15 November 2019 T-PD(2019)06FIN

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

Convention 108

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

Report by Jen Persson, Director of defenddigitalme.

Directorate General of Human Rights and Rule of Law

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 education 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.

It is also critical to recognise that despite the differences in the education landscape across different geographies, it is common practice to use children in education as test beds for new technologies, both by companies to develop their products, and by state actors, before adoption at scale.

There are little researched but significant questions of human health and safety, and issues of ethics and governance, related to the adoption of emerging technologies in the classroom, such as motion sickness in immersive virtual reality. Neuro- technology development and post-digital science, require concerted attention from education researchers (Williamson, 2019) as well as regulatory and legislative authorities.

While Data Protection supervisory authorities grapple with data protection and privacy across a wide range of sectors, concerted attention and systemic action has been limited to date, to uphold children's rights in education and tends to look at what is, not scan the horizon.

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, in different systems of education each with their own personal experience of cultural, social, economic and political changes, may not have changed significantly in those ten years, but there has been rapid growth in the available technologies in their classrooms.

Schools have opened their doors, and databases of school children's personal confidential information, to a growing number of commercial actors. Children may already be subjected to brain scanning tools, 360º cameras including voice capture, RFID tracking, and interact with

augmented reality headsets in the classroom. Companies and their financial backers are keen to exploit education as a new market, where states have moved from less state controlled to more commercially driven models of education. Similarly, successful companies in existing markets, such as security cameras, are expanding into the education sector. The resulting exposure of children to a wide range of data processing technologies has been largely unseen.

Children's rights under data protection law, have remained almost unchanged in the decade. But whether they are respected depends on the companies behind the scenes and regulators' enforcement, since controls and safeguards at school level can be weak.

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.*"

I.1.1 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 in England, 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, 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 for which 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."*

The question of how long current models are sustainable for data collection in terms of trustworthiness and levels of societal tolerance is being tested by new and emerging technologies in the classroom, such as facial recognition. (CNIL, 2019)

Regulators play a vital role in enforcement of the rule of law, that should offer trusted and sustainable frameworks to make sure the minimal digital footprint possible, follows each child into adulthood.

Furthermore, while there is a growing proliferation of ethics institutes and materials from them talking about ethics and a digital footprint, we are yet to see substantial consideration given to the effect of these technologies in a holistic way in a child's life for now, and their future, or assessment of their impact on each child's carbon footprint and whether we can build more sustainable models of hardware so as to not additionally burden their future world through their interactions in today's digital environment.

Some schools' growing ICT legacy from early adoption, is a cupboard full of unusable devices they cannot afford to replace, built with operating systems that the company no longer supports.

Any complete ethics impact assessments of emerging technologies must also include their environmental impact and how companies can be held to account for the necessary steps to minimise their consumption of natural resources and energy.

The inherent risks of outdated systems include exposure to ransomware and other security threats.[1]

1.1.2 Volume and variety of data actors on the educational stage

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 types of actors on the premises of educational settings who are involved in processing children's personal data from schools, may be grouped into those who have a direct relationship with the child (teachers, school administrators) and those who do not (regional administrators processing data for analytics purposes, teacher performance, and pupil progress measures).

But the vast majority of actors involved in the everyday data processing in a child's day, year, and lifetime while very hard to visualise due to their large volume, are not on the school premises, but outside it, in hundreds of companies, processing cloud-based data.

The types of data gathered can be broadly grouped into administrative data, and learning data.

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. Technology is used to teach, track students' progress, and test.

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 legal guardians are not aware.

[1] School districts are a particularly easy target for ransomware operators because of their low budget for information technology and limited security resources ArsTechnica (2019) https://arstechnica.com/information-technology/2019/08/rash-of-ransomware-continues-with-13-new-victims-most-of-them-schools/

1.1.3 Data mining and exploitation

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 to deliver low-cost state education, and marketisation, the infrastructure used to deliver state education and the children in it, are exposed to commercial 'freeware', software that companies offer at no cost, often in a non-explicit exchange for data.[2]

Insufficient training and change management often accompanies the introduction of new technologies, with insufficient learning materials and under-qualified teachers. (Sabates, R. 2010)

1.1.4 Hidden predictions

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)

In England, Essex county council uses predictive analytics to identify children who would not be "school ready" by their fifth birthday, and Bristol City Council is experimenting with new algorithmic capabilities, using nightly extractions of school pupil data[3] to factor into their predictive analytics for children's social care interventions. (Pegg, McIntyre, 2018)

The predictive nature of such data processing applied to early interventions could have significant impact, and any inadvertent consequences could be lifelong from an early age.

Software marketed as using Artificial intelligence are also being used for predicting behavioural risk in Internet monitoring products, in personalised learning platfoms, and even for low level decision-making at school classroom level, such as assigning class seating plans based on the recording of children's behaviour data in apps, analysed in opaque ways to determine room layouts optimised for behaviour.

Findings from Regan and Steeves (2019), suggest that,

> *'competing discourses on personalized learning revolve around contested meanings about the type of expertise needed for twenty-first century learning, what self-directed learning should look like, whether education is about process or content, and the type of evidence that is required to establish whether or not personalized learning leads to better student outcomes.'*

The potential global implications for the security and stability of the state sector education infrastructures and interplay with other public sectors where children's data are used for interventions in their lives, the personal costs to children in terms of privacy, and effects of

[2] For example, the NetDragon Websoft Group in 2019 was "under way to monetize its user base" from the online community of Edmodo. (page 4 (6/84) http://file.download.99.com/down/ir_e_20191011f.pdf)
[3] http://specification.sifassociation.org/Implementation/UK/2.0/html/

normalisation of automated decision-making, may beyond the lifetime of this datafied generation.

1.1.5 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)

Predictions based on machine analysis of large sets of personal data, automated decisions that make on and offscreen changes to the child's lived experience simply through nudging screen interactions, and personalised interventions taken as a result by adults, are all already possible at levels of invasiveness and in ways that are covert or opaque, that most families and school staff themselves do not see. Why transparency obligations fail and how this can be rectified demands a different systemic approach to supporting children and families' understanding of their own data processed by others.

