telecommunications Working Paper on e-Learning Platforms. (April 2017))

> "Some of these e-learning platforms and the learning analytics they facilitate have enormous capacity to foster the development of innovative and effective learning practices. At their best, they can enhance and complement the interactions of students, parents and educators in the educational environment and help them fulfil their respective potential. Nevertheless, e-learning platforms may pose threats to privacy arising from the collection, use, reuse, disclosure and storage of the personal data of these individuals." (ICDPPC Resolution on E-Learning Platforms, 2018)

The potential for harm from misuse of the simple digitised record may seem mild in comparison with more complex technologies that are already in use in education. But when one appreciates the scale of pupil databases, containing hundreds of items of personal data, about named individuals, in millions of records at national level, the risks to people and the institutional and reputational risks of even the most simple data loss, may be more apparent.

Significant ethical and governance issues also exist related to emerging technologies: neuro-technology development and post-digital science and require concerted attention from education researchers. (Williamson, 2019)

While Data Protection supervisory authorities grapple with data protection and privacy across a wide range of sectors and can fine or enforce as penalties for failures to meet obligations in the legislative data infrastructure, it is urgent that they hear the same call for concerted attention and take systemic action, to uphold children's rights in education.

In 2009 the Working Party on Article 29 published an Opinion (2/2009) on the protection of children's personal data (General Guidelines and the special case of schools). They recognised that, "from the static point of view, the child is a person who has not yet achieved physical and psychological maturity. From the dynamic point of view, the child is in the process of developing physically and mentally to become an adult. The rights of the child, and the exercise of those rights – including that of data protection -, should be expressed in a way which recognises both of these perspectives."

Children, from those perspectives, each with their own personal experience of cultural, social, economic and political changes in education, may not have changed significantly in those ten years, but the available technology in their classroom has. Children may already be subjected to brain scanning tools, 360º cameras including audio capture, RFID tracking, and interact with augmented reality headsets in the classroom. The introduction of a growing number of technologies and tools into the classroom, means schools have opened their doors, and pupil databases, to a growing number of commercial actors.

Their rights have remained almost unchanged in the decade. But whether they are respected depends largely on the companies behind the scenes, and regulators' enforcement, since controls and safeguards at school level can be very weak.

The current approach means rights are compromised

There is a myth that children don't care about privacy. It is simply not true. There is a breadth of evidence on children's expectations. Children and young people themselves, can be more alert to risks than many adults imagine (Paterson, L. and Grant, L. (eds 2010)) and young people are concerned about privacy, or data getting into 'the wrong hands'.

The Children's Commissioner believes that we are failing in our fundamental responsibility as adults to give children the tools to be agents of their own lives. (Children's Commissioner England, 2017)

At national level, public authorities may need to rethink their approach to the re-use of population wide education data sets for secondary purposes such as risk profiling for interventions, or public policy research, well beyond the scope of the purposes the data were collected.

Public administrative use of education data may become increasingly compromised, if it is felt 'Big Data has rendered obsolete the current approach to protecting privacy and civil liberties.' (Mundie, 2014).

A growing awareness of data misuse will lead to a growing number of data collection boycotts. (Against Borders for Children (UK) (2016-2018) which result in long term harm to both public and commercial interests. (Parent Coalition for Student Privacy, (US) InBloom, 2012-14) and potentially jeopardise the benefits that serve the best interest of the child.

Commercial introductions of products and approaches need better due diligence and consultation. When the online Summit Learning program imposed commercial tech-centric models into public education there was fierce pushback from parents (Summit schools, Kansas, 2019).

Trust is fragile and some practices jeopardise the public's perception of everyday technology in the growing Internet of Things that has also crept into the classroom. Data use that continues to ignore this, increases the collective risk for other companies using personal data. As the Norwegian Consumer Council report #Toyfail suggested in 2016,

> "If it's not scary enough for the public to think that their sex secrets and devices are hackable, perhaps it will kill public trust in connected devices more when they find strangers talking to their children through a baby monitor or toy."

Volume and variety of data actors

The volume of data created and collected in school systems for administration and learning creates staggering implications for the 'datafied child' (Lupton, Williamson 2016).

The numbers of actors involved in the everyday data processing in a child's day, year, and lifetime cannot be visualised.

The purposes of data processing in education can include absence and attendance management, attainment testing and tracking, behavioural surveillance, communications and parental engagement, classroom management and seating, administering cashless payments, safeguarding and countering violent extremism, asset tracking and staff accountability and performance management and benchmarking. All before any data are processed for the purposes of assessing intelligence, supporting learning, homework, or for research purposes.

Without sufficient checks, due to the volume of different individual providers involved in a child's day and lifetime in education, the collection and re-use of children's data across a school life-cycle can expand in ways that schools themselves and parents are not aware.

Data mining and exploitation

In the words of the then education company CEO at Knewton, Jose Ferreira in 2012,

> "the human race is about to enter a totally data mined existence...education happens to be today, the world's most data mineable industry– by far."

For a variety of motivations, there is a rapid growth of commercial actors and emerging technologies in the global edTech market, propagated not only by angel investors and tech accelerators in US and UK English language markets, but across the world. Estimations of market value and investments range widely, from $8bn to research from Metaari, 'The 2018 Global Learning Technology Investment Patterns: The Rise of the Edtech Unicorns', that suggested that Chinese edtech companies were the majority recipients of global edtech investment in 2018, snapping up 44.1% of a total $16.34bn market spend.

At the same time, under the global pressures of poverty, to deliver low-cost state education, and marketisation, the infrastructure to deliver state education is exposed to risk via commercial 'freeware', software that companies offer at no cost, often in a non-explicit exchange for data.

Insufficient training and change management accompanied by the introduction of new technologies, with insufficient learning materials and under-qualified teachers. (Sabates, R. 2010) The complex socio-economic factors for high dropout rates and under-completion of primary school education are not solved by automating education.

Hidden predictions

The potential global implications for the security and stability of the state sector education infrastructures, the personal costs to children in terms of privacy, and effects of habitualisation and normalisation, may last a lifetime for this datafied generation.

In an experiment in the City of Espoo, Finland, in cooperation with the company Tieto, Artificial Intelligence was applied to analyse health and social care data linked with early years education from 2002 -2016. (Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch 2019)

The predictive nature of such surveillance applied to early interventions could have significant impact and inadvertent consequences from an early age.

Artificial intelligence can also be used for low level decision making, such as assigning class seating plans based on the recording of children's behaviour data, analysed in opaque ways to determine room layouts optimised for behaviour. (ClassCharts)

As Lupton and Williamson pointed out in 2017, "Children are becoming the objects of a multitude of monitoring devices that generate detailed data about them, and critical data researchers and privacy advocates are only just beginning to direct attention to these practices."

There has been little consolidated approach to the protection of children's rights in this environment, since the Working Party 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools.) But in the ten years since, the exposure of children to data processing technologies has been rapid and intense.

Building a Rights' Respecting Environment for Life

Concerns about technology and their effects on connectivity and the role of the human in society are not new. Author Anaïs Nin in her 1946 diary wrote about, "the dangerous time when mechanical voices, radios, telephones, take the place of human intimacies, and the concept of being in touch with millions brings a greater and greater poverty in intimacy and human vision." (The Diary of Anais Nin, Vol. 4: 1944-1947)

But the scale, speed and simplicity of data transfer has been exponential since the creation of the Internet and world wide web, while data storage cost has diminished. The barriers to data access, copying and distribution have been diminished through easier accessibility, and with it the protections offered to data subjects in practical terms, have fallen away and failed to be respected by companies and institutions.

In paragraph 8 of its general comment No. 1, on the aims of education, the UN Convention Committee on the Rights of the Child stated in 2001:

> **"Children do not lose their human rights by virtue of passing through the school gates. Thus, for example, education must be provided in a way that respects the inherent dignity of the child and enables the child to express his or her views freely in accordance with article 12, para (1), and to participate in school life."**

As set out in the Council of Europe Recommendation CM/Rec (2018)7 of the Committee of Ministers, member States have a duty to respect, protect and fulfil the rights of the child in the digital environment. If vendors are not rights-respecting, their products should not be used.

Data used in childhood for profiling, and predictive analysis in particular, have the potential to have opaque lifetime effects. And there is enthusiasm in many scientific communities to begin this datafication for risk stratification and interventions, even before birth. Intelligence — the ability to learn, reason and solve problems — is at the forefront of behavioural genetic research. (Plomin, Stumm 2018)

There may be technologies, based on children's data capture, mining, and interpretation, that are determined to be too invasive and too interfering in a child's full and free development, that should not be accepted for children to be exposed to within education. Regulation should be proactive, by requiring cooperation between consumer safety law and data protection

authorities where products and services are introduced to the classroom or are deigned to be used on children.

Regulation should return to robust enforcement of first principles

The full range of human rights enshrined in the United Nations Convention on the Rights of the Child (UNCRC), in the Convention for the Protection of Human Rights and Fundamental Freedoms (ETS No. 5), and their protocols, should be fully respected, protected and fulfilled in education.

This rights-based approach can be described as an impediment to data exploitation and its repurposing for product development and "innovation'.

If it is impossible for a child to give consent to data harvesting, and yet the advantages of an Internet connected classroom are felt to be positive, what measures are meaningful to ensure protection of a child's fundamental rights and freedoms?

The fundamental principles of data purpose limitation, data minimisation and transparency are often inadequate without strong and dissuasive enforcement.

It is furthermore, incumbent upon adults to ensure that protections offered to children are not only appropriate for the duration of their childhood but promote the ability of children to reach adulthood unimpeded and able to develop fully and freely, to meet their full potential and human flourishing.

The principles of necessity, proportionality and practical application of data retention periods should be reinforced to provide for a default position on children's school records of statutory time limitation of identifiable, individual level data.

The single solution proposed by the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their Policy and Investment Recommendations for Trustworthy Artificial Intelligence, should be applied to better protect in the education environment:

> "Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data."

I.2 The education landscape and outlook for technology

Lawmaking and procurement at all levels of government must respect the UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.

> "a State should not engage in, support or condone abuses of children's rights when it has a business role itself or conducts business with private enterprises. For example, States must take steps to ensure that public procurement contracts are awarded to bidders that are committed to respecting children's rights. State agencies and institutions, including security forces, should not collaborate with or condone the infringement of the rights of the child by third parties. States should not invest public finances and other resources in business activities that violate children's rights."

The changing landscape of what is permissible, what is possible, and what is acceptable in education is theoretical for many academics, and policy makers. Three years to trial and bring a product to market, or to discover the efficacy or pedagogy of an edTech tool is poor, could be a short term for developers, but could be more than a quarter of a child's lifetime in compulsory education.

The hope and hype of 2012, the year of the MOOC (New York Times, 2012) has somewhat died down, that free online courses could bring the best education in the world to its most remote corners, effortlessly retrain people in their careers, and 'expand intellectual and personal networks'.

Some remain suspicious of the MOOC business model, leaving lecturers encouraged to participate in MOOC delivery, asking whether students and faculty profit intellectually as investors accrue monetary gains. (Davidson, C.2017)

However, while learning platforms have grown perhaps less well than forecast, the number of new platforms often promising what is perceived as newer technologies, AI and machine learning supported functionalities, are growing. New administrative tools abound in the education sector, often promising reduced workload and efficiency for staff, and better educational outcomes for children. This is at the same time, at least in the UK, as the sector is increasingly managed along business lines and with the promotion of marketisation, falling numbers of state education teaching staff, and education spending.

This brief summary of the state of personal data use gives an insight into some of the types of technology that exist, are in use, and challenge us to pose questions about the suitability and adequacy of the existing data protection regulations in addressing the rights of the child in the education environment.

I.3 Scope considerations

For the purposes of this report, definitions are the same as for the purposes of the Convention. The definition of a data subject is a child, and according to the UN Convention on the Rights of the Child (UNCRC) (para 1); a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier. References may use pupil and student interchangeably depending on country of origin.

The references to data processing in the education sector, do not differentiate between the models of education offered around the world, or whether the provision is compulsory, private or state funded. Rather the author presents a selection of areas within the delivery of education which may involve the data processing of children by authorities and commercial third-parties and is already common and transcends national boundaries.

The same mobility constraints faced by children in accessing educational facilities in sub-Saharan Africa, in Ghana, Malawi or South Africa (Porter, 2010) may not be experienced by children in the United States, but they share the surveillance implications of using digital tools on a mobile phone or portable tablet.

Bridge International for example claims that their "smartphone application allows Academy Managers to seamlessly sync their academy's tablets, pupil and teacher attendance, tuition payments, instructional monitoring, and more."

Criticisms of its 'technology solutionism', standardized high-tech pedagogy developed in their US headquarters and its use in for-profit education, can be seen reflected in other countries. (ESCR-Net- International Network for Economic, Social & Cultural Rights (2018)) In March 2018, 88 civil society organizations joined voices in a collective letter urging prominent financial investors to stop backing Bridge International Academies (BIA), a multinational for-profit corporate network running more than 500 schools in Kenya, Liberia, Nigeria, Uganda and India.

When Silicon Valley solutions Summit Schools were exported to Kansas, they met with strong objections even from children themselves.

Refugees are recognised by agencies and development actors, to be actively avoiding some refugee camps to avoid the capture of biometric IDs. The role of the right to privacy and data protection are not often as clearly demonstrated as enabling rights that underpin the links between article 29 (1) and the struggle against racism, racial discrimination, xenophobia and related intolerance.

The aims, set out in the five sub-paragraphs of article 29 (1) are all linked directly to the realisation of a child's human dignity and rights, taking into account the child's special developmental needs and diverse evolving capacities.

The universality of the principles of the UNCRC should underpin the rights-respecting approach to the data protection of every child.

> (Article 3) "In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration."
>
> (Article 16), "(1) No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. (2) The child has the right to the protection of the law against such interference or attacks."

Recognising that personal data can be processed for necessary administration of education and for the benefit of children, data protection law under Modernised Convention 108, Article 5(4)(a) and GDPR Article 5(1)(a) requires that processing be done, fairly, and in a transparent manner in relation to the data subject. In relation to Internet services, the features of data processing must make it possible for data subjects to really understand what is happening with their personal information. The principle of fairness goes beyond transparency and is linked to processing in an ethical manner aligned with an individual's reasonable expectations.

Where we do include specific issues of data protection and privacy on selected technologies, we exclude consideration of the wider effects that are outside the remit of education and the Council. By example, we omit the future National Security consequences of widespread adoption of biometrics in schools, including voice data collection and fingerprints.

The report is intended to provide assistance to relevant stakeholders in the implementation of the rights enshrined in international and European human rights conventions and standards, with particular reference to the modernised Convention 108.

II. The Challenges and Recommendations

III. II.1 Children's agency

Children should be equipped with the information and skills necessary to enjoy their privacy, protect their reputation and exercise their freedom of expression online (Nyst, (2018)) in line with the evolving capacities of the child.

Navigating the online environment can be especially challenging for children, who often do not understand the commercial nature of the digital services they are using or how their data are used by them. But if it is difficult for children to grasp how their personal data are being collected, processed, shared and monetised online, when they sign up for services themselves, then it is near impossible for them to do so, when school staff make that decision on children's behalf. Even if children were adequately educated and informed about how to manage their privacy, it is impossible for them to do so when schools decide which apps and platforms they will use, on children's behalf.

What children want, is rarely asked. [Stoilova and Livingstone, 2019]

Online commercial providers can be sent children's personal data contained in the school information management system, without pre-notification to families or children. The biggest challenge for the role of schools in education data management, may be for them to accept that their own public task of providing education, that requires some personal data processing, should not by default mean that the same personal data may be passed on to commercial app and platform providers who have no statutory obligation to provide education, and that the companies processing for their own purposes, such as product development, are beyond the remit of the public task.

Children have little opportunity for autonomy in education, or to have control over the distribution of their personal data. But increasingly, schools have lost control of it as well. There are common 'daisy-chains' of data passed from one controller to the next, which originate from collection or creation in the educational setting.

Schools and 'Click-Wrap' commercial terms

Schools set up multiple contracts with outside third parties, often by accepting a standard set of terms and conditions that require a user to click to accept the agreement in order to access the service or application for the first time. These types of agreements are commonly referred to as "Click--Wrap" agreements. Such agreements can mean the extraction of large volumes of pupil data from school information management systems at scale, on the company terms, and without the school's discretion to limit the parcels of data sent to a company, to only the minimum necessary. (US Department for Education (Privacy Technical Assistance Center), 2015) For example, cashless catering systems may access data on religion or ethnicity.

Furthermore, changes to those terms and conditions may not be rejected without the service ceasing to work. They may be sent by email to the school system administrator, by companies such as Google for Education, and any new terms will rarely be communicated to parents or children.

Schools must accept state and government data extractions

In addition to the question of the power imbalance in contracts between companies and schools that want services, there is a significant power imbalance between schools and government at national and local levels. Schools dependent on state funding models have little administrative ability to reject national data requests or the necessary technical ability to withhold data from automated extraction systems, or census data collections in which required fields are pre-determined by the state. Schools may not have a choice whether to submit data where legislation compels the school to submit the data it holds.

Governments should compel the provision or sharing of sensitive personal data only for narrow and strictly defined purposes, and in almost all cases, sensitive data should be kept on local rather than national systems. (Anderson et al, 2009)

> "Government policy and children's online activities raise all kinds of questions about confidentiality and the integrity of data, and they push the vital issue of who can or should consent to the collection, storage and sharing of children's confidential information to the top of the agenda." (Dowty, 2009)

Pupils and parents have little say on their own terms

Public authorities, employers and other organisations in a position of power may find it more difficult to show valid freely given consent, according to the UK ICO. Accordingly, it should not be the routine basis for everyday core data processing.

There are growing and ongoing objections by pupils and families to technology centric impositions in education that claim to restore lost agency to children. While Summit and its funders, including Bill Gates, Mark Zuckerberg, and the Chan Zuckerberg Initiative all claim Summit students are able to demonstrate" "greater ownership of their learning activities," the McPherson Kansas students are actually taking ownership of their education by walking out of school and engaging in sit-ins to protest against its introduction. (Parent Coalition for Student Privacy, 2019)

On leaving school settings, children typically no longer have an ongoing relationship with the institution, however they may continue to process a child's data or maintain relationships with third party vendors who do so. Information about the data held and its processing should be something that is passed on to a family and child, for as long as their data continue to be processed, perhaps on an annual basis.

Recommendations on children's agency.

- Children have the right to express themselves freely in all matters affecting them, and their views should be given due weight in accordance with their age and maturity. It is for public authorities to provide sufficient information and in such accessible manner, to adequately support children's capacity for informed understanding.

- Companies must meet their responsibility to respect the rights of the child in the digital environment and ensure that processing is safe, fair and transparent regardless of product complexity. If it is too hard to explain, processing should not be deemed suitable for

applications using children's data for interventions, that may infringe on their fundamental human rights or freedoms, or with significant effect.

- States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child. (The UN Guidelines on Children in the Digital Environment (2018)) Further support should be offered if it comes to seeking redress. (See I.5)

- Agency should be restored to children and the imbalance of power reduced by requiring that data that leave a setting are not by default identifiable, and identifiable data remains on site, except after assessment of necessity and with accountable approval. Any daisy chain of data onwards distribution must be explainable at the point of collection.

- Apps and platforms should not include direct marketing, or in-product adverts and marketing, in particular using user data to target or measure engagement.

- Minimum viable data should be retained at the point when a child leaves education, and only in the child's best interests, such as to demonstrate attainment, safeguard their future rights of access to necessary and proportionate personal data and to meet statutory obligations. A full copy of their record should be made available to them, with ongoing requirements for data usage and retention reporting, throughout the data life cycle.

II.2 The permanent single record

The importance of a clean slate

In 2009, the Working Party 29 recognised that, "because children are developing, the data relating to them change, and can quickly become outdated and irrelevant to the original purpose of collection. Data should not be kept after this happens."

Ten years on, in June 2019, the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their Policy and Investment Recommendations for Trustworthy Artificial Intelligence, proposed:

> "Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data."

These recommendations and current regulation on data retention are most commonly overlooked in education, based on subjective claims of research exemptions, conflation of de-identification with anonymisation, and risk-averse records management policies that fail to see excessive data as a toxic asset. Enforcement is needed to ensure retention regulation is respected.

Advances in technology have made it possible to store unlimited volumes of personal information about every child in a school, a whole country, or even globally in potentially permanent records.

Excessive retention is impossible for a child to oversee and open to misuse

Those records can be rapidly distributed to other computers in cloud services, and copied unlimited times, to an indefinite number of people, in perpetuity. A child's entire educational record can be shared in a single mouse click. Information that would once have stayed in local records and occupied a large room full of filing cabinets can be fitted on to a portable device, and an entire database of millions of records duplicated and downloaded quickly. Permanent records held by government of ethnicity, of nationality, or of religion have been used to abuse communities throughout history.

defenddigitalme exposed the misuse of national pupil records in 2016 by the UK Home Office for immigration enforcement purposes, when the Department for Education added nationality to the school census. (defenddigitalme, 2016) The risks posed by government misuse for non-educational purposes are too great and demonstrate that national records should not be retained at individual, identifying level.

Comprehensive school census data from children age 2-19 was first collected in 2002, in England, including individual pupil names. Parliamentarians were assured on the changes to the "Central Pupil Database" by the then Minister of State for Education and Skills, that, "The Department has no interest in the identity of individual pupils as such, and will be using the database solely for statistical purposes, with only technical staff directly engaged in the data collation process having access to pupil names."

Thirteen years later under a different government, and in secret, children's names, date of birth, gender and address data began to be matched with records the Home Office sought monthly, for immigration enforcement purposes.

Children have a right to their reputation

The lasting effects of a permanent record and decisions based upon it can follow children into adulthood from state and commercial interventions. Such data can also be drawn on in later years and repurposed easily without an individual's knowledge.

Children's reputations are increasingly shaped by the growing quantities of information available about them online. This not only influences children's interpersonal relationships but may also have an impact on their ability to access services and employment as they enter adulthood. (UNICEF, Children's Online Privacy and Freedom of Expression, Discussion Paper and Industry toolkit, 2018).

Data life cycles need addressed with particular attention for children. Children must have a right to restriction of disclosure to private companies to ensure their full development and adult flourishing in particular for sensitive data, which may not always meet the criteria of special category data. For example, it should be possible for school records with behavioural history to be suppressed from distribution without consent, for purposes beyond the direct care of the individual; records such as violence, sexual misconduct, or drugs, if criminal may be suppressed from release; but as indicators of behaviour and **non**-criminal records, they may be passed on for life to third parties, without a child's (or their later adult) knowledge, and may be sent beyond the school or to other jurisdictions.

In assessing cases of such data processing, there is significant imbalance of power between the school authorities and child, and discussion should be held with families before third-party

distribution. Opt out is an insufficiently robust mechanism of protection in particular since so much data can be extracted from schools in an automated fashion.

When human decision-makers cannot have effective oversight of AI decisions, the broader question arises about whether to adopt these systems rather than human-based methods, in particular for special category data processing at all. (Mantelero, 2018)

Commercial claims for excessive retention should be rejected

Commercial educational product vendors (edTech) while supporting the role of data portability, and records transfer across the same commercial provider to successive schools, should not retain children's unique and identifying records beyond necessity for their education. Subsequent necessary retention for audit purposes should be retained by the local education provider, not vendors. Examination results provide a record of achievement and need to be accessible for as long as individuals wish to reference them, or employers and others may ask for evidence of results. However, classroom behavioural records, sickness and attendee, or usage of apps should not need to be kept in detail by commercial providers.

It is common for commercial online educational services to not allow school staff to delete virtual classrooms, accounts or online content (including student information) but the companies archive them for a period of one to two years or longer instead. (IPC Ontario GPEN Privacy Sweep Report of Educational Online Services, 2017)

Some apps offer a limited window by when a school may request for pupil data to be deleted, after which the company keeps it forever.

Recommendations on the permanent single record

- Follow the HLEG-AI recommendations: (HLEG-AI Policy and Investment Recommendations for Trustworthy Artificial Intelligence) to support the principle of data minimisation:
    - Children should be ensured a free and unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data related to them.
    - Children's formal education should be free from commercial and other interests, and
    - The integrity and agency of future generations should be ensured by providing children with a childhood where they can grow and learn untouched by unsolicited monitoring, profiling and interest-invested habitualisation and manipulation.
- Schools should ensure that pupils' records on departure which are necessary and proportionate to retain, are retained locally but that third parties and commercial vendors in particular without statutory functions, do not maintain a permanent record of the child or their behaviours.
- National records should not be retained at individual, identifying level. The risks posed by government misuse for non-educational purposes are too great.

- Children must have a right to restriction of disclosure of their school records to private companies during their direct education and for indirect secondary purposes.

- Sensitive data that may not meet the criteria of special category data i.e.: school records of behavioural history should be suppressed by default from distribution for purposes beyond the direct care of the individual

- In assessing cases of such data processing, there is significant imbalance of power between the school authorities and child, and discussion should be held with families before third-party distribution. Opt out is an insufficiently robust mechanism of protection in particular since so much data can be extracted from schools in an automated fashion.

II.2.1 Identity management

How do young people create a sense of themselves? The processes of being and becoming through social and institutional interactions, are important for children. Children will develop and manage multiple persona, as they grow up.

The need for younger children to stay anonymous online is generally associated in teaching with stranger danger, and the protection of personal details.

Children under 11 are often regarded as too young to comprehend the implications of online privacy. Researchers at Oxford found that children could identify and articulate certain privacy risks well, such as information oversharing or revealing real identities online. (Zhao et al, 2019) However the asymmetries in the digital age between companies and children means they are particularly susceptible to data exploitation, in part due to them having little sense of the risks posed by the accumulation of personal data over time and by the fact that they may be among the first generation to have their life held in data by companies, from birth.

Recent research has shown that although teenagers are typically concerned about being personally identified by unknown users of their personal data, and reputation management, they failed to perceive the potential threat of re-identification via the particular fragments they shared, e.g., images or geo-location, where they are not considered identifiers, and in particular the concept of longitudinal data are hard to grasp. (Zhao et al, 2019)

In contrast with the changing character of a child over time, the school system may create an immutable central record that grows incrementally and never forgets. A range of third parties may be permitted to each extract a partial version of it. The narrative of personalisation that pervades many learning technologies focuses on the individual. Individualisation consists in transforming human ‘identity’ from a ‘given’ state of being, into a ‘task’ of becoming. (Livingstone, 2016)

The core of the fundamental right to privacy is the freedom from the unlawful interference over and against the government. This is a prerequisite for the freedom to develop one’s identity, in a democratic society. (Hildebrandt, 2015)

The permanent school record and its sharing with others creates increased risk of discrimination through who the system believes we are in, and from, childhood.

The ICDPPC resolution on e-learning platforms, that can be broadly applied, recommends;

> "Consistent with the data minimisation principle, and to the greatest degree possible, the identity of individuals and the identifiability of their personal data processed by the e-learning platform should be minimised or de-identified."

Age and ID verification

Calls for the use of mandatory use of real identity, and age verification mechanisms to validate it for children, are currently gaining momentum. However, both come at a cost to children's privacy and the loss of the safe space that anonymity offers.

Age Verification is a narrow form of 'identity assurance' — where only one attribute (age) need be defined. The method by which this is done is not prescribed, but it would be perverse were the desire for privacy and protection to create more new databases and even more risk. (Booth, P. 2017)

In 2008, the Berkman Center for Internet & Society at Harvard University published a report considering children online and concluded that age verification was not appropriate.

> "Age/identity verification/authentication is a non-solution as it pertains to the online social networking industry or any other online entities where minors interact with adults. We have long believed that the risks were great, and there were no rewards." (Symantec statement, 2018)

Safe apps and platforms allowed in school validated through appropriate procurement and due diligence, and appropriate filtering and blocking of content, should create an environment free from the need for additional age-related protections.

However, educators are also outsourcing identity management through tools, to a wide range of companies, not only for AV, but including social media platforms. Many of which enable social logins to perform the task of log in credentials to other apps and platforms, used in homework and classroom activities.