Some applications of technology, based on children's data capture, mining, and interpretation, should be determined to be too invasive and too interfering in a child's full and free development, that it should be unacceptable for children to be exposed to within education. The 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 used for interventions with children. But that should not mean the imposition of live-product trials and testing on children in the classroom as part of compulsory state education systems, for the primary benefit of the product manufacturers.

1.1.6 Regulation should ensure 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.

The fundamental principles of data purpose limitation, data minimisation and transparency are often inadequate in practice, 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 data minimisation principle is at the heart of what children need if data protection is to have a meaningful effect to protect their personhood and human dignity, not only enable safe, fair and lawful processing of their data. The limitations of how far the approach proposed by the High Level Expert Working Group on Artificial Intelligence (HLEG-AI) in their April 2019 Policy and Investment Recommendations for Trustworthy Artificial Intelligence, should be applied to better protect in the education environment, should not be determined by state actors or commercial products wants, but rather by the needs and best interest of the child, to enable their full and free development into adulthood.

> *"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."* (HLEG-AI, 2019)

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 some 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 adequacy of the existing data protection regulations and its enforcement mechanisms that rely on individual complaints, in addressing the rights of the child in the education environment.

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, eighty-eight 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 Mark Zuckerberg tried to export Silicon Valley style solutions, in the Facebook funded Summit Schools model of education, to Kansas, a U.S. state in the Midwestern United States, they were met with strong objections even from children themselves.(Bowles, 2019)

The largest commercial contributors to reshaping the delivery of education infrastructure are also those shaping the business world; Google, Microsoft and Apple. In addition, some of the world's largest publishers are also involved in the delivery of online educational tools. Pearson, and Wiley, for example, and NewsCorp. Companies that track academic writing and content, also create online content tags, and this allows for tracking the use of that content at scale in ways that non-digital content does not allow. 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."

This further raises the question who owns big data? (Ruppert 2015) as digital data is being used by increasingly powerful technical organisations to produce knowledge and drive decision making. (Williamson, 2017) And as the knowledge extracted from data in education are increasingly used to nudge and predict behaviour inside and outside the classroom, the balance of power in a child's life is changed in ways that are not made obvious to a child.

The role of data protection in the protection of the child in an educational setting, therefore has multiple roles of importance; but should be less focussed when transforming the words into action, about enabling compliance of lawful data processing, and more about a child-centric focus on the protection and exercise of their rights. The protection of data about a child, is protection of the child itself to safeguard their free development and dignity, and should create a check-and-balance on exploitation of the power and influences that a child is exposed to. Privacy is also an enabler of further rights.

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.

The role of the right to privacy and data protection are not often as clearly demonstrated as enabling rights as they are in education, underpinning the links between article 29 (1) and the systemic struggle against racial discrimination, xenophobia and related intolerance.

The aims, set out in the five sub-paragraphs of the UNCRC 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.

While both education and digital tools are unequally distributed around the world, the issues that come with some tools in digitised education are new for particular populations. Refugees are recognised by agencies and development actors, to be actively avoiding some refugee camps, so as to avoid the capture of biometric IDs. Similar chilling effects of data surveillance may be found in education.

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. For 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

II.1. The challenge of consent

We already have broad data protection laws, so why does education need anything more?

II.1.1 Consent must be informed and freely given

Perhaps the greatest challenges to the rights and freedoms of the child in the education environment are also the starting point for why the sector merits more specific attention over and above the existing standards of universal data protection.

1. Education is compulsory for children and young people.

2. Consent as the ultimate tool of personal empowerment is fundamentally flawed and hard to be freely given without detriment in the relationship between child and adult, between family and institution.

   Conform, or you won't have a place in this school. (Taylor, 2015) At its heart, compulsory schooling can be at odds with Article 12 of the UNCRC that the views of the child should be given due weight in accordance with the age and maturity of the child. This imbalance may or may not be a desirable learning environment, connected with country specific cultural norms, policy and member state law, but is outwith the scope of this report.

   In reality the imbalance of power means children's rights are rarely protected through principles that champion individual rights under the Convention 108+ and GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Educational institutions everyday practice can often demand disempowerment by default.

   > *"As one can see, surveillance in public education implies a great deal more than watching and discipling students. Surveillance is the dominant organising logic of modern institutions, shaping all the operations (Lyon 2007). [..} We define surveillance as watching, monitoring, tracking, or data analysing for purpose of control. Surveillance as a form of knowledge production, draws upon and thereby reifies normative categories of appearance and behaviour. Surveillance is an operation of power. As Michael Focault (1980) noted long ago, power is not simply about one person's control over another but instead signifies an entire apparatus of material, social, and symbolic relations within which human actors are caught."* (Monahan and Torres, 2009)

   In education, consent is not the norm even though it is often asked for and collected through a compulsory tick box exercise, which is not a consent process but rather an acknowledgment of the processing that school has disclosed to a family, with a greater or lesser explanation of terms and conditions. Education from a child's perspective is generally compulsory, even where it is not statutory. Whether through parental choice or school staff enforcement of policies and rules, the child in education, regardless of age, is not in a position of power.

   The Swedish Data Protection Authority recognised this in its ruling in August 2019, regards the Skellefteå kommun, 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 ($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'.

II.1.2 Consent cannot be withheld only with detriment and be considered freely given

An alternative approach the collection of 'consent' is to offer an objection process. However, this suffers from some of the same challenges that obtaining active consent does, in so far as the power imbalance. Families and children cannot easily object or opt out without experiencing a level of discomfort or stigma through being different or a 'difficult' parent. Even where an 'opt out' approach or objection to processing may be offered as an alternative model from consent, the alternative can mean 'missing out' and the perception that a lower level of support or teaching will be offered to children who prioritise their personal privacy over using commercial products in the classroom or parental engagement. It is therefore incumbent on education providers to do so in a rights-respecting manner, that enables a trustworthy process founded on good practice that does not leave families without practical routes to exercise the full range of data rights (of subject access, to restrict and object to processing or automated profiling) and leaves them no alternative but to object to the use of everyday technology in the classroom, in order to ensure their child's privacy rights are protected.