Social log-ins as ID verification

The ICDPPC (2018) recommended that schools;

> "Avoid the use of social media login as it can result in excessive collection and disclosure of detailed profile and other identifiable information between the social networking site and the e-learning platform and can limit the students' ability to prevent the tracking of their online activities across the web."

Facebook, as an example, is commonly used as group administrative tools in some schools, in particular for older children, and in technical and further education colleges, but the company has been criticised increasingly by US and European regulators for how it treats the information of users and non-users through tracking and website analytics. Its registration and real-name policy mean that personal data are used by the company but may be merged with school accounts where it is required by staff.

School staff should consider their own obligations to protect student and school data very carefully when requiring the use of such platforms, and carefully assess its lawful basis. The hidden uses of personal data, and hidden manipulation by Facebook of user news feeds to create emotional responses, would appear to make their values incompatible with the obligations of educators to respect the rights and freedoms of the child. (Forbes, 2014)

However, this does not stop evangelists for the technology championing its use in the classroom. (Education Foundation, 2013) They suggested in 2013 that it was, "Already being widely used in colleges and universities across the UK and globally, but it has the potential to be a game changer for teachers, schools and the classroom. It is a 'Swiss Army Knife' of tools to unlock learning for young people within and beyond the classroom."

Children and young people have little understanding of what a company can do behind the choices they make that ostensibly manage their privacy settings, using personal data provided for the purposes of user registration. Such uses should be avoided in education.

Biometric data for ID verification

Identity management can also be performed by the interaction between schools and third-party technology providers in house, and via Internet connected services. Biometric data offer high, though still imperfect, degrees of certainty over identity. But there has yet to be debate whether such high-level methods of identity verification should be used for low level transactions, as they are today in schools, such as to register the borrowing of library books and to pay for food and drinks in the school canteen using cashless payment systems.

Facial detection and facial recognition technologies have been established in the education system for some time. The World Economic Forum advocated for the increased use of "fostering social and emotional learning through technology" in 2016.

Biometric ID systems using facial recognition are used increasingly in examinations to verify the candidate not only on entry, but throughout the taking of the test, through constant re-capture of the candidate's biometric features.

In August 2019, the regulatory authority in Sweden, ruled that the introduction of facial recognition system for the purposes of attendance registration was unlawful. (see: II. 6.2 Biometric data) And similar introductions by Aurora Computer Services were already in the news in 2010 in England.

Other biometric wearables and facial recognition systems, though, are being developed for purposes of gathering data about student emotions, engagement and attention in school settings, as a way of delivering data back to teachers on students' social and emotional skills and characteristics, (IEEE, 2018) and in order to 'personalize' the ways they teach.

II.3.1 Data sources, and opaque processing

Not all data are equal, in education there are large differences between data sources:

. Provided by family
. Provided by child
. Created by teachers
. Created by school administrative systems

. Created by Public Authorities
. Created by company's education tools and platforms seen by children and families, and
. Created by third-parties external to the education system, such as data brokers, that may be linked with educational records.

Hidden data

Hidden data include records based on data and/or metadata used by companies to create user profiles about app usage for example, for the purposes of targeting pupils or their parents for advertising and marketing. These are not seen by teachers, parents or children, and can violate e-privacy and consumer laws, as well as data protection law.

For example, the growing trend in UK for wellbeing apps, some of which are undoubtedly subject to the same flaws as mental health apps, researched by NGO Privacy International in 2019. (Privacy International, 2019)

Privacy International published a study of 136 popular web pages related to mental health in France, Germany and the UK reveals how websites share user's personal data with advertisers, data brokers and large tech companies like Google, Facebook and Amazon.

Some depression test websites also leak answers and test results with third parties. The findings show that some mental health websites treat the personal data of their visitors as a commodity, while failing to meet their obligations under European data protection and privacy laws.

Hidden data also include new information or insights created through linkage and secondary re-use of data collected for education but used for other societal assessments by local government, such as predictive scoring of social risks.

These repurposed data analytics uses are far beyond what many people may have reasonable expectation of when they send their child to school and have far reaching implications for privacy and family life.

Health data must be recognised as special category data even in an educational context

Parents in the UK surveyed by defenddigitalme in 2018, considered children's special educational needs data merits extra consideration, before a school passes that sensitive information on to government for secondary re-uses. Those data are not treated as health data, or as having special category features today, despite describing social, emotional and mental health needs, physical disability, autistic spectrum disorder, hearing and visual impairments. (Department for Education, SEND, 2019)

Special category data can be exported behind the scenes through School Information Management systems in bulk processing, without communications to the data subjects. They may also be increasingly extracted through classroom equipment that has no screen and no visible sign of data collection. These need additional recognition and protections.

Repurposing must be made preventable

Collect once, use multiple times may be seen as efficient but can lead to inadvertent data misuse, when the purposes are not compatible or transparent to the child or family.

There is pressure to re-use data collected for direct purposes in school, for the indirect purposes of benchmarking data analytics, to pool pupil data into data lakes, and link school pupil data with higher education student data with other government departments' longitudinal datasets (Graduate Outcomes LEO data, UK Department for Education, Department for Work and Pensions, Her Majesty's Tax and Revenue Collection).

There is growing extensive linkage of education data with other administrative data about the child or family for assessing risk scores and predictive interventions in child abuse detection, domestic violence, and reducing school exclusions (Cardiff Data Justice Lab, 2018). These data were never deigned or collected for such purposes. There is significant risk where decisions are based on collected opinions, not facts.

Many companies assume that processing pupil personal data in order to create de--identified data for other purposes is an acceptable practice without informing families or schools, since data protection law does not protect anonymous data. But this is flawed, not least because the process of rendering data anonymous is itself processing of personal data. It is also difficult to render data anonymous and retain school or location identifiers, even if not seen as personal data, since they can also greatly increase the risk of re--identification.

At the present time there is no method for children and families to be made aware of data repurposing until after the fact. Such data protection breach of principles must be dissuaded by vigorous enforcement.

Recommendations on hidden data issues

- Recommendations must include a prohibition on controllers/providers and their sub processors selling children's personal data collected in the course of their education, including a ban on reprocessing for the purposes of selling the reprocessed data or products built upon it.

- Data linkage should not be routine and must be communicated to the data subjects in advance of new processing, for strictly purposes that are compatible with Article 5(3)(b) of the Convention. The data to which the education data are to be linked must also be made accessible to the data subject. Data processing for similar purposes should follow privacy impact assessment and have ethics oversight where used for research purposes.

- Ensure high standards of consumer protection, privacy, security, and data protection laws are applied to educational apps and platforms consistently and enforced in cooperation, by working together transnationally. (Articles 15, 16, and 17(3))

- Special educational needs data should be recognised as special category data.

- Special educational needs data should be processed accordingly as special category data and require a high bar of exemptions from data protection law, before it could be repurposed from school information management systems or apps. Consent for sharing for direct purposes should allow the same ethical and professional standards as health data and should be given due recognition as confidential data.

- The data minimisation principle in data protection must be respected at the point of collection. The minimum viable amount of data should be collected for narrow purposes.

II.3.2 The role of parental involvement in children's data in schools

Children's rights are treated carelessly and routinely ignored by data controllers in the classroom environment where third parties claim that schools can 'consent' on behalf of their children, while in loco parentis. However, they may not always take decisions that are in the best interest of a child, but in the most practical or convenient interests of the school.

Although the classroom experience is very different from place to place, the emergence of low-cost Internet connected things, hand-held devices, AI and voice supported objects that are easily introduced to a classroom, threaten children's rights at unprecedented global scale, including their privacy, and autonomy and ability to control their digital footprint.

Prevention from misuse in school is an impossible parental task

What if any, distinction must be made between communication to parents about a product introduction for routine classroom activity, and a one-off research trial? What should the expected standards be for ethics committee approval for a product pilot in a school? How can the high bar of consent for special category data processing be met, if children are unable to consent due to age, and in any case, the power imbalance means that a child and indeed parent of any age, may find it impossible to give truly free and informed consent to a school setting, without the choice being to the detriment of the child?

Children's rights need to be protected in a forward-looking manner, based on the principles of Convention 108 as the foundations for their full development without interference, and to champion their full flourishing.

Schools should not override parental responsibilities for a child's digital footprint or create one that they would not otherwise have done, and that cannot be controlled or expunged on leaving education. Parents rights are diminished and disempowered in doing so.

Parental understanding

To promote parental understanding, education records should be accessible to parents. This is currently an impossible task, when perhaps over thirty external data processors may be commonly processing a child's data at any one time. Furthermore, we can ask whether children are well−supported by their parents concerning online privacy risks, and who supports the parents? (Zhao J., 2018)

Zhao argues that,

> "Parents of children aged 6-11 often believe that children are too young to face or comprehend online privacy issues, and often take a protective approach to restrict or monitor what children can access online (at home), instead of discussing privacy issues with children. Parents work hard to protect their children's online safety. However, little is known how much parents are aware of the risks associated with the implicit personal data collection by the first-or third-party companies behind the mobile `apps' used by

their children, and hence how well parents can safeguard their children from this kind of risks," —

Families' awareness is even lower about the tools and their risks in the school environment, outwith parental oversight. To date, institutions appear to underestimate the level of risks and concerns about data processing in schools, and that may be still to catch up with the scale of data processing, as a result of poor parental awareness. Whether schools keep parents deliberately 'in the dark,' or assume there will be no objection since mechanisms are not in place to respect them, is yet to be researched.

A sample of parents' views in England

In 2018, defenddigitalme commissioned a survey of parents' views. The State of Data 2018 survey was carried out online, in February 2018. Survation polled 1,004 parents' opinions of children's data collection and uses of everyday technology in state education in England. Respondents were parents of state-educated children age 5-18 in England. They were asked detailed questions about their child's personal data in school, their understanding of which technologies were used, as well as questions about their attitudes towards the use of children's personal confidential data at national level by third parties.

As many as one in four (24%) parents said they do not know if their child has been signed up to systems using personal data. Most are unaware personal data on every child in school age 2-18 are submitted in the school census to the Department for Education or how a child's personal data from the National Pupil Database are used. 69% of parents said they had not been informed the national Department for Education may give out data from the National Pupil Database to third parties.

Most strongly from all answers, parents appear to consider children's special educational needs data merits extra consideration, before a school passes that sensitive information on to the Department for Education (DfE) for secondary re-uses. Those data are not treated as health data, or as having special category standards, despite reflecting characteristics of social, emotional and mental health needs, physical disability, autistic spectrum disorder, hearing and visual impairments. (Department for Education, SEND, 2019)

- 81% of parents agreed that parental consent should be required before a child's special educational needs data is shared.
- 60% parents agreed parental consent should be required before schools pass data to the DfE National Pupil Database.
- 65% agreed the Department for Education should have parental consent in order to pass children's personal data to commercial data analytics companies.
- Over three quarters (79%) if offered the opportunity to view their child's named record in the National Pupil Database would choose to see it using a Subject Access Request.

In order to enact the recommendations of the ICDPPC and the intentional and purposeful protections of the Convention, there must be a parental right to object to secondary indirect

purposes of data processing, those beyond which a parent does not expect their child's data are processed in the course of their education.

Parents expect that schools will protect and fulfil the rights of the child

In line with the CM/Rec (2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment,

> "States and other stakeholders should ensure that children are made aware of how to exercise their right to privacy and data protection, taking into account their age and maturity and, where appropriate, with the direction and guidance of their parents, carers, legal guardians or other persons legally responsible for the child in a manner consistent with the evolving capacities of the child."

Furthermore,

> "The personal data of children and youth merit specific protection and should be processed only on the basis of sufficient legal ground. Children and youth are entitled to have their privacy protected and must be able to exercise their data protection rights with the support of their parents or guardians. Parents have to be able to assist their children and participate actively in the exercise of these rights." (ICDPPC Resolution on E-Learning Platforms, 2018)

However, the evidence for a lack of awareness and information passed from school to parents, means that parents are disempowered and cannot act to protect their child's rights in school. Unless legislation enables parents to be able to veto a use of a child's personal details already stored by the school, there is no mechanism to object to processing without informed processing. Schools may follow the mantra collect once, use many times and in doing so, fail to inform the parents of additional processing after personal data have been collected for the first time, without a clear and narrow purpose other than for the purposes of the school to enrol the child. It is therefore inadequate to protect a child's fundamental rights and freedoms for the obligation to do so, to fall solely upon the parent.

Parents personal data rights

Parents can also find their own personal data transferred to commercial education companies through the school system, connected to their child's record, without their knowledge.

Particularly manipulative 'bait-and-switch' business models should be unlawful in education. These see schools encouraged to sign up for free products, which then either charge the school at a later date for continuing or extending the service, or that begin to target teachers, and parents via direct email marketing, or in app adverts and marketing for supplementary commercial content.

Parents' own personal data can also be viewed as a mineable data source by schools and educational bodies. The UK education inspectorate, Ofsted, was in talks in 2017 with the Department for Education in a "data science project" to "explore the possibility of using near-realtime data and information from social media and other sources to predict and prevent decline in school performance". The planned snooping on pupils' and parents' social media pages to monitor whether a school's standards were dropping was met with criticism from teaching unions and civil liberties groups, concerned with data unreliability of what may be

untrue statements and gossip, and the harm to public trust of institutional surveillance. (i-news, 2017)

Recommendations on the role of parents

- Public authorities should establish a default position of involving parents in decisions before sharing their children's personal data, unless a competent child refuses such involvement or where sharing poses a risk to the child's best interest.

- Introduce a parental right to object to secondary indirect purposes of data processing, those beyond which a child or parent does not expect their data are processed in the course of their education by the public body. (Indirect uses)

- Consent should be recognised as an exceptional lawful basis for data processing, and not appropriate for routine tasks required of compulsory education. This means that schools cannot assume consent on behalf of parents or children, to provide to third party providers, without an alternative lawful basis for third-party data processing.

- Schools should ensure active freely given consent is required for secondary indirect purposes of data processing, those beyond which a parent would expect their child's data are processed in the course of their everyday direct education, provided for enrolment or in the admissions process. This however should not be deemed sufficient for processing beyond what is reasonable and should not infringe upon a child's rights and freedoms. (For example, photographs for use in school marketing and news reporting)

- Informed parental consent should be required before a child's special educational needs data may be shared outside their direct care and education by the institution the pupil attends.

- Informed parental consent as the lawful basis provided by the institution the pupil attends for data processing, to third parties, should expire upon the child leaving education. The lawful basis must transfer to and be asked of the child at 18.

- Commercial vendors to public education providers should be banned from significantly changing terms and conditions for apps and platforms without re-informing schools, children, and parents, and providing the opportunity to cease processing.

- Parents should be asked for consent before their own personal data are transferred to commercial education companies through the school system, and consent must be informed and freely given, and able to be refused without detriment. For example, parents should not find that their email address has been provided to set up a Platform Classroom account and link a child's record to theirs, where data will leave the school.

- Social media content from personal accounts and public fora, from parents, children or staff, should not be surveilled by schools for any purpose, outwith the school's statutory role and remit, and where there is no lawful basis for the processing of personal data. Where schools fear reputational institutional risk, processing such information should not form part of a child's permanent record.

II.3.3 The role of teachers and school staff

In England, researchers at LSE in 2019 found that, “teachers are unclear what happens to children’s’ data and there is common misunderstanding of how much data leaves a school.” (Stoilova, Livingstone et al (2019))

Further, they found that teachers acknowledge “the numerous challenges they need to address, in relation to the digital literacy curriculum —from the format of delivery and embeddedness of technologies in the learning process to more engaging content focusing on opportunities and positive messages.”

It is surprising perhaps, given the volume of data processing that takes place in a typical day-in-the-life of a child in education, from school-home communications, registration and attendance, facilities and equipment management, learning platforms and apps, classroom tools, behaviour and safeguarding management, homework apps, and the hidden use of pupils’ personal data for benchmarking and measuring school and teacher performance management, that teachers are so ill equipped by the state system to deal with data, that requires so much of them.

Teachers trust the system and providers without training

Teachers may discuss school’s practice around GDPR compliance, but also simply, “trust that the school system works and is properly regulated.”

Basic teacher training and CPD requirements may not contain any basic data protection or children’s rights content. External companies may supply a technology into the hands of teachers who are untrained and expected simply to ‘learn by doing.’

Data protection training is viewed as an addition, rather than integral to public sector teacher training which means for any technology introduction they are inadequately able to assess lawfulness and perform balancing test with fundamental rights.

Due diligence in introductions and Audit process afterwards, need to be part of a risk assessment loop for the lifetime of the child’s education and their data processing, rather than static process carried out at the point of data collection.

Where teachers ask children to use apps, neither party may have adequate information to understand whether the terms and conditions are fair, or how they may process a child’s personal data over their lifetime.

A Data Protection Officer in a school is a necessary role, although it may not be a dedicated member of staff. Under the additional obligations of the Convention (Article 10 (1)) it should be made clear that the officer is necessary for bodies processing children’s data in education, and must have sufficient means, including capacity, to fulfil the duties.

In 2009, Dowty and Korff found that standard of training in information security given to practitioners varies widely, and that in some UK local authorities the inaccuracy of security advice and the inadequacy of security procedures give cause for concern.

Today it is common for the lawful bases for children’s personal data in education to be misinterpreted as all part of a statutory duty, or public task. However, third parties have no public task to fulfil, and for example, most apps’ terms and conditions set out, that they process

on the basis of consent. Teacher and staff training are required, and schools should audit current practices.

Recommendations for schools and staff

- Staff must recognise that children cannot freely consent to the use of third-party services in particular where the power imbalance is such that it cannot be refused, or easily withdrawn. Schools must accordingly address teachers' involvement in product due-diligence and procurement, to ensure respect for child/parental rights in all processing.

- Basic teacher training and professional development should offer mandatory content on basic data protection, privacy, and other related children's rights.

- School agreements should prohibit processing personal data by third parties / providers in order to render it de-identified or anonymous for re-use for their third-party purposes and retention, beyond the purposes of the school's reasonable expectations and purposes, in support of the principles of purpose limitation and data retention.

- 'Click—Wrap' agreements that remove the discretion of a school to control which data may be extracted by a company should be prohibited. Schools must be able to keep control of the data about their children by preventing a provider from changing its Terms and Conditions without a school's ability to refuse and continue service for a fair business transition period.

- Procurement processes should ensure adequate due diligence including risk assessment, and the maintenance of a school-level register of data processing vendors and sub-contractors, as well as a data register of third-party data access and distribution.

I.4 The investigative burden

While children's agency is vital and they must be better informed of how their own personal data are collected and their digital footprint, there is consensus that children cannot, and should not, be expected to navigate a very complex, even for adults, online environment. (Livingstone, 2019)

The investigative burden in schools at the moment is too great, to be able to understand some products, do adequate risk assessment, retrieve the information required to provide to the data subjects, and be able to meet and uphold users' rights. So that much of it does not happen, and staff often accept using a product in ignorance.

By the end of compulsory education, a child's digital footprint is untrackable

Due to changes in contract terms over time, raw data distribution, foreign data transfers, edTech companies using multiple sub processors, and business sale and ownership changes, even the most informed parent and child at the point of data collection may have no mechanism by end of compulsory education, to understand the extent and the distribution of their digital footprint enabled by the school.

Since children are insufficiently well-Supported by their parents concerning online privacy risks, the obligation must fall on schools and their contacted third parties, to ensure the

communication of any data retention and any continued processing when the child leaves an educational setting.

Business too, have a duty to rights-respecting products and practice.

> "Providing transparency about the mechanism's performance to wider stakeholders, through statistics, case studies or more detailed information about the handling of certain cases, can be important to demonstrate its legitimacy and retain broad trust." (UN Guiding Principles on Business and Human Rights (2011)

The 2017 GPEN privacy sweep, noted that "links to privacy policies and terms of service were often absent or hard to find once the account had been created. This means an educator or student cannot easily refer back to the policies and terms of use once they have clicked "I Agree.""

Recommendations on reducing the investigative burden

- Commercial vendors to public education providers should be banned from significantly changing terms and conditions for apps and platforms in the event of a new business policy, or owner, without re-informing schools, parents, and children, with a fair notice period (i.e. one month) and providing the opportunity to cease processing.

- Data Protection Impact and any associated Risk Assessments, including links to third party privacy notices, should be published as part of the due diligence before a new technology or product is introduced to a school.

- On demand and on leaving an educational setting, the body must be able to provide a child with their data usage report, describing the third parties to whom which personal data have been distributed, each retention policy, and expected destruction date.

I.5 Data subject assistance, representation, and remedies

Under Article 9 and 12 of the (modernised) Council of Europe Convention 108, every individual should be able to exercise their rights to redress regards the processing of personal data relating to them. For children the judicial system is inaccessible, incomprehensible and intimidating. (Guidelines on child friendly justice adopted by the Committee of Ministers of the Council of Europe (2010).)

Without support it is therefore impossible for a child to have the possibility to judicially challenge a decision or practice. The assistance to data subjects in Article 18 makes no particular reference to children.

The Council of Europe 2016-21 strategy on the rights of the child, makes clear that all children's rights are considered equal and their views must be accordingly, until adulthood aged 18. "Children have the right to be heard and participate in decisions affecting them, both as individuals and as a group. Indeed, everyone has the right to freedom of expression, as guaranteed under Article 10 of the European Convention on Human Rights. The UNCRC grants children the right to express their views freely in all matters affecting them and to have their views given due weight in accordance with their age and maturity."

> "According to the UNCRC, children shall be provided the opportunity to be heard in any judicial and administrative proceedings affecting them and to access competent, independent and impartial complaints mechanisms when their rights are breached. Furthermore, States Parties to the UNCRC recognise the right of every child in conflict with the law to be treated in a manner consistent with the promotion of the child's sense of dignity and taking into account the child's age and the objective of his or her reintegration into society. In all actions concerning children, whether undertaken by public or private social welfare institutions, courts of law, administrative authorities or legislative bodies, the best interests of the child shall be a primary consideration." (The Council of Europe 2016-21 strategy on the rights of the child, para 37 and 52)

The UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, highlights the challenges in particular for children to obtain remedy to problems online.

> "There are particular difficulties in obtaining remedy for abuses that occur in the context of businesses' global operations." (para 67) "States that do not already have provision for collective complaints, such as class actions and public interest litigation, should introduce these as a means of increasing accessibility to the courts for large numbers of children similarly affected by business actions. States may have to provide special assistance to children who face obstacles to accessing justice, for example, because of language or disability or because they are very young." (para 68)

Children cannot easily enforce their rights, without engaging others. Someone who sues a national government department or global corporation may be faced with a damaging bill of costs.

Recommendations on representation and remedy

- Representation of child data subjects to supervisory authorities (Article 18) should be made easier and strengthened. The data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the data subject rights on his or her behalf, and to exercise the right to receive compensation on his or her behalf where provided for by Member State law.

- Member States may provide that anybody, organisation or association independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the competent supervisory authority and to exercise the rights referred to the Convention if it considers that the rights of a data subject have been infringed as a result of processing. States that do not already have provision for collective complaints such as class actions and public interest litigation, should introduce these as a means of increasing accessibility to the courts for large numbers of children similarly affected by business actions.

- Where regulatory routes have already been exhausted, child litigants who bring a judicial case founded on the Convention 108 should be shielded from court cost orders.

- Subject access rights should be standardised for children to change the inconsistency between different school models of support of parental and child rights to subject access and access to the educational record and the wide variety of school information management systems (stored in schools or offsite on companies' cloud servers which are commonly abroad), platforms and apps in use. Guidance is required by schools, on when competent children may decline the sharing of their educational record with parents and for the provision of personal data to a competent child rather than parent via subject access.

II. 6 Specific technology, trials and emerging issues

The conclusion of Rovrouy's report, Of data and men: Fundamental rights and freedoms in a world of Big Data, applies equally in education as it does to the uses of large-scale data processing as a whole.

> "Accordingly, this "digital revolution" calls for constant vigilance and a continually renewed examination of the relevance and appropriateness of the legal instruments for protecting our fundamental rights and freedoms."

'Big data' in education has all the same issues as other sectors

This report does not attempt to draw up an exhaustive list of all the current and future challenges that data processing in education poses. At most, this report is able to provide a few examples highlighting some relevant issues from the point of view of data protection and, more generally, the protection of fundamental rights and freedoms for a child.

However, the overarching challenge of new and emerging technologies is the desire for vendors and academics to develop and test the products.

Can children be safely shaped by participation in live product trials?

Southgate et al argue in their 2019 report Artificial Intelligence and Emerging Technologies in Schools, commissioned by the Australian Government:

> "AI and emerging technologies need to be carefully 'incubated' in a controlled way in a diverse range of school settings, including rural and low-income school communities, in order to identify practical, safety, ethical and technical issues. This 'incubation' must be accompanied by robust, theoretically informed research on their pedagogical potential and impacts of the technologies on learners and learning."

However, this 'incubation' and in effect live pilot and trials, could be in potential direct conflict with good practice using precautionary principles as demonstrated by the findings of the Swedish Data Protection Authority in August 2019 on trials using facial recognition.

It is vital that the identification of 'practical, safety, ethical and technical issues' is done before applying a technology to children who have no choice but to be in the classroom.

Can state education systems be safely shaped under commercial capture?

There are also significant global players in the sector shaping the available technology and its widespread adoption. They are not always aligned with lawful or ethical practice. Germany has ordered the global platform company, Google, to change its user data processing, which the

DPA ruled was in violation of the country's laws both in 2015 around profiling, and again more recently in 2019, to ensure that personal data were not processed outside the German territory.

Google does enable worldwide users of the school platform Google for Education, and the paid model Google Enterprise, to opt out of data storage in the Russian Federation for example, but users otherwise find their data are split and stored against a variety of server locations, including outside the EU.

The culture and purpose of education are being shaped by global companies as their gradually control the data management infrastructure of large parts of the education sector.

Google has even developed its own language and terms in education just as the company name has become interchangeable with the verb, 'to perform an Internet search,' Google's innovation rhetoric is also about creating particular kinds of subjects beginning with the internalisation of Google's platform values, delivered free to school staff. (Sujon, Z., 2019)

> "The GE (Google Education) roadshow is also about enrolling ordinary people to voluntarily extend the Google universe, for free. The 70 million GFE and GE users are also working for Google in exchange for the promise of educational and personal enrichment. This is the heart of GFE's expansion strategy, one that resonates with those outlined in existing literature addressing Google's soft power, platform and surveillance capitalism, and data colonialism (Srnicek 2016; Zuboff 2019, Couldry and Meijas 2018; Sandoval, 2014; Fuchs 2014; Hillis et al.,2013). Thus, GE is an amazing example of Google's power to make, push and define the terms of educational engagement and to stake claims on educational futures.
>
> While this is a valuable contribution to education and technology studies, many more questions need to be asked, including the question of what is really at stake in this balance between enrichment and colonialism? What is Google extracting from schools, where does it go, and how are they making profit –economic or strategic –from this work? And most importantly, what are the real implications of extending Google's role into young people's lives and into public infrastructures and social institutions?"

Challenges to its market dominance have begun in the US, Switzerland and by parents in Spain, at the time of writing. (Ars Technica, 2019) And authorities and parents are beginning to push back, at the company, that at first glance, is a welcome free gift for schools infrastructure, in times of austerity. (Republik, 2019)

Can the value of a child's education be measured by more than data?

As data analytics becomes an increasingly dominating force in accountability and performance measurement of teachers based on children's data, how we continue to value what machines can't measure in education (Smith, S. (2016)) is a question that needs intentional action to decide what values society wants education to reflect in future.

Inaction will mean companies decide for us, and their values will be the foundation of future societies, and citizens, developed through our education systems.

The UN Committee on the Rights of the Child, in General Comment No. 1: The Aims of Education (article 29) (2001) urges that international bodies concerned with educational policy

and human rights education seek better coordination so as to enhance the effectiveness of the implementation of article 29 (1).

Data protection and privacy law can set parameters on what is permissible from what is possible. It is urgent that the values of those shaping our children through education, are built on universal human rights that prioritise people and their human flourishing; and that includes recognition that data created in the public sector if used for broad public good, should seek to promote full participation in a free society, ahead of narrow private profit.