The base level of the expected standards of data processing using technology providers must be raised, while at the same time maintaining an equal level of an acceptable alternative standard of education (i.e. an objection to the use of a provider, should not result in a lesser educational experience for the child.)

- Consent cannot be freely given and is suitable for children's data processing in education only for very narrow purposes where objection is not detrimental to the child's education. (e.g. school event photographs used by press)

- Often data are collected about the child, but not from the child.
- Data may be created about the child by school staff, that the child and their family never see.
- Often the secondary processing is expressly prescribed by law.

Article 8(3) on Transparency under the Convention reduces data subjects' rights in such circumstances to be told how their data are processed, assuming such cases are exceptional, and that consent is the status quo:

> Where the personal data are not collected from the data subjects, the controller shall not be required to provide such information where the processing is expressly prescribed by law or this proves to be impossible or involves disproportionate efforts.

In education, however, consent to data processing is not the status quo even though it may be requested from legal guardians and children, in the form of home-school agreements or computer acceptable use policies.

In other environments, the relationship between the parent and the child may offer an additional level of protection and expectations of oversight, between the vendor and the child, for example in the purchase of an app in the home, for personal use. This role is expected to change over

time, and for the right of the child to be heard to increase with maturity.
"The fact that a child's views are given increasing weight is not, however, to imply that parents' own views on matters affecting their children can simply be disregarded as irrelevant, or that their over-arching responsibility can be supplanted or ignored where it is convenient to do so. Rather, the process envisaged is one of a gradual shift in the balance of power and responsibility from parents towards their children as each child's experience, maturity and capacity to understand the implications of actions and decisions increases." (Anderson et al., 2009)

In the school environment, this relationship still has an important role to play, however fails to offer the same level of protection through agency, and instead families can find that their own preferences conflict with the school policies.

II.1.3 Consent cannot be fully informed under current practices

The implementation of technology into this environment further disempowers children because it introduces new actors who have more control and power over how the child interacts with the app or platform, than the child, their family and often, their teacher.

The multitude of companies and developers behind a single product is hidden in particular where personal data can be processed not only for the direct school purposes of the application; such as homework, behaviour tracking, home-school communications or cashless payment processing; but by the companies' many partner organisations, subsidiaries and third-party processors and that companies terms and conditions can assert authority over the personal data as assets in case of company sale, merger or takeover.

In addition to the direct third-party data processing there can be yet another layer of personal data processing introduced by developers borrowing code from code libraries, copying from other people's designed code and slotting it into their own creations. This can lead to apps' behaviour and processing of personal data that even the developer at the point-of-sale or distribution cannot entirely understand or control, and can have unintended consequences.

It is therefore impossible for schools to obtain lawfully valid consent for processing personal data on behalf of their vendors.

Children and legal guardians simply cannot understand what they are consenting *to*.

But it is the volume of even the visible third-party interactions that leads schools to say they cannot manage consent.

This can in part explain why currently obtaining consent is viewed as difficult by schools, and companies can claim that it creates a "barrier to innovation". Schools may ignore consent because it is too complex for schools or companies to manage, and schools often 'consent by proxy'.

This rightly enables the release of information in an emergency context which is by its nature specific, in the direct care for a child in their vital or best interests, and time limited. It wrongly enables schools to overlook families and children's rights in routine data processing tasks.

II.1.4 Case study of assumed consent

The Think-Tank in England, 'Nesta' launched a test-bed program in conjunction with the Department for Education to trial edTech products in mid-2019. As regards the personal data processing, they suggest that there is no need for consent to be asked for, but conflate their third party commercial processing with that of the schools' under public task, and do not take into account the additional requirements of special category (sensitive) data.

> *"Since this project is generating evidence on products to help existing school and college objectives, and is in the public interest, there is no need for individual consent.*" (Nesta, EdTech Innovation Testbed, 2019)

The economic incentive to develop edTech for export is clear. How the exploitation of a State's child population is avoided while doing so, will depend on the rule of law and the ability of its subjects to rely upon its enforcement, where practice is guided by decisions based on the inadequate ethical position of policy makers, or political aims.

The challenge therefore is two-fold:

- How to assure the data and privacy protection of the child when consent is not the lawful basis for data processing and is interpreted by schools as there being no requirement to operate in a consensual manner.
- How to gather consent appropriately when consent is a valid lawful basis for data processing and required, taking the role of the parent / family and role of the child into account, and their relationship with each other, and with the institution.

II.1.5 Consent and contract terms may need rethought in the context of schools

The patriarchal power model of the majority of western educational institutions and settings, and its intrinsic power imbalance, requires a different model of empowerment for children and families, more than current data protection law affords us. Current models champion individual autonomy and consent as a strong safeguard for data control.

Children's opinions are to be heard according to their age and capacity. Where the boundaries lie on this under the law, varies according to jurisdiction, such as the age of criminal accountability at 10 in the UK. When it comes to school, they are generally represented by whomever is their legal guardian, or institution.

This institutional model may or may not be desirable in terms of autonomy and individual rights, but unless schools are prepared to significantly reduce the number of actors involved in data processing, there may be no other model which is realistically manageable.

It does however mean that strong legislative framework is required, in order for the data flows across, into and out of the institution are tightly controlled with clear accountability.

For example, under US educational law, FERPA requires that federally funded institutions, under programs administered by the U.S. Department of Education, comply with certain procedures with regard to disclosing and maintaining educational records.

This offers one potential model for managing the communication of agreed companies and third parties with who the school intends to share personal data in the course of the child's academic year

The data protections that the US model offers, include strong expectations of company behaviour. The contract terms and conditions are agreed at regional state level. The FERPA approved standard,,can only be achieved by companies willing to meet and maintain common pre-agreed terms of compliance throughout their life cycle.

In effect, it should be exceptional for a commercial third party to become a data controller rather than processor of school children's personal data collected during their education.