II. 6.1 Artificial Intelligence and education

Under the supervision of the CDMSI, drawing upon the existing Council of Europe standards and the relevant jurisprudence of the European Court of Human Rights, the MSI-AUT is preparing follow up with a view to the preparation of a possible standard setting instrument on the basis of the study on the human rights dimensions of automated data processing techniques (in particular algorithms and possible regulatory implications).

From personalised learning platforms to automatically identifying dyslexia in children (Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch (2019)) AI currently occupies a significant amount of debate space and funding in sectors of academia, policy makers and industry.

> "Companies are thoroughly engaged in a reimagining of capacities, skills and dispositions required of young people — as well as of professional teaching practitioners in a period of significant technological and economic change. Late in 2016 IBM and Pearson joined forces in a new global partnership." (Williamson, 2017, Big Data in Education)

The UNESCO Beijing Consensus on Artificial Intelligence and Education published in May 2019 offers guidance and recommendations on how best to harness AI technologies for achieving SDG 4. However, such advocacy rarely asks if, how and why personalisation delivers a better educational experience or outcomes. To date, the limited evidence of such comes from the product vendors or their incubators.

Bias and discrimination in data are universal issues

The Consensus did conclude from a rights position on AI in education that,

> "the development and use of AI in education should not deepen the digital divide and must not display bias against any minority or vulnerable groups."

Whether or not 'monetisable' personalised solutions address causes of inequalities and has potential to better address them is only beginning to be assessed by independent third parties. (Davies, H., forthcoming)

New technologies with vast data processing power, and opaque practice or decision-making capabilities, have significant implications for education in the public sector and as a workplace in particular, whether in recruitment, in data analytics, or prediction and interventions.

With respect to data-intensive applications, such as AI collecting user interactions-data every two seconds, the role of ethics committees is attracting increasing attention in AI circles,

though there is no a unanimous consensus on their nature, independence or function. Theoretical studies, policy documents and corporate initiatives all offer differing and sometimes contradictory solutions in this regard.

Children's rights can be infringed by product design choices

There need be no conflict between privacy and innovation, yet some product development in emerging fields, including machine learning, Artificial Intelligence, biometrics, and facial recognition technology, can quickly infringe on rights, at scale. Data Protection and privacy by design take a precautionary approach and this is especially important for data processing in interventions with children.

Southgate et al point out in their 2019 report Artificial Intelligence and Emerging Technologies in Schools, commissioned by the Australian Government, that:

> "Luckin and colleagues (2016) also identify the potential for AI teaching assistants to be used to unfairly or surreptitiously surveil the performance of teachers (using pupils' data), a point supported by Campolo et al. (2018) who recommends that 'more research and policy making is needed on the use of AI systems in workplace management and monitoring' (p.1). Other concerns include the way in which AI aims to change learning behaviour through making recommendations, using persuasion and offering feedback, which may not ultimately be in the best interests of the learner. There are some who suggest that AI learning companions that are intended to support students on their lifelong learning journeys 'may result in the perpetual recording of learner failure to the detriment of future progress' (Luckin et al., 39).
>
> "Boyd and Crawford's (2012) observation regarding big data is particularly relevant in the AI context: 'Many (people) are not aware of the multiplicity of agents and algorithms currently gathering and storing their data for future use.' (p.673). This leads to the third area of awareness - Students, parents and teachers should be made fully aware of AI data harvesting, storage and sharing arrangements with informed parental opt-in consent and student assent obtained. This is supported by the recommendations from the IEEE (2017)."

On October 17, 2017, the Article 29 Working Party ("Working Party") issued Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (the GDPR). The Working Party does not consider Recital 71 to be an absolute prohibition on solely automated decision-making relating to children but notes that it should only be carried out in certain narrow circumstances (e.g., to protect a child's vital interests).

However, the regulation of these tools, may be leading us to accept the use of the technology in ways that should be questioned as to necessity, more robustly.

> "In short, the preoccupation with narrow computational puzzles distracts us from the far more important issue of the colossal asymmetry between societal cost and private gain in the rollout of automated systems. It also denies us the possibility of asking: Should we be building these systems at all?
>
> "Artificial intelligence evokes a mythical, objective omnipotence, but it is backed by real-world forces of money, power, and data. In service of these forces, we are being spun potent stories that drive toward widespread reliance on regressive, surveillance-based

> classification systems that enlist us all in an unprecedented societal experiment from which it is difficult to return. Now, more than ever, we need a robust, bold, imaginative response." (Powles, 2018)

Awareness and education are vital, but not a panacea. Some technology and its data processing will infringe on rights even where the processing is transparent, because the full risks, including those time-shifted risks, may not be. States must recognise the need to educate children about their own data and how they are used, to enable them to adequately understand the effects of their digital history on their future, in education and in the workplace, and to be able to challenge automated decisions where they seem unfair in accordance with the Convention Article 9(1)(a), to be able to develop fully to fulfil their potential.

Recommendations on data use with automated decisions and AI

- The principle of Article 9(1)(a) of the Convention needs developed fully into guidelines for education, and in ways that are rights respecting and understandable for children. Any AI or profiling should be explainable, and in a way that can be understood by a child.

- The High-Level Expert Working Group on Artificial Intelligence (HLEG-AI) proposal should be adopted into guidelines and legislation: "Children should be ensured a free unmonitored space of development and upon moving into adulthood should be provided with a "clean slate" of any public or private storage of data."

- Any product testing and pilot should be treated in the same manner as a research trial requirement ethics committee oversight, privacy and risk impact assessment, opt-in consent, and for non-participation to not be at the detriment of the child.

- Profiling should only be carried out in certain narrow circumstances (e.g., to protect a child's vital interests) and children's attainment should not be routinely profiled in order to measure systems i.e. for benchmarking schools or teacher performance management.

- Where AI is employed, the development and use must be assessed to ensure it should not deepen the digital divide and does not display or entrench bias. Any use with a child or using data from children, must require data protection and privacy impact assessments.

- Policy makers should adopt the IDPCCP approach on e-learning platforms, that where data is used for automated assessments or decisions which affect learners beyond the narrow confines of the educational experience provided by the platform, this process should be transparent to educators, learners, and parents. The latter should always be provided the right to object to use, and to challenge resulting assessments and decisions.

II. 6.2 Biometric data

Using one's biometric data is a more data intrusive way of accessing schools services than a PIN or swipe card. Many different types of biometric technology have been used in schools. The biometric most used is fingerprint, used in UK schools since 1999. (King, P., (2019))

These technologies have been established for some time. The Marie-José school in Liege, Belgium, was equipped despite mounting criticism even in 2007.

Biometric measurements are used already around the world in education to administer cashless payment systems, manage locker and print facilities, particularly to authenticate student identity, ensure academic integrity, and enforce security.

Over 2 million children were estimated to have been compelled to have their fingerprints processed in UK schools and by commercial canteen service providers before 2012, when legislation, The Protection of Freedoms Act 2012, Chapter 2 Protection of biometric information of children in schools etc. was introduced in England and Wales to deal with consent required when schools process children's biometric data. Schools must gain written parental consent if they wish to store/process a child's biometric data as of 1st September 2013. However, in 2019, a survey commissioned by defenddigitalme, found that of the 1,000 parents whose children were using biometrics in schools, 38% had not been asked for permission. The question is therefore open whether or not permissive legislation for such high stakes special category data, that may be vital to verification in adult life for significant transactions, should be used at all in schools for comparatively trivial processes.

Should biometric data be prized or habitualised?

Research with children carried out by Sandra Leaton Gray and Andy Phippen, and documented in their book, Invisibly Blighted (UCL IOE Press, 2017) found concerning evidence of this normalisation of biometric surveillance, and that schools, freely collected biometric data with little concern for children's privacy rights:

> "While technically the value of the biometric to administrators is clear, what is more concerning is that there is no consideration of the worth of this comparatively high-value biometric to the individual. Indeed, it seems as though it is being undervalued by being associated with something as mundane and everyday as the school cafeteria or library. This is particularly significant given the age of the individuals concerned, and the fact that their social identities are still being heavily influenced by the institution around them, namely school."

Biometrics technologies, however, such as fingerprint and iris scanners, are becoming increasingly prevalent in schools and universities too, particularly to authenticate student identity, ensure academic integrity, and enforce security. (Paul, 2017)

Iris scans and monitoring eye movement are often used in conjunction with learning platforms and automated online proctoring solutions. These will attempt to authenticate and re-authenticate online learners' identities using facial recognition by way of webcams and frequent data collection during an examination.

Facial detection and recognition

Facial detection and facial recognition technologies have been established in the education system in China for some time (Greene, 2018), and are starting to be employed in a wider range of school settings in a number of different ways.

The Swedish Data Protection Authority (SDPA) decision on Skellefteå kommun ruled in August 2019, that the introduction of facial recognition system for the purposes of attendance registration was unlawful and ordered the school authority to pay a dissuasive monetary penalty of 200,00 Swedish crowns (£16,800, $20,700) for the violations of privacy and data

protection law. Consent could not be freely given for the sensitive data collection, there was no prior consultation with the supervisory authority, and inadequate data protection risk impact assessment.

It is important that this decision sought to protect children's rights and not accept the inappropriate use of manufactured 'consent'. The infrastructure for widespread adoption of facial detection and recognition systems in schools and wider society deeply concerns civil liberties groups and some in the academic community, though awareness of its introduction in schools, is as yet low in parents.

Schools commonly already routinely have an image database of every enrolled child, and many use closed circuit television cameras for site surveillance.

> As Selwyn notes in the Data Smart Schools project, involving researchers from Monash University & Deakin University,
>
> "Another factor hastening the implementation of facial recognition systems in schools is the prevalence of video monitoring and closed-circuit surveillance infrastructure…. surveillance cameras systems placed everywhere from playgrounds to student toilet areas. School enthusiasm for surveillance technologies has also seen the tentative adoption of teacher body-cameras, fingerprint enrolment and RFID-tagging of students." (Selwyn, Data Smart Schools, 2019)
>
> "Using RFID is already commonplace in countries, such as Brazil, where the sociocultural landscape welcomes an additional layer of tracking children, to protect against potential threats." (Taylor, 2017)

CCTV alone, brings with it its own risks for children's rights to privacy and data protection. There is a great deal of evidence on children's experience and own views on CCTV, how they invade individuals need for privacy in bathroom areas, the mistrust generated, and work arounds of technological surveillance have impacts and implications that were not anticipated. The uptake of CCTV in schools continues apace, as rarely as its usage beyond crime control is ever raised and dissenting and critical voices are seldomly given a platform (Taylor, Rooney (2017).

There is a presumption that school CCTV is only about crime prevention, but in fact documented uses in the UK have included exam invigilation, surveillance of teacher performance, and to bring about chilling effects on pupil behaviours.

From analysis of global news about technology implementations there is clearly significant disparity in cultural norms and expectations of children's and parental privacy, between and within countries, and that the rights of the child are not equally accepted.

It was reported in July 2019, that the Delhi government planned to install CCTV cameras in all government schools by November. The data would however not remain onsite, but be cloud based so as to enable parents to be provided with live CCTV video feeds in order to keep a watch on their child's behaviour in school, "for a limited amount of time, via a mobile app called 'DSG live'." (Vatsalya, Youth Ki Awaaz 2019)

Such systems are often introduced with limited technical capability in schools. Mistakes can leave systems open to breach, such as discovered in February 2018 when UK schools' CCTV

images were found broadcast live on a US website with data feeds from the unsecured cameras, reportedly “showing hundreds of pupils going about their day.” In this case, CCTV was not capturing images from private spaces in toilets. But it can be common.

Body cameras and head cams are also becoming more prevalent where schools choose to use them for behavioural monitoring. Web cam activation can also be remotely controlled. In the cat of Robbins v. Lower Merion School District, the schools could take web cam photographs of children secretly, while they were in the privacy of their homes.

Recommendations on biometrics

- Controllers of children’s biometric data should be required to register this explicitly with supervisory authorities.

- Biometric data definitions should expand to recognise personal data collection not only for verification of identity, but for use to influence physical or mental experience, such as physical attributes and experience in immersive virtual reality; voice, eye movement, mood, mental activity, polygenic scoring, reactions to neurostimulation, and data for the purposes of emotional developmental influence, nudge and change.

- Prohibit the use of facial detection and recognition in education, among other biometric data processing of children, for insignificant routine activities, with exceptions for use in support of people with disabilities, for example in screen eye tracking for their system access and for their direct benefit.

- Biometric data collection should remain within the educational setting.

- Respect for the Rule of Law must continue to be a leading principle in any developing standards. These may want to consider alignment with forthcoming standards of processes for AI.

II.6.3 Safeguarding and countering violent extremism

In 2009 The Working Party 29 suggested that, “It should never be the case that, for reasons of security, children are confronted with over-surveillance that would reduce their autonomy. In this context, a balance has to be found between the protection of the intimacy and privacy of children and their security.’ (Opinion 2/2009 on the protection of children's personal data)

But today school safeguarding software company Gaggle CEO, Jeff Patterson recognises some of the safeguarding software used in schools are deeply invasive. “Privacy went out the window in the last five years. For the good of society, for protecting kids.” (Education Week, May 2019)

Without enforcement of practical applications in the intervening decade, children’s privacy has been downgraded by vendors in education, no longer valued as a right, but as a commodity. The price to be paid for companies that claim to offer security in its place.

In Principles for Children’s Online Privacy and Free Expression, Carly Nyst (United Nations Children’s Fund (UNICEF) 2018) and an accompanying toolkit for industry, set out some of the risks of the software tools used to offer safeguarding in schools online.

> "Children's privacy online is placed at serious risk by those who seek to exploit and abuse them, using the Internet as a means to contact and groom children for abuse or share child sexual abuse material. Yet children's privacy is also at risk from the very measures that have been put in place to protect them from these threats. Laws designed to facilitate the prevention and detection of crimes against children online often mandate Internet monitoring and surveillance, oblige intermediaries to generate and retain personal information, and provide government authorities with access to privately-held data. Meanwhile, at home, popular parental control mechanisms to monitor and restrict Internet access promise to expose every last detail of children's online activity"

An assessment of the key providers of such software in the UK and US by defenddigitalme in 2018-19, found that personal data were processed outside of the home territory, and it was common for no information at all to be given to parents or the children about how the systems work or the profiles that systems generated.