The investigative burden is reduced for families at individual level, by having adequately trained staff at regional level in the schools' system, who can make procurement decisions in line with the outcomes of thorough data protection and ethical impact assessments, and then contract with companies, giving schools in effect a green light to proceed into entering into contracts with such companies at local level.

Individuals and families can access the data protection and ethical assessments online or on request from a school, and therefore ask questions and be closely informed if they choose to. While a level playing field is created for all to have a similar level of trust in the standard of compliance expected in order to permit a company to engage with the public education system at all.

FERPA classifies protected information into three categories: educational information, personally identifiable information, and directory information. The limitations imposed by FERPA vary with respect to each category.

However, the US model is insufficient to adequately protect privacy as well as all personal data, which may be in any of these categories because it is impossible to separate personal data into distinct and clean categories, since the nature of the data being personal does not only rely on the item itself, but its context, and whether the controller may possess or come to possess other personal data that would make the first set of data, identifying.

In order to uphold rights, the schools are obliged to offer an objection to the use of a third-party provider, and schools have a responsibility to maintain a suitable level of alternative provision of education, should families or the child object to the product.

Much greater clarity and guidance is required by school staff in order to understand the boundaries of what is permitted and required under consent rather than other lawful grounds. Practical considerations need attention as to how schools communicate effectively with children and families, not only to meet their check-list of lawful obligations

II.2. Children's agency

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, Livingstone, and Nandagiri, 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.

II.2.1 Schools and one-size-fits-all click-wrap agreements

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 or changes in processing requirements by the company, will rarely be communicated to legal guardians or children.

II.2.2 State and government data extractions place obligations on schools

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)

II.2.3 Pupils and legal guardians 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.

II.3 The permanent single record

11.3.1 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.

11.3.2 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 have once 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.

The misuse of national pupil records by the UK Home Office for immigration enforcement purposes, was exposed in 2016 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.

11.3.3 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)

11.3.4 Commercial claims for excessive retention or marketing purposes 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.

11.3.5 Case studies on the permanent record

The mathematics app used by children worldwide, mathletics, until recently offered a cut off point in the year by when teachers must have requested that children's account data were deleted, otherwise the company retained pseudonymous data indefinitely. In addition, the company 3P learning considers IP address, contrary to the Breyer CJEU judgement, as not constituting personal data. And instead requires its indefinite retention together with behavioural activity data. "

> When agreeing to the Term and Conditions, Registrants grant us the right to use this anonymous information for our own purposes, such as the preparation of statistical reports or to improve and change the content of our products. "

The behaviour tracking platform Class Dojo have stated, by contrast that they do not create **not** a permanent record.

> *'Profile data not explicitly saved by a parent or student will expire and be deleted after one year.'*
>
> And they commit to not exploiting personal data of itself,
>
> *'We do not sell, lease or share your personal (or children's) information to any third party for advertising or marketing purposes.'*

However, such companies' business model is one that some families may consider unreasonable or unethical. Companies rely on using legal guardians' email linked to the child's account. Processing personal data provided from the school obtained for the direct purposes

of the education of the child by the school, a public task, should not be used in order to market further products to families, the for-profit purposes of the company, that are out with the public task, and therefore may be seen as incompatible to rely on the lawful basis of public task for processing.

”We plan to make money through premium features we’re developing that schools and parents can pay for”. (ClassDojo: What The New York Times Got Wrong)

II.4 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 be anonymous online is generally associated in teaching online safety, and the protection of personal details from strangers. Personal information about children are usually linked to their family information in school records, and required in educational apps to register accounts. Loss of privacy and identity data can therefore be collective about the family or community, and not only the individual, when it comes to educational products and systems.

Children under 11 are often regarded as too young to comprehend the implications of online privacy at all. Researchers at Oxford found in fact that children could identify and articulate certain privacy risks well, such as information oversharing or revealing real identities online. (Zhao et al, 2019) Families are rarely taught however, about the asymmetries in the digital age between companies and children, which means children 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.

The digitised student record may also be copied an indefinite number of times. And the context of the data collection, any inferences made, and quality of a record may be lost with each copy and shared use.

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 right to make free choices, free from interference, is fundamental to autonomy and the full and free development of personality.

The core of the fundamental right to privacy as a citizen, is the freedom from the unlawful interference over and against the state. 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 increases the risk of the loss of identity data, control over that decisional privacy through influence and decisions made by

others about interventions in your life, and discrimination through who the system believes we are, both in childhood, and into adulthood.

The ICDPPC resolution on e-learning platforms, that can be more broadly applied to any personal data in the learning environment, 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.”

II.4.1 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 including data brokers, not only for AV, but social media platforms, many of which enable social logins to perform the task of verifying log in credentials to other apps and platforms, used in homework and classroom activities.

11.4.2 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.

Schools and edTech apps should not use social media and other personal data about children or family members, obtained from public sources, to respect the purpose principle.

II.4.3 Biometric data for ID verification

Identity management can be carried out in school in a number of ways, but is often through the interaction between schools and third-party technology providers, either on site, or 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 identify verification should be used for low level transactions, as they are today in schools, such as to identify the child borrowing library books or 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, as an identity check of pupils and visitors to schools. However, as technology becomes more sophisticated, so can its uses.

Such technology is now being used to read expressions and track de-identified individuals from the camera to camera across shopping malls with the intention of inferring the gender, age, and ‘mood’ of individual shoppers (Anscombe 2017). Tellingly, these applications are beginning to shift from detection technology to identification technology as commercial outlets strive to link camera data with purchasing information. When facial recognition systems become widespread, detection applications (such as ‘mood’ inference) will also be implemented for purposes including marketing and security. For instance, the US Department of Homeland Security is developing systems to infer ‘malintent’ (the intent to do harm) from visual and biometric cues (Ackerman 2017). (Andrejevic and Selwyn, 2019)

In other less routine circumstances, children may be subject to facial recognition for verifying their identity for a particular time period. In testing and examinations for example, biometric ID systems using facial recognition are used increasingly 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 identifying pupils as part 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. This report addresses this further in part II.10.8 Biometric data.

The World Economic Forum advocated for the increased use of "fostering social and emotional learning through technology" in 2016.

It is unlikely that today's data protection legislation is sufficient to protect children from increasingly invasive uses of personal information about their bodily characteristics, including gait and emotion analysis that are collected not for the purposes of identity verification of a unique person, under Article 6 and Special categories of data under the Convention, but rather to infer their emotions, and intent.

II.5 Data sources, and opaque processing

Not all data are equal and in particular it should be recognised that large amounts of data about children in education are opinion, or inferred. 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 companies educational tools and platforms seen by children and families, and
- Created by the companies tools, but never seen by schools, families and children.
- Created by third parties external to the education system, such as data brokers, or social media companies, that may become linked with educational records.

II.5.1 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, legal guardians or children, and can violate e-privacy and consumer laws, as well as data protection law.

For example, the growing trend in UK for using mental health and wellbeing apps in the classroom, some of which are undoubtedly subject to the same flaws as mental health apps designed for adults, researched by NGO Privacy International.

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. (Privacy International, 2019)

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.

II.5.2 Repurposing must be preventable in practice

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 can be pressure in education systems to re-use data collected for direct purposes in school, by local and national governments for the indirect purposes of benchmarking data analytics, to pool pupil data into data lakes for use by third-parties, and link school pupil data with higher education student data with other government departments' longitudinal datasets (Graduate Outcomes LEO data, UK Department for Education, welfare and tax data).

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.

II.6 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 without parental knowledge, permission or oversight, threaten children's rights at unprecedented global scale, including their privacy, and autonomy and

ability to control their digital footprint.

II.6.1 Prevention from misuse in school is an impossible parental task

What if any, distinction must be made between communication to legal guardians 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. Legal guardians' rights are diminished and disempowered in doing so.

II.6.2 Parental understanding

To promote parental understanding, education records should be accessible to legal guardians. 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, out with 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 legal guardians 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.

There is a need for tools and processes to enable schools to exercise their transparency obligations in ways that can be open about data processing before it happens, and demonstrate their accountability after the processing occurs. To ensure that schools fulfil these obligations may need legislation and independent oversight.

II.6.3 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. 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 intent and purposes of the 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.

II.6.4 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 legal guardians, means that families are disempowered and cannot act to protect their child's rights in school. Unless legislation enables legal guardians 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 legal guardians 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.

II.6.5 Legal guardians' personal data rights

Legal guardians 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 legal guardians via direct email marketing, or in app adverts and marketing for supplementary commercial content.

Legal guardians' 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 legal guardians' 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)

II.7 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, and Nandagiri, 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.

II.7.1 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." (Stoilova, Livingstone, and Nandagiri, 2019)

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 is required and schools should audit current practices.

II.8 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, 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 to the detriment of children.

II.8.1 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 legal guardians 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."

II.9 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. This could be expanded upon in Guidance.

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.

II.10 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."

II.10.1 Data at scale challenges in education 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, at scale, sometimes called 'Big Data' 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.

Perhaps the greatest challenges in the protection of the rights of the child, their dignity and full and free development without interference supporting their human flourishing into adulthood, comes from the promise of machine learning and prediction, using large amounts of data collected in school, passed on through states of education, and analysed for early interventions. The presumption that this is possible and desirable continues through education into student life as well.

> *"AI algorithms can be used to identify issues based on the analysis of routine information – Student retention has become a major issue for universities, and institutions are now analysing data to pinpoint when and why students are at risk of dropping out, including how often students access their student management system, visit the library or submit assignments. Spotting causes for concern allows universities to proactively engage with troubled students and offer support and assistance as soon as possible.*
>
> *As well as increasing student retention rates, this helps universities to enhance student welfare by identifying problems and offering assistance earlier, rather than putting the onus on students to ask for help. It also enables institutions to provide early support for students with personal or mental health issues."*

However, the overarching immediate challenge of new and emerging technologies for children of all ages, is the desire from vendors and academics alike, to develop and test products.

II.10.2 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.

Children that are required to take part in trials, cannot freely consent and as already set out, the concept of legitimate consent in the school setting is fundamentally problematic. Failure to consent should never lead to essential services becoming unavailable, but neither can consent be dismissed and products tested as part of a public task if schools have less invasive ways of carrying to routine tasks in education.

The development of algorithmic systems should not mean that testing or deployment involves risks or costs for individuals, families, or communities, and this needs legislative support.

II.10.3 Can state education systems be safely shaped under commercial capture?

There are also significant global players 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.

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 adoption of Google's platform values, delivered through free training to school staff.

> *"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 are 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?" (Sujon, Z., 2019)

Challenges to its market dominance have begun in the US, Switzerland and by legal guardians in Spain, at the time of writing. (Ars Technica, 2019) The Attorney General for the US State of New Mexico filed a lawsuit in February 2020 against Google LLC, claiming that the that the use of Google Education and other Google products, "comes at a very real costs that Google purposefully obscures." (Balderas, New Mexico, vs GoogleLLC, 2020). The Norwegian Data Protection Authority has also announced it is investigating whether it is legal to use Google in schools. (Aftenposten, February 2020.) 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)

II.10.4 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.

That includes the 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.10.5 Artificial Intelligence (AI) and education

Recommendations should draw upon the existing Council of Europe standards and the relevant jurisprudence of the European Court of Human Rights, as well as the ongoing and developing human rights dimensions of automated data processing techniques, in particular algorithms and possible standards and regulatory implications.

> *"There is currently no agreed definition of "Artificial Intelligence". However, for the purposes of this Recommendation, AI is used as an umbrella term to refer generally to a set of sciences, theories and techniques dedicated to improving the ability of machines to do things requiring intelligence. An AI system is a machine-based system that makes recommendations, predictions or decisions for a given set of objectives."* (Council of Europe, May 2019)

From personalised learning platforms to automatically identifying dyslexia in children (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 signifiant 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.

When looking for recommendations, the first may be to not use the word Artificial Intelligence at all, with its loose yet limited definitions, but "Autonomous Intelligent system" or "algorithmic decision making" since there is a lack of legal definition. The second would be to treat data processing using these tools, with the same high expectations as other decision-making data methods.