There are conflicting stories of the ability of staff to edit records and delete errors. Searches involving cliffs and black rhinos have earned children flags as potential suicide risk and gang member respectively. These are simply wrong, but staff may be unable or unwilling to delete the flags, rather, "If a keyword is triggered which the school deems to be a false match, a note can be added allowing the reviewer to explain why." This means inaccurate information may recorded against a child, without their ability to see that record or to have it corrected.

The research also found that fifty per cent (50%) of schools impose a Bring-your-own-device policy which is an opaque level of surveillance of personal property, active wherever logged in to school network, and some at all times, regardless of network connection.

The behavioural effects on children's use of the Internet as a result, are under researched, but their qualitative feedback suggests a chilling effect on searches for sexuality, health, and teenage development questions.

This may exacerbate rather than diminish children's vulnerability to risks.

On filtering, The UN Special Rapporteur's 2014 report[1] on children's rights and freedom of expression stated:

> "The result of vague and broad definitions of harmful information, for example in determining how to set Internet filters, can prevent children from gaining access to information that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use. This may exacerbate rather than diminish children's vulnerability to risks."

As state concerns about how to counter violent extremism have increased since 2001, what is considered significant by these softwares, has drifted from clear intent to action classed as terrorism, into more vague and broad terms of extremism and radicalisation. What systems might flag as suspicious, or a 'risk', has drifted from some assessment of intent and capability

[1] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression https://documents-dds-ny.un.org/doc/UNDOC/GEN/N14/512/72/PDF/N1451272.pdf

of action, towards interception and making interventions for potentially insignificant inferred assumptions of disposition towards such ideas.

The outcomes of these data collections include creating profiles about children labelled terrorism and extremism, self-harm, and mental health concerns.

Analysis carried out by Professor Andy Phippen, of the evidence from 4,507 of 6,950 schools in England that carried out e-safety self-reviews, shows school staff are not equipped to deal with or challenge the outcomes from these technologies.

Data linkage under the umbrella of child protection creates a surveillance panopticon

One step further, from applying CCTV to school spaces, and web monitoring to surveil children's personal activity online, is to join it all up into a panopticon of authorities, law-enforcement and a child's private communications.

Facial recognition technologies are being developed for education institutions to address similar concerns (Guardian, 2019), with 'emotion detection' technologies being proposed to detect school violence events.

In June 2018, as part of their efforts to prevent school shootings, Florida (US) lawmakers mandated the creation of a centralized database that would combine individual-level pupil records from the state's law-enforcement and social-services agencies with information from pupils' personal social media accounts. (Herold, Education Week)

> "the Florida case gives us a taste of the potentially huge scope of the re-appropriation, re-circulation and re-combination of school data. It also points to the need for caution before generating any single data point on a student or teacher that is personally identifiable, and therefore able to be connected to other personally identifiable records.
>
> "Many Florida politicians and parents understandably see the state's plans as a valid use of student data in the name of 'school safety'. This is an emotive area, with few effective responses in a country that is seemingly unwilling to introduce effective gun control. In such circumstances, increased digital surveillance offers a compelling alternative for policymakers and school officials keen to be seen to be 'doing something.'"

Research with parents and their teenagers has shown that current tools often work counter to parents' and children's values of privacy, and they would prefer tools to facilitate parental mediation of children's use of technologies rather than providing surveillance capabilities. (Zhao, 2019)

Recommendations on data processing in safeguarding

- The use of web monitoring a child that builds personal profiles should end, and be used for generically filtering and blocking content, not monitoring individuals. Systems should not be intended to catch children out or for covert surveillance. This capability should be regulated in law due to the capacity for extensive intrusion into privacy and family life, to freedom of expression, to a full and free development through their chilling effect.

- Transparency duty: Commercial companies providing child monitoring services should be regulated and required to transparently report on an annual basis. This may include corporate considerations such as filtering rates and content, blocking and monitoring capability expansion, monitoring and blocking appeal routes. Any monitoring at child level should require a reporting obligation to report on children's profile categories, data retention, access and distribution, logfile volumes and content, correction rates and redress. At school level, a report should be provided to parents and pupils on an annual basis, made available on request, and be regularly reviewed to ensure practice complies with principles of necessity and proportionality and increase transparency of any discrimination and bias.

- Fairness: To ensure children and young people are informed about their data processing before it begins, schools and colleges should provide pupils, parents and staff with adequate information, tailored for different age groups, to understand how their online activity is monitored and recorded, and that and how they can be tracked, profiled and reported to third-party agencies and bodies. Before being asked to opt-in to Home-School IT agreements, pupils and parents must be informed how systems work and of its foreseeable consequences. Requirements should be set out in a Statutory Code of Practice.

- Targeted home web monitoring of children for the purposes of State countering violent extremism programmes identified in education, should further require judicial oversight.

- The capability and use of webcams to photograph a child without their knowledge should be banned in schools. It is deeply invasive and impossible to enable for only the rare and exceptional need for individuals, but not open it up to misuse for many.

- States should ensure that the processing of special categories of data, which are considered sensitive in accordance with Article 6 of the Convention, such as genetic data, biometric data uniquely identifying a child, personal data relating to criminal convictions and related security measures, and personal data that reveal racial or ethnic origins, political opinions, religious or other beliefs, mental and physical health, or sexual life and orientation, should in all instances be prohibited, except in exceptions where appropriate safeguards are explicit, transparent, and enshrined in law.

- Camera use should never be covert. Data should be collected locally and retained for the minimal amount of time that is necessary and proportionate.

II. 6.4 Horizon scanning: cognitive science, affective and behavioural nudge

Educational environments are increasingly using online technologies that aim to identify and manage students through affect. These forms of monitoring can be understood as a method of approaching students through the lens of positive psychology. (Nemorin, 2018)

In 2017 Wired magazine revealed that the UK government's 'Nudge Unit' or the Behavioural Insights Unit had been experimenting with using machine learning algorithms to rate how well schools were performing, and they were opaque by design:

> "Data on student's ethnicity and religion were deliberately excluded from the dataset in an effort to prevent algorithmic bias. Although some factors will

> influence the algorithm's decision more than others, Sanders refused to say what those factors where. This is partly because he doesn't want schools to know how the algorithm makes its decisions, and partly because it is difficult to know exactly how these algorithms are working, he says. "The process is a little bit of a black box – that's sort of the point of it," he says.

Regulation of one particular technology is often ineffective, since a small change to a design can render it out of scope of the intended protections. However, over the coming decade, student data may be collected through the use of increasingly advanced technologies that become increasingly physically and psychometrically invasive, such as those that can detect individual psychological characteristics, physical traits, neural activity in the brain, and genomic information from DNA. If States decide to use these at scale, whether to covertly assess its institutions or individuals, or does not understand exactly how the technology works, people need significant protection from hidden harms.

None more so, than children who are still physically and mentally growing and malleable.

What protections have our children in school from unproven, untested or unwanted brain and behaviour shaping technologies?

Researchers in Australia recently concluded that, "there are ethical and safety issues associated with immersive VR (virtual reality). Some of these include the potential for young children to potentially experience false memories and cybersickness (which is like motion sickness). There are ethical and legal concerns around the areas of privacy, intellectual property and copyright, especially in regard to student and teacher creating and sharing VR content." And on AR (Augmented reality they found similarly, "There are ethical and legal concerns around the areas of privacy, intellectual property and copyright, especially in regard to student and teacher creating and sharing AR content."

Ben Williamson of Edinburgh University provided a comprehensive contribution to some of the current issues in technology being used in education and how children can exercise their agency.

> "In the field of psychology, 'digital psychometrics' and 'digital phenotyping' have emerged as ways of constructing detailed psychological profiles of individuals from online activities, although they have been tarnished by association with microtargeted political advertising. (Mats, S., Wired, 2017)
>
> Nonetheless, aspects of digital psychometrics are beginning to surface in education. The OECD Study on Social and Emotional Skills, for example, will use an online survey instrument to assess young people according to the OCEAN personality model. (OECD, 2018) OCEAN is the same five-factor personality model used by Cambridge University digital psychometricians in the myPersonality test delivered over Facebook. Other organizations involved in the movement to assess social and emotional learning and skills are also exploring innovative technologies to conduct digital psychometrics within the education sector. (McKown, 2017)
>
> Biometric technologies such as wearable skin sensors and facial recognition are fast becoming of interest as educational applications. (Hand, 2019) Wearable biometrics are perhaps most clearly in evidence in physical education, where a range of devices has been launched for gathering physiological data from students. (Pluim, 2016)

‘Neurotechnologies’ such as brain-computer interfaces and neurostimulators are already being developed and trialled to gather data on students’ neural activities during educational activities. (Williamson, B. 2019) For example, BrainCo has developed a headband that reports ‘real-time’ brainwave data to a teacher’s dashboard to indicate levels of attention and engagement and inform neuro-feedback-based brain-training programs to improve students’ concentration. (Jing, M., 2019)

Similarly, researchers from the University of Cambridge have developed a wearable ‘cognitive biometric’ device that tracks ‘diaphragmatic neuro-respiratory signals’ as proxies for states of concentration and arousal. FOCI uses machine learning to analyse and visualise the results, and a ‘focus-enhancing AI Mind Coach’—based on cognitive training, positive reinforcement and neurofeedback techniques—to provide ‘real time advice to optimise focus’. Other developments in neurostimulation are designed to more actively intervene in students’ brain states. (FOCIAI, 2019)

Neurostimulation techniques such as transcranial electrical stimulation (tES) have been explored for their potential as cognitive enhancers with young people.

According to a review of neurostimulation research in relation to education, the use of tES techniques has been linked to improvements in several cognitive domains, including memory, attention, language, mathematics and decision-making, some of which have been found to be long-lasting. (Schuijer, J. (2017)

Educational neuroscientists are increasingly interested in the potential of neurostimulation, (UCL, Centre for Educational Neuroscience, 2019) which is also catalysing an industry in cognitive enhancement technologies marketed directly to consumers.

Bioinformatics is the computational study of human DNA. Recently, bioinformatics studies have begun to emerge in education using a method called ‘polygenic scoring’ to make predictions about students’ school attainment, achievement and intelligence from their genetic data. (Williamson, B. 2018). These ‘big data’ studies in bioinformatics are opening up the possibility of genetic data being used increasingly to ‘personalise’ education according to students’ inherited genetic propensities and behavioural characteristics. Other companies may see market potential in educational genomics, such as start-up producers of cheap DNA kits for genetic IQ testing in schools, ‘intelligence apps’, or other genetic ed-tech products.” (Zimmer, 2018)

What should the face of education look like?

The fact that a national Department for Education and parliamentary Committee should consider the role of genetics in the underachievement of working-class boys should give us all pause for thought. (Underachievement in Education (2014) House of Commons Education Committee)

If genetic predictions become accepted as forecasts of a child’s future ability in education, new approaches may emerge to artificially select future generations (Conley, Fletcher 2017), or to target interventions, thereby anticipating a ‘eugenics 2.0’ for selecting ‘smarter’ children (Regalado, 2017) or treating children differently not based on individual presentation and needs apparent to teaching staff, but decided by their data.

> "Companies may see market potential in educational genomics, such as start-up producers of cheap DNA kits for IQ testing in schools, 'intelligence apps', or other genetic ed-tech products.
>
> "Consumer companies such as *23andMe* have exploited the sequencing of the human genome to launch genetic testing services as commercial products, exemplifying movements in the biomedical field to subject personal data to corporate control (Stevens, 2016b). In the same week the SSGAC study was released, *23andMe* also agreed a $300million deal with big pharmaceutical company *GlaxoSmithKline* to apply machine learning and artificial intelligence to analyse data from its 5 million customers for medical discovery and pharmaceutical innovation, positioning itself as part of the infrastructure and bio-economy of genetic pharmaceuticals and education alike." (Zimmer, 2018)

Critics argued that the things we associate with intelligence are too complex and ambiguous to pin down in such a simplistic way. Meanwhile, eugenicists used the emerging concept of intelligence in their campaign to recast society. (Zimmer, 2018)

There is an argument for regulation to ensure children can reach adulthood in as unaltered a state as possible without interference with their body through altered reality or behavioural nudges based on euro-technology or opaque uses of data, to emerge with their autonomy intact, in a world increasingly active in making hidden nudges to covertly influence behaviour and emotional states, in order to make their own decisions.

II. 7. Tools for privacy basics

II. 7.1 Privacy risk assessment

In the face of these advances in the volume and velocity of data collection and transfer, and the next level of technologies already with access to children in the classroom in trials, there is urgent need for regulation to support rights in practical and meaningful ways.

Assessment of risk in data processing is not a onetime risk at the start of data collection but is spread across the life cycle of data processing. Indeed, some of the most significant risks may be shifted to the future adult. That should be reflected in the assessment carried out, and the information given to children and families as a result, at the start, during, and at the end of their personal data processing. This would increase informed processing and raise controllers' awareness of their accountability role and for risk.

Data Protection Impact Assessments about children must be tailored to them. (The Danish Institute for Human Rights. 2016) and adequately explain passive data collections. Invisible information about a child whilst in school (RFID, beacons, virtual assistants in the classroom and Internet Connected Things) can create a vast digital footprint that neither the family nor child nor even the teacher may have actively provided.

Data impact assessments must become routinely integrated into procurement processes. Lawmaking and procurement at all levels of government must respect the UN General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.

Data impact assessments need to be published in the public sector, especially in education and where there is children's data processing, that gives civil society and families the opportunity to scrutinise the data processing activities of third parties.

II. 7.2 Data Minimisation

The data minimisation principle in data protection must be respected at the point of collection if children are going to have any opportunity to minimise their digital footprint created in education. Personal data processing should be adequate, relevant and not excessive in relation to the purposes for which they are processed, but in education there is conflation of purposes between the many users of data inside and outside education systems. The minimum viable amount of data should be collected for narrow purposes.

Increasingly, personal data processed in the context of education are not stored only with the school administrator, but also sent to external storage locations as 'institutions rely on external, cloud-based providers to store and process pupil data.' (International Working Group on Data Protection in Telecommunications Working Paper on e-Learning Platforms. (April 2017))

Data import and export are quick and at scale. A variety of companies act as data integrators offering to be the man in the middle for data transfers in a controlled manner. However, as data storage costs have dropped, so has the volume of data collected risen, and offers the possibility of increased longitudinal data profiling and data linkage.

As suggested by Mantelero in the Big Data Guidelines, (2017), it is recognised that data minimisation poses challenges for AI product training. However, the technology sector appears to often to content itself with acceptance of children's privacy as the cost of dealing with AI, rather than seeking out the more privacy-preserving solutions. The call for more data to feed AI systems is often loud, but regulators should avoid confusing want with necessity. There are also a range of techniques available for preserving privacy which can be used to minimise data processing at the training phase.

Binns, R (2019) Research Fellow in Artificial Intelligence (AI), and Gallo, V. Technology Policy Adviser, discuss some of the techniques organisations can use to comply with data minimisation requirements when adopting AI systems, in a recent blog on the ICO AI Auditing Framework:

> "Some of these techniques involve modifying the training data to reduce the extent to which it can be traced back to specific individuals, while retaining its utility for the purposes of training well-performing models. This could involve changing the values of data points belonging to individuals at random – known as 'perturbing' or adding 'noise' to the data — in a way that preserves some of the statistical properties of those features (see e.g. the RAPPOR algorithm).[2]
>
> These types of privacy-preserving techniques can be applied to the training data after it has already been collected. Where possible, however, they should be applied before the collection of any personal data, to avoid the creation of large personal datasets altogether.

[2] http://www.chromium.org/developers/design-documents/rappor

A related privacy-preserving technique is federated learning. This allows multiple different parties to train models on their own data ('local' models), and then combine some of the patterns that those models have identified (known as 'gradients') into a single, more accurate 'global' model, without having to share any training data with each other. Federated learning is relatively new but has several large-scale applications. These include auto correction and predictive text models across smartphones, but also for medical research involving analysis across multiple patient databases.

While sharing the gradient derived from a locally trained model presents a lower privacy risk than sharing the training data itself, a gradient can still reveal some personal information relating to the data subjects it was derived from, especially if the model is complex with a lot of fine-grained variables. Data controllers will therefore still need to assess the risk of re-identification. In the case of federated learning, participating organisations are likely to be to be considered joint controllers even though they don't have access to each other's data."

Supervisory Authorities should encourage organisations and governments to promote a rights framework and values that avoid pay-for-privacy models of data processing, which intrinsically disadvantage children financially, and will increase the disproportionate exploitation of more marginalised children, young people and families, living in poverty.

II. 7.3 Audit mechanisms

Audit mechanisms should be adopted by schools to enable children and families to understand Who Knows What About Me. (Children's Commissioner, (2017) UK) These could include annual reports from school and their data integrators, to facilitate an overview of which third parties had access, for what purposes, and for use by how many natural persons. It is not enough for a family to be able to understand what was done with their child's personal data, from a general processing policy, one-size-fits-all, on a school website.

II. 7.4 Subject Access and Usage Reports

Trust in use of confidential data is affected by understanding data security, anonymisation, having autonomy and control, knowing who access will have, how accurate are records, how people are kept informed of changes, who maintains and regulates the database, and how people will be protected from prejudice and discrimination through use of their data.

Recommendations on school transparency

- Fair processing notices must be tailored to children in education. It is insufficient to post a privacy notice on a website to meet fair processing obligations.

- Subject Access Requests about children must be tailored to them in how they can make requests, read the resulting information, and have accessible routes of redress.

- To close the loop with Data Protection Impact Assessments at the start of any data collection process, subsequent data processed reports, "Data usage reports" must be made available on request, and on an annual basis, to demonstrate that what children were told would be

done with their data in privacy notices, is what happened in practice, for the full life cycle of the data processing.

- Data retention and destruction plan notices should also be introduced as routine, when a child leaves an educational institution, and completes each stage of compulsory education (nursery, primary, secondary, further, Higher).

- Educational settings should publish an annual 12-month school-level data protection audit report including a register of third-party personal data distribution, data protection impact assessments, provision of privacy notices and any significant amendments, to report on any breaches, and any audit reports carried out of vendors or pupil data users.

References

Article 29 Working Party pinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp160_en.pdf

Against Borders for Children (2016) https://www.schoolsabc.net/2016/09/letter-justine-greening/ (accessed August 2019)

Anderson, R., Brown, I., Clayton, R., Dowty, T., Korff, D. and Munro, E., (2009), Children's Databases - Safety and Privacy. A Report for the (UK) Information Commissioner.

Are Technica, Cox, K. (2019) 50 states and territories launch massive joint probe into Google https://arstechnica.com/tech-policy/2019/09/50-states-and-territories-launch-massive-joint-probe-into-google/

Automating Society: Taking Stock of Automated Decision-Making in the EU. AlgorithmWatch (2019) https://algorithmwatch.org/wp-content/uploads/2019/01/Automating_Society_Report_2019.pdf

The Berkman Centre for Internet And Society at Harvard (2008) Enhancing Child Safety and Online Technologies report https://cyber.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report.pdf (accessed November 2017)

Binns et al. Measuring third party tracker power across web and mobile. WebSci'18. https://ora.ox.ac.uk/objects/uuid:86310ed1−762e−4037−a4d2−80568c5ee7c4 (2018) (accessed September 2019)

Binns et al. Third Party Tracking in the Mobile Ecosystem. TOIT. https://arxiv.org/abs/1804.03603 (2018) (accessed September 2019)

Big Brother Watch (2014), report: Biometrics in Schools https://www.bigbrotherwatch.org.uk/files/reports/Biometrics_final.pdf (accessed 12 November 2017) and Classroom Monitoring; Another Brick in the Wall (2016) https://www.bigbrotherwatch.org.uk/wp-content/uploads/2016/11/Classroom-Management-Software-Another-Brick-in-the-Wall.pdf (accessed 12 November 2017)

Binns, R. et al. 2018. "It's Reducing a Human Being to a Percentage"; Perceptions of Justice in Algorithmic Decisions. ArXiv:1801.10408 (Cs), 1–14. https://doi.org/10.1145/3173574.3173951.

Booth, P. (2017) Age Verification as the new cookie law? http://www.infiniteideasmachine.com/2017/08/age-verification-as-the-new-cookie-law/

Boyd, D. and Crawford, K. 2012. Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon. 15(5) Information, Communication, & Society 662–679

Breyer vs Germany, http://curia.europa.eu/juris/document/document.jsf?docid=184668&doclang=EN (accessed 1 November 2017)

Bridge International (accessed September 2019) https://www.bridgeinternationalacademies.com/supporting/teacher-tools/

Cardiff Data Justice Lab, Data Scores as Governance Report (2018) https://datajusticelab.org/data-scores-as-governance/

Carter, P., Laurie, G., Dixon-Woods, M. (2015) The social licence for research: why care.data ran into trouble, J Med Ethics 2015;41:404-409 doi:10.1136/medethics-2014-102374

The Children's Commissioner, (2017) (England) Growing Up Digital https://www.childrenscommissioner.gov.uk/publication/growing-up-digital/

The Chromium Projects: Rappor (Randomized Aggregatable Privacy Preserving Ordinal Responses) http://www.chromium.org/developers/design-documents/rappor

Classcharts https://www.classcharts.com/

Conley, D. and Fletcher, The Genome Factor - What the Social Genomics Revolution Reveals about Ourselves, Our History, and the Future (2017) ISBN : 9780691164748 Princeton University Press

Council of Europe 2016-21 Strategy on the Rights of the Child, https://rm.coe.int/168066cff8 (accessed 1 November 2017) Para 30 CM/Rec (2013) 2. 1.2. Countering discrimination

Council of Europe. 2017. Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a

Council of Europe, MSI-AUT Committee of experts on Human Rights Dimensions of automated data processing and different forms of artificial intelligence (work in progress) https://www.coe.int/en/web/freedom-expression/msi-aut

Committee of Ministers to member States, Recommendation CM/Rec (2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (Adopted by the Committee of Ministers on 4 July 2018 at the 1321st meeting of the Ministers' Deputies) https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016808b79f7

Davidson, C. (2017) The New Education: how to revolutionise the university to prepare students for a world in flux (Basic Books)

Department for Education, (UK) (2019) Special educational needs: an analysis and summary of data sources https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/804374/Special_educational_needs_May_19.pdf

The Danish Institute for Human Rights. 2016. Human rights impact assessment guidance and toolbox (The Danish Institute for Human Rights, 2016) https://www.humanrights.dk/business/tools/human-rights-impact-assessment-guidance-and-toolbox

defenddigitalme, (2016) Timeline of school census use for immigration enforcement purposes https://defenddigitalme.com/timeline-school-census/ and https://en.wikipedia.org/wiki/England_school_census

defenddigitalme, (2016) Distribution of national pupil records to commercial companies, charities, think tanks and the press https://defenddigitalme.com/faqs/

Denham, E. The Information Commissioner, ICO, July 2017 on “innovation”, findings on Google DeepMind and Royal Free https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/royal-free-google-deepmind-trial-failed-to-comply-with-data-protection-law/

Dowty, T., Korff, D. (2009), Protecting the Virtual Child: the law and children’s consent to sharing personal data https://www.nuffieldfoundation.org/sharing-childrens-personal-data

Durkin, E. (2019) The Guardian, New York school district's facial recognition system sparks privacy fears https://www.theguardian.com/technology/2019/may/31/facial-recognition-school-new-york-privacy-fears

Education Foundation (2013) Facebook Guide for Educators https://www.ednfoundation.org/wp-content/uploads/Facebookguideforeducators.pdf Criticised by civil society in England as promotion

The Economist (December 22, 2012), Learning new Lessons www.economist.com/news/international/21568738-online-courses-are-transforming-higher-education-creating-new-opportunities-best (accessed November 2017)

Elliot, M., Purdam, K., Mackey, E., Data Horizons: New forms of Data for Social Research, School of Social Sciences, The University Of Manchester, 2013.) http://hummedia.manchester.ac.uk/institutes/cmist/archive-publications/reports/2013-05-Data_Horizons_Report.pdf (accessed 11 November 2017)

ESCR-Net (2018) Civil society denounces for-profit ICT4D network of schools (accessed August 2019) https://www.escr-net.org/news/2018/civil-society-denounces-profit-ict4d-network-schools and their list of Bridge International Academies Investors http://globalinitiative-escr.org/wp-content/uploads/2018/02/List-of-BIA-investors.pdf

Evening Standard (2012) The CCTV in your child's school toilet: More than 200 admit using cameras in loos and changing rooms, https://www.standard.co.uk/news/education/the-cctv-in-your-childs-school-toilet-more-than-200-admit-using-cameras-in-loos-and-changing-rooms-8129753.html

Fichter, A., Der Republik (2019) Der Spion im Schulzimmer https://www.republik.ch/2019/07/02/der-spion-im-schulzimmer

Ferreira,J., CEO at Knewton (2012) https://www.youtube.com/watch?v=Lr7Z7ysDluQ Source: YouTube channel at the Office of Educational Technology at the US Department of Education

FOCIAI https://fociai.com/

Forbes (2014) Facebook Manipulated User News Feeds To Create Emotional Responses (accessed September 2019)

https://www.forbes.com/sites/gregorymcneal/2014/06/28/facebook-manipulated-user-news-feeds-to-create-emotional-contagion/

Google Family Link app https://families.google.com/familylink and reference to Blog: Google Family Link for Under 13s: children's privacy friend or faux? Persson, J.(2017) http://jenpersson.com/google-family-link/

Greene,T. (2018) China's facial recognition AI has a new target: Students https://thenextweb.com/artificial-intelligence/2018/05/18/chinas-orwellian-surveillance-state-turns-its-ai-powered-gaze-on-students/

Guidelines on child friendly justice adopted by the Committee of Ministers of the Council of Europe on 17 November 2010. Accessed September 2019 https://rm.coe.int/16804b2cf3 (See also Parliamentary Assembly Resolution 2010(2014) "Child-friendly juvenile justice: from rhetoric to reality", and the orientations on promoting and supporting the implementing of the Guidelines on child-friendly justice by the European Committee on Legal Co-operation (CDCJ(2014)15).)