II.10.6 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.

II.10.7 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.

II.10.8 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 technology 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.

II.10.9 Should biometric data be prized or normalised?

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.

II.10.10 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.

So far, these technologies have largely been seen as routine additions to school systems with already extensive cultures of monitoring and surveillance. This presents a number of social challenges and concerns that merit specific attention. This includes the likelihood of facial recognition technology altering the nature of schools and schooling along divisive, authoritarian and oppressive lines. (Andrejevic and Selwyn, 2019)

Growing public concern is starting to be reflected by regulatory action. 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 legal guardians.

In February 2020, the French courts upheld the CNIL supervisory decision, that facial recognition was unlawful in schools.

> Schools commonly already routinely have an image database of every enrolled child, and many use closed circuit television cameras for site surveillance, often as part of security measures. This raises the possibility of the easy adoption of facial recognition systems. 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 legal guardians 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. The 2010 case of Robbins v. Lower Merion School District exposed that the schools could take web cam photographs of children secretly, while they were in the privacy of their homes using software installed on the child's laptop. The highly invasive nature of such practices has expanded since then, often to include bring your own device policies, with little debate or oversight, as part of countering violent extremism programmes in Australia, US and the UK.

II.11 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 by comparison, 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 legal guardians 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 a 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.

II.11.1 This may exacerbate rather than diminish children's vulnerability to risks.

On filtering, the UN Special Rapporteur's 2014 report[4] 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 software, 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 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 technology.

---

[4] 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

II.11.2 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)

II.12 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.

II.12.1 What protections have our children in school from brain and behaviour shaping, and immersive 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 regards 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 regards 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 startup producers of cheap DNA kits for genetic IQ testing in schools, 'intelligence apps', or other genetic ed-tech products." (Zimmer, 2018)

II.12.2 What should the face of education look like?

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

Should polygenic scoring play a role in education at all? 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 startup 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.13 Tools for privacy basics in educational settings

II.13.1 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 one time 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.

Some are keen that Data Protection Impact Assessments about children must be tailored to them. (The Danish Institute for Human Rights. 2016) and also adequately explain passive data collections and risk. 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.

Arguably risk assessments should be thorough and technical documents with summary explanations of functionality and risk that can be extrapolated into lay terms. Data impact assessments must become routinely integrated into procurement processes.

Adequate data protection, privacy and ethical impact assessment must become embedded in the introduction of any technology and require appropriate levels of knowledge and training. Shared services are likely to provide a greater level of trustworthy competency, and could underpin schools' confidence in new technology introductions, as well as reduce local level workload requirements that the necessary levels off due diligence should demand. This would be especially useful where a regional contract model were to be adopted, with recognised minimum standards, under statutory Codes of Practice.

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.13.2 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 t h e 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 RAPPORT algorithm)[5].*
>
> *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.*
>
> *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*

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

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.13.3 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.13.4 Subject Access and usage reports

Trust in use of confidential data is affected by understanding data security, anonymisation, having autonomy and control, knowing who will have access, 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.

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.

II.14 The role of developers and industry

II.14.1 Disproportionate effort

Guidance should clarify that enabling the exercise of all rights under Article 9 of the Convention, is a requirement of data protection-by-design not an optional extra, and that design that relies disproportionate effort *by design* for school children to exercise their rights, should be regarded as unfair and unlawful. At the moment, we encounter products and data controllers that state their database of subjects is too enormous to be able to communicate with, highlighted in the case of the first fine imposed by the Polish DPA under the GDPR and Poland's Act on Personal Data Protection of May 10, 2018 implementing the GDPR. The decision provides some limited insights into the interpretation of the term "disproportionate

effort” within the meaning of Article 14(5)(b) of the GDPR. We suggest that this of itself must be seen as failure to respect the Article 25, not be used as an excuse to disempower the data subjects from their rights. It is therefore processing that should be found unlawful, not support the idea that disempowerment from the ability to exercise rights, is acceptable.

Ekambaranathan and Zhao (2019) found that developers of family-oriented technologies largely believe that it is an unethical practice to collect and sell children's data as a commodity (5/5 interviewees and 71/81 survey respondents). Some developers would also decline access to their users’ data from third parties in exchange of monetary gains due to moral reasons and liabilities. However, insufficient data privacy safeguarding practices are still often identified in these technologies aimed at children.

II.14.2 Third-party developer libraries

In software development, reusing existing code libraries developed by other developers is accepted as essential practice, allowing development communities to reduce development overhead and make better use of existing resources (such as cloud-based computing). However, the use of these code libraries often means that the developer does not see or fully understand the full extent of the effects of these code libraries and its interactions with their own. This can be for innocent reasons - for example, code libraries are frequently created by developers in countries which do not have data protection frameworks, and who therefore have no knowledge of COE or EU frameworks - or it can be less innocuous, for example, code libraries created by developers funded by adTech. This may mean that software may distribute user data to third parties of whom the developer may not be fully aware.

"Third-party libraries are increasingly prevalent in today's apps. A leading factor in this is that developers rely on targeted advertising for generating revenue, which in turn uses third-party libraries to collect targeted data. Additionally, they also simplify development, provide increased functionality, and may be more secure than proprietary software modules. However, these libraries have permissions to collect sensitive data, have been shown to frequently access location permissions, track call logs, browser history, and contact information for the purpose of targeted advertisements, even if that was not the intended functionality." (Zhao et al, 2019 upcoming)

Look at Facebook’s Software Developer Kit for example, on how android apps share data with Facebook (even if you don’t have a Facebook account. (Privacy International, 2019)

"App developers share data with Facebook through the Facebook Software Development Kit (SDK), a set of software development tools that can be used to develop applications (Apps) for a specific operating system. Facebook's SDK for Android allows app developers to integrate their apps with Facebook’s platform and contains a number of core components: Analytics, Ads, Login, Account Kit, Share, Graph API, App Events and App Links. For example: Using Facebook's SDK, allows for support of "Login with Facebook" based authentication, which allow users to login using a phone number of email address with their Facebook password. Facebook's SDK also offers Analytics (data, trends, and aggregated audience insights about the people interacting with the app), as well as Ads and reading and writing to Facebook's Graph API.”

Product terms and conditions often suggest consent is a necessary basis for data processing, not because of the purposes to which the school will use a school child’s personal data but how the product and its suppliers will use it. However, when one accepts that consent as a data processing lawful basis, it cannot be freely given and therefore cannot be lawful in the school environment for routine tasks due to the imbalance of power in the relationships

between children, families and school staff — and with only an indirect relationship between the child and the product owners. This means third-parties' expectations of what they are permitted to do must change.

II.14.3 Lawful basis for processing

The European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects (October 2019) in most cases, a user enters into a contract to avail of an existing service. While the possibility of improvements and modifications to a service may routinely be included in contractual terms, such processing usually cannot be regarded as being objectively necessary for the performance of the contract with the user, and this is in particular true in the school environment in which there is no direct relationship between a child and a company.

In relation to the processing of special categories of sensitive personal data, in the guidelines on consent, the working party 29 also observed that GDPR Article 9(2) does not recognize 'necessary for the performance of a contract' as an exception to the general prohibition to process special categories of data. It should therefore follow that, 'necessary for the performance of a product' is not a substantive reason for seeking an exemption from data protection law. In other words, schools, companies and product developers should not expect to be exempt from enforcement action, simply because the product works in ways that are not rights-respecting.

If the majority of data processing services and tools to schools available to today, do not meet the high standards of the law as well as as ethical expectations of what should be done with children's personal data, then a new approach is needed.

Even the US, which has traditionally resisted privacy legislation, is changing its tune. At the time of writing, the US Federal Trade Commission has a consultation open on the Implementation of the Children's Online Privacy Protection Rule (COPPA). It asks whether the consent requirement been effective in protecting children's online privacy and safety. Given how much data on children in Europe is either collected or processed by US companies, the COPPA consultation must be monitored closely.

II.14.4 Guidance for developers in the context of edTech is needed

The expected standard for the processing of children's data in the education sector should set a high bar by design, to meet acceptable quality levels and the rule of law. This must be supported by a combination of sector guidelines, statutory codes of practice and more sector specific enforcement by regulatory authorities.

Such standards may be set out in Codes of Practice and it is imperative that there is wide cooperation in drafting with developers, industry, with education practitioners, academia, organisations representing teachers, families, and civil society.

Conclusion: Who will frame the future?

Policy makers should not be afraid to be ask to what extent the rapid growth of technology aimed at school children and the automation of their school administration is in the best interests of the child.

> *"Taken together, the correlational and experimental evidence does not offer a convincing case for the general impact of digital technology on learning outcomes. This is not to say that it is not worth investing in using technology to improve learning. But it should encourage us to be cautious in the face of technological solutions to educational challenges. Careful thought is needed to use technology to best effect.*" (Higgins, S., Xiao, Z. and Katsipataki, M., 2012)

It is similarly wise to apply caution to the claims in company marketing in all emerging technologies.

> *"What is meant when organisations apply 'AI' to a problem is often indistinguishable from the application of computing, statistics, or even evidence. The usage of the phrase has become so laughably ambiguous and general, it is almost like saying that to solve an urban infrastructure problem, one must 'apply power tools'…*
>
> *Ben Green addresses these issues in his recent book, The Smart Enough City, highlighting the need to see technology as just one tool in a toolkit: just one of many means that might potentially be used to head towards a complex and societally negotiated end. The focus should be on taking off the 'tech goggles' to identify problems, challenges and needs, and to not be afraid to discover that other policy options are superior to a technology investment.*" (Veale, M. 2019)

The purpose of this Convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection"). Respect for one's "private and family life, his home and his correspondence, subject to certain restrictions that are "in accordance with law" and "necessary in a democratic society" means a right to be free from interference.

This report should support policy makers' understanding of the need to shift from a compliance culture, to a rights'-respecting culture in education data processing. Recommendations must recognise professional autonomy, and also ensure additional prescription of expected high standards.

If we remain on the current path and its direction of travel with regard to data processing in education, the balance of power will be forever in corporate giants' favour. It is they that will determine the offering, the safety, and the institutional memory of state education systems, and the effects those systems have on millions of children every day.

The state and corporate knowledge base of individual lives stored in school information management systems, thousands of apps and platform systems will follow a child seamlessly across each stage of education into employment. Vast volumes of data from the past will be relied upon by school staff ever more fearful that their human judgement is less worthy than that of the machine-led decision. Predictions will pre-determine children's curriculum and life choices from ever earlier ages.

Genetic differences between children will be used to risk stratify them from birth, and apply or withhold educational interventions differently. Selection of a child's school place that shapes

so much of their life today, could shift to selection in the womb based on which cognitive characteristics will be seen as desirable and which as anomalies, or whether a child with additional needs will have a place in the world at all.

Or policy makers can prioritise ways to enact and enable the human rights and values that underpin the Convention in practice.

If this generation is not to be held back by the data burdens of their past, but should have the freedoms needed to shape it, then children must be able to exercise their right to education in a way that is not detrimental to their own and their collective future. The balance of power between organisations and institutions compared to that of the child and the family must be made to change with urgency,

"The eyes of all future generations are upon you. And if you choose to fail us, I say - we will never forgive you." (Greta Thunberg, UN Climate Summit, September 2019)

Definitions

1. For the purposes of this report

a. “Personal data” means any information relating to an identified or identifiable individual (“data subject”).

b. “Sensitive data” means personal data over which an individual may have an expectation of confidence, such as behaviour markers that are indicative of violence but have not been determined in a court so are not technically ‘criminal convictions’ or familial income, but that may not fall under the definitions of special category data of data protection law.

c. “Special category data” has the same meaning as Article 6 of the Modernised Convention 108+. “The processing of: genetic data; personal data relating to offences, criminal proceedings and convictions, and related security measures; biometric data uniquely identifying a person; personal data for the information they reveal relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life, shall only be allowed where appropriate safeguards are enshrined in law, complementing those of the Convention. Such safeguards shall guard against the risks that the processing of sensitive data may present for the interests, rights and fundamental freedoms of the data subject, notably a risk of discrimination.”

d. “Processing” means any operation or set of operations carried out partly or completely with the help of automated processes and applied to personal data, such as storage, conservation, adaptation or alteration, extraction, consultation, utilisation, communication, matching or interconnection, as well as erasure or destruction.

e. “Profile” (n) refers to a set of data characterising a category of individuals or behaviours that is intended to be applied to an individual or group of individuals.

f. “Profiling” means an automatic data processing technique that consists of processing data with the intention of applying a “profile” model to an individual, to fit the individual to a category or match attributes with the model, particularly in order to take decisions concerning the subject, or to make interventions, or for analysing or predicting their personal preferences, behaviours and attitudes. These may be created from data the data subject others provide, or that are opaque to them, such as interaction data from using a platform, that are sent from the device to the company, but the users do not see.

g. “Information society service” refers to any service, normally provided for remuneration, at a distance, by electronic means and the same definition as the Article 1(1)(b) of Directive (EU) 2015/1535.

h. “Controller” means the natural or legal person, public authority, agency or any other body which alone, or in collaboration with others, determines the purposes of and means used in the collection and processing of personal data.

i. “Processor” means the natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.

j. “Click-Wrap' agreements” means agreements about terms and conditions that the company or product vendor does not permit the school or user to change. They come as

a package that the school can only accept or refuse, and refusal will mean they are no longer able to continue to use the product or platform.

k. “Daisy-chain” of distribution means a series of transactions that are joined together, which enable multiple third parties to extract or receive data from the previous party in the chain. The image is of a linked chain of flowers that children may commonly join together.

Acknowledgements

The author would like to express her thanks to the very many individuals who have shared their own work and insights in support of this work, from around the world. In particular to thank those who contributed directly and most significantly on their specialist subjects, including Dr. Ben Williamson, Chancellor's Fellow at the Centre for Research in Digital Education and the Edinburgh Futures Institute; and Dr. Jun Zhao, Senior Research Fellow at the Department of Computer Science, Oxford University, with insights for developers.

References

Aftenposten (2020) *Datatilsynet undersøker om det er lovlig å bruke Google i skolen*. The Norwegian Data Protection Authority has announced it is investigating whether it is legal to use Google in schools. (accessed February 21, 2020) https://www.aftenposten.no/norge/i/pLvba6/datatilsynet-undersoeker-om-det-er-lovlig-aa-bruke-google-i-skolen

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)

Alim, F., et al (2017). (Electronic Frontier Foundation) Spying on Students: School-Issued Devices and Student Privacy, https://www.eff.org/files/ 2017/04/13/student-privacy-report.pdf

Andrejevic, M. and Selwyn, N. (2019) Facial recognition technology in schools: critical questions and concerns, Learning, Media and Technology, DOI: 10.1080/17439884.2020.1686014

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. (accessed October 2019) https://www.cl.cam.ac.uk/~rja14/Papers/kids.pdf

Ars 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

Balderas (New Mexico) vs Google LLC, 2020 https://cdn.vox-cdn.com/uploads/chorus_asset/file/19734145/document_50_.pdf (accessed February 24, 2020)

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

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

Bowles, N., (2019) New York Times. Silicon Valley Came to Kansas Schools. That Started a Rebellion. https://www.nytimes.com/2019/04/21/technology/silicon-valley-kansas-schools.html

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/

Campaign for a Commercial Free Childhood (2015) https://commercialfreechildhood.org/3-million-teachers-mcdonalds-were-not-lovin-it/

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

Class Dojo (company blog) What The New York Times Got Wrong.https://web.archive.org/web/20191113122736/ https://www.classdojo.com/en-gb/nyt/

CNIL decision on facial recognition (lycée les Eucalyptus à Nice et lycée Ampère à Marseille) (2019) Expérimentation de la reconnaissance faciale dans deux lycées : la CNIL précise sa position https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

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

Council of Europe study DGI(2019) 05 Responsibility and AI (Rapportuer: Yeung, 2019) Prepared by the Expert Committee on human rights dimensions of automated data processing and different forms of artificial intelligence (MSI-AUT)https://rm.coe.int/responsability-and-ai-en/168097d9c5

Council of Europe (2017) Unboxing Artificial Intelligence, Ten Steps to Protect Human Rights https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64

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) 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/ based on https://www.gov.uk/government/publications/dfe-external-data-shares

Denham, E. The Information Commissioner, ICO, (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

EdTech Innovation testbed, Nesta (2019) https://www.nesta.org.uk/project/edtech-innovation-testbed/ frequently-asked-questions/ permanent record at https://web.archive.org/web/20191015162357/ https://www.nesta.org.uk/project/edtech-innovation-testbed/frequently-asked-questions/

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 (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., (2013) Data Horizons: New forms of Data for Social Research, School of Social Sciences, The University Of Manchester,) 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

European Union Agency for Fundamental Rights (2019) FRA has collected information on AI-related policy initiatives in EU Member States in the period 2016-2019. The collection currently includes about 180 initiatives. https://fra.europa.eu/en/project/2018/artificial-intelligence-big-data-and-fundamental-rights/ai-policy-initiatives

European Data Protection Board Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects https://edpb.europa.eu/ sites/edpb/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.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/

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

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 (2019) 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

Higgins, S., Xiao, Z. and Katsipataki, M. (2012) The Impact of Digital Technology on Learning: A Summary for the Education Endowment Foundation. School of Education, Durham University

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:// d e f e n d d i g i t a l m e . c o m / w p - c o n t e n t / u p l o a d s / 2 0 1 9 / 0 7 / AIHLEGPolicyandInvestmentRecommendationspdf.pdf) (Following an open selection process, the Commission appointed 52 experts to a High-Level Expert Group on Artificial Intelligence, comprising representatives from academia, civil society, as well as industry.)

IB Times, (2017) 77 Million Accounts, Students, Teachers, Parents Stolen, by AJ Dellinger