Hand, B 92019) Biometrics In Schools: 4 Ways Biometric Data Can Be Used To Enhance Learning https://elearningindustry.com/biometrics-in-schools-data-enhance-learning-4-ways

Herold, B. (2018) Education Week, To Stop School Shootings, Fla. Will Merge Government Data, Social Media Posts, https://www.edweek.org/ew/articles/2018/07/26/to-stop-school-shootings-fla-will-merge.html

Hildebrandt, M. (2016) Smart Technologies and the End(s) of Law : Novel Entanglements of Law and Technology (Edward Elgar Publishing).(Chapter 9)

HLEG-AI Policy and Investment Recommendations for Trustworthy Artificial Intelligence (accessed July 1, 2019) (published June 26, 2019) https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence (permanent copy https://defenddigitalme.com/wp-content/uploads/2019/07/AIHLEGPolicyandInvestmentRecommendationspdf.pdf)

IB Times, 77 Million Accounts, Students, Teachers, Parents Stolen, by AJ Dellinger, 05/17/17 http://www.ibtimes.com/edmodo-hacked-77-million-accounts-students-teachers-parents-stolen-education-social-2540073 (accessed 1 November 2017)

ICDPPC Resolution on E-Learning Platforms (40th International Conference of Data Protection and Privacy Commissioners (October 2018) https://edps.europa.eu/sites/edp/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

IEEE Global Initiative for Ethical Considerations in Artificial Intelligence and Autonomous Systems. 2016. Ethically Aligned Design: A Vision For Prioritizing Wellbeing With Artificial Intelligence And Autonomous Systems, Version 1. IEEE, 2016. http://standards.ieee.org/develop/indconn/ec/autonomous_systems.html.IEEE

IEEE, (2019) Computer Vision for Attendance and Emotion Analysis in School Settings https://ieeexplore.ieee.org/document/8666488

India Today, July 2019, Delhi school becomes first ever to provide live CCTV video feed to parents https://www.indiatoday.in/education-today/news/story/delhi-school-becomes-first-to-provide-live-cctv-video-feed-to-parents-cm-arvind-kejriwal-1564401-2019-07-08

International Working Group on Data Protection in Telecommunications Working Paper on e-Learning Platforms. (April 2017) https://epic.org/IWG/workingpapers/e-learning-platforms.pdf

i-news (2017) Ofsted to 'snoop' on parents' and pupils' social media https://inews.co.uk/news/education/teachers-given-less-days-training-safeguarding/

IPC Ontario GPEN Sweep Report (2017) https://www.ipc.on.ca/wp-content/uploads/2017/10/gpen-sweep-rpt.pdf (accessed August 2019)

Jing, M. (2019) BrainCo CEO says his 'mind-reading' tech is here to improve concentration, not surveillance https://www.scmp.com/tech/innovation/article/3008439/brainco-ceo-says-his-mind-reading-tech-here-improve-concentration

Judgement of the Supreme Court (2016) UKSC51 https://www.supremecourt.uk/cases/docs/uksc-2015-0216-judgment.pdf

Judgment of the Court of Justice of the European Union in the Bara case (C-201/14) http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150110en.pdf (October 2015)

King, P. Biometrics in Schools https://pippaking.blogspot.com/

The Law Society, Event Report: Artificial Intelligence, Big Data and the Rule of Law, (accessed 12 November 2017) https://www.biicl.org/documents/1798_ai_event_-_final_report_15_11_2017_002.pdf

Learning Analytics blog on Civil Learning by the University student body (NSU) VP for Communications (August 2017) Northumbria University https://www.mynsu.co.uk/blogs/blog/tallykerr/2017/08/02/Learning-Analytics/ (accessed November 11, 2017)

Livingstone, S. (2016) The GDPR: Using evidence to unpack the implications for children online, LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/ (accessed 1 November 2017)

Livingstone, S.. (2017) Online challenges to children's privacy, protection and participation: what can we expect from the GDPR?, LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2017/02/09/online-challenges-to-childrens-privacy-protection-and-participation-what-can-we-expect-from-the-gdpr/ (accessed 1 November 2017)

Lievens, E., (2016) Wanted: evidence base to underpin a children's rights-based implementation of the GDPR LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/11/10/wanted-evidence-base-to-underpin-a-childrens-rights-based-implementation-of-the-gdpr/ (accessed 1 November 2017)

Lupton, D. and Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. New Media & Society Vol. 19, Iss. 5, 780–794;

Mantelero A. 2018. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Assessment. Computer Law & Security Review (2018), https://doi.org/10.1016/j.clsr.2018.05.017.

Mantelero, A. 2017. Regulating Big Data. The guidelines of the Council of Europe in the Context of the European Data Protection Framework' (2017) 33(5) Computer Law & Sec. Rev. 584-602.

Mats, S. (2018) WIRED, Psychological microtargeting could actually save politics https://www.wired.co.uk/article/psychological-microtargeting-cambridge-analytica-facebook

McKown et al (2017) Key Design Principles for Direct Assessments of SEL: Lessons Learned from the First Design Challenge (social and emotional learning) https://measuringsel.casel.org/wp-content/uploads/2017/09/AWG-Design-Challenge-Direct-Assessments-of-SEL.pdf

Mundie, C. Privacy Pragmatism, Focus on Data Use not Collection, Foreign Affairs, March/April (2014), Volume 93

Nemorin,S. Dr. University College London, Affective capture in digital school spaces and the modulation of student subjectivities. Emotion, Space and Society, 24. pp. 11-18. ISSN 1755-458
http://discovery.ucl.ac.uk/10066766/11/Nemorin_Affective%20capture%20in%20digital%20school%20spaces%20and%20the%20modulation%20of%20student%20subjectivities.pdf

Nemorin,S. Selwyn, N. (2018) Everyday Schooling in the Digital Age: High School, High tech? https://www.routledge.com/Everyday-Schooling-in-the-Digital-Age-High-School-High-Tech-1st-Edition/Selwyn-Nemorin-Bulfin-Johnson/p/book/9781138069374

The Norwegian Consumer Council report #WatchOut (2017) https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children and #ToyFail https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/ (accessed 1 November 20170

The Norwegian Data Protection Authority. 2018. Artificial Intelligence and Privacy Report. https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf.

Nyst, C. (UNICEF) (2018) Principles for Children's Online Privacy and Free Expression Industry Toolkit https://www.unicef.org/csr/files/UNICEF_Childrens_Online_Privacy_and_Freedom_of_Expression(1).pdf

OECD (2018) The OECD Study on Social and Emotional Skills (10-15 year old children) http://www.oecd.org/education/ceri/thestudyonsocialandemotionalskills.htm

Pappano, L. (2012) New York Times, The Year of the MOOC http://www.nytimes.com/2012/11/04/education/edlife/massive-open-online-courses-are-multiplying-at-a-rapid-pace.html

Paterson, L. and Grant, L. The Royal Academy of Engineering (2010), Privacy and Prejudice: Young people's views on Electronic Patient Records.(permanent record http://http://jenpersson.com/wp-content/uploads/2016/08/Privacy_and_Prejudice.pdf (page 40)

Patterson.J. Gaggle CEO, Education Week, (2019) https://www.edweek.org/ew/articles/2019/05/30/schools-are-deploying-massive-digital-surveillance-systems.html (accessed September 2019)

Parent Coalition for Student Privacy, Starting in 2012 and continuing to 2014, there was a grassroots rebellion against the plans of states and districts to disclose personal student data with a corporation funded by the Gates Foundation called inBloom Inc. https://www.studentprivacymatters.org/background-of-inbloom/ (accessed November 2017)

Parent Coalition for Student Privacy, McPherson KS students join the rebellion vs Summit and depersonalized learning and win the right to opt out (2019) https://www.studentprivacymatters.org/kansas-students-join-the-rebellion-vs-summit-and-depersonalized-learning/

Parents reassured after live footage from Blackpool schools' CCTV cameras was 'hosted on US website, The Gazette, (February 2018) https://www.blackpoolgazette.co.uk/education/parents-reassured-after-live-footage-from-blackpool-schools-cctv-cameras-was-hosted-on-us-website-1-9036288

Paul, J. (2017) The Rise of Biometrics in Education https://www.d2l.com/en-eu/blog/rise-biometrics-education/

Plomin, R., Stumm, S. (2018) The new genetics of intelligence https://www.nature.com/articles/nrg.2017.104

Pluim, C. and Gard, M. (2016) Physical education's grand convergence: *Fitnessgram*®, big-data and the digital commerce of children's health https://www.tandfonline.com/doi/abs/10.1080/17508487.2016.1194303

Porter, G. (2010) Mobility, surveillance and control of children and young people in the everyday : perspectives from sub-Saharan Africa https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/sub-saharan and https://www.theimpactinitiative.net/project/impact-mobile-phones-young-peoples-lives-and-life-chances-sub-saharan-africa-three-country

Powles, J. University of Western Australia. (2018), The Seductive Diversion of 'Solving' Bias in Artificial Intelligence, https://medium.com/s/story/the-seductive-diversion-of-solving-bias-in-artificial-intelligence-890df5e5ef53

Privacy International (2019) Report: Your Mental Health for Sale https://privacyinternational.org/campaigns/your-mental-health-sale

Protection of Freedoms Act 2012 (England and Wales) Biometric data protection for children in schools (Chapter 2) http://www.legislation.gov.uk/ukpga/2012/9/part/1/chapter/2/enacted

The Proverbial Permanent Record, New York University Information Law Institute (October 9, 2014), Elana Zeide http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2507326 https://defenddigitalme.com/wp-content/uploads/2019/09/SSRN-id2507326.pdf

Rouvroy, A. 2016. “Of Data and Men”: Fundamental Rights and Liberties in a World of Big Data’ https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a6020.

Sabates, R. et al (2010) School Drop out: Patterns, Causes, Changes and Policies https://unesdoc.unesco.org/ark:/48223/pf0000190771

Savirimuthu, J., (2016) EU General Data Protection Regulation Article 8: Has Anyone Consulted the Kids? LSE Media Policy Project blog, the London School of Economics http://blogs.lse.ac.uk/mediapolicyproject/2016/03/01/eu-general-data-protection-regulation-article-8-has-anyone-consulted-the-kids/ (accessed August 2019)

School Surveillance: The Consequences for Equity and Privacy. Education Leaders Report (4), National Association of State Boards of Education, J. William Tucker and Amelia Vance. (2016). http://www.nasbe.org/wp-content/uploads/Tucker_Vance-Surveillance-Final.pdf (permanent copy https://defenddigitalme.com/wp-content/uploads/2019/09/Tucker_Vance-Surveillance-Final.pdf)

Schuijer, J., (2017) Transcranial Electrical Stimulation to Enhance Cognitive Performance of Healthy Minors: A Complex Governance Challenge https://www.frontiersin.org/articles/10.3389/fnhum.2017.00142/full

Selwyn, N., Monash University, Australia, What are the acceptable limits of school data? The case of the Florida ‘school safety’ database (2019) https://data-smart-schools.net/2019/06/05/what-are-the-acceptable-limits-of-school-data-the-case-of-the-florida-school-safety-database/

Selwyn, N. (2015). Data entry: towards the critical study of digital data and education. Learning, Media and Technology, 40(1), 64-82.

Selwyn, N. (2016) ’Is Technology Good For Education?' (Polity). Chapter 4, ’Making Education More Calculable' (discussing the 'data' turn' in education' / Chapter 5, ’Making Education more Commercial' (discussing Big Tech).

Smith. S, Shadow of the smart machine: Will machine learning end? Nesta 2016 https://www.nesta.org.uk/blog/shadow-smart-machine-will-machine-learning-end (accessed September 2019)

Southgate et al. Artificial Intelligence and Emerging Technologies in Schools, commissioned by the Australian Government (2019) https://defenddigitalme.com/wp-content/uploads/2019/09/aiet_final_report_august_2019.pdf

Spying on Students: School-Issued Devices and Student Privacy, (2017) Alim, F., Cardozo, N., Gebhart, G., Gullo, K., and Kalia, A. (Electronic Frontier Foundation) https://www.eff.org/files/2017/04/13/student-privacy-report.pdf

The State of Data survey of parents' views on technology and data in UK schools. Survation (2018) https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf

Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age, http://www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf And what do children ask for? http://www.lse.ac.uk/my-privacy-uk/what-do-children-ask-for

Sujon, Z. (2019) Disruptive Play or Platform Colonialism? The Contradictory Dynamics of Google Expeditions and Educational Virtual Reality. Digital Culture and Education, 11 (1). ISSN 1836-8301

Swedish DPA decision on Facial recognition used for attendance registration in schools BBC ref https://www.bbc.co.uk/news/technology-49489154 original decision Teaching as a Design Science, Diana Laurillard, Routledge, 2012, p. 4. (English translation forthcoming from the DPA)

Taylor, E. and Rooney, T. (2017) Surveillance Futures: Social and ethical implications of new technologies for children and young people, https://www.taylorfrancis.com/books/e/9781315611402

UN Guiding Principles on Business and Human Rights (2011) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.p

UCL, Centre for Educational Neuroscience (2019) The future of education is brain stimulation http://www.educationalneuroscience.org.uk/resources/neuromyth-or-neurofact/the-future-of-education-is-brain-stimulation/)

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH, in the presence of Facebook Ireland Ltd (Case C-210/16). http://curia.europa.eu/juris/document/document.jsf?docid=195902&doclang=EN

UNCRC Committee on the Rights of the Child General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.unicef.org/csr/css/CRC_General_Comment_ENGLISH_26112013.pdf

UNCRC Committee on the Rights of the Child General comment No. 1 (2001) on the Aims of Education (Article 29) https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/a)GeneralCommentNo1TheAimsofEducation(article29)(2001).aspx

Underachievement in Education (2014) House of Commons Education Committee http://defenddigitalme.com/wp-content/uploads/2016/08/Plomin_-December-2013_142.pdf

US Department for Education (Privacy Technical Assistance Center) (2015) Protecting Student Privacy While Using Online Educational Services: Model Terms of Service, https://studentprivacy.ed.gov/sites/default/files/resource_document/file/TOS_Guidance_Jan%202015_0%20%281%29.pdf

Vatsalya, Youth Ki Awaaz, 2019, CCTV in Delhi schools https://www.youthkiawaaz.com/2019/08/cctv-surveillance-in-schools-boon-or-bane/

Veale M., Binns R. 2017. Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data & Society, 4(2):2053951717743530, https://doi.org/10.1177/2053951717743530.

Who Knows What About Me. (Children's Commissioner, (2017) UK) https://www.childrenscommissioner.gov.uk/publication/who-knows-what-about-me/

Williamson, B. (2017) University of Edinburgh, Centre for Research in Digital Education and the Edinburgh Futures Institute. Big Data in Education, the digital future of learning, policy and practice (Sage)

Williamson, B. (2018) Brain Data: Scanning, Scraping and Sculpting the Plastic Learning Brain Through Neurotechnology https://link.springer.com/article/10.1007%2Fs42438-018-0008-5

Williamson, B. (2018) postgenomic science, big data, and biosocial education (on_education) https://www.oneducation.net/no-02-september-2018/postgenomic-science/

World Economic Forum (WEF) (2016)New Vision for Education: Fostering Social and Emotional Learning through Technology http://www3.weforum.org/docs/WEF_New_Vision_for_Education.pdf

Zhao et a. 'I make up a silly name': Understanding Children's Perception of Privacy Risks Online. CHI'2019. https://arxiv.org/abs/1901.10245 (2019) (accessed September 2019)

Zhao J. Are Children Well−Supported by Their Parents Concerning Online Privacy Risks, and Who Supports the Parents?. https://arxiv.org/abs/1809.10944 (2018) (accessed September 2019)

Zimmer, C. (2018) The Atlantic, Genetic Intelligence Tests Are Next to Worthless https://www.theatlantic.com/science/archive/2018/05/genetic-intelligence-tests-are-next-to-worthless/561392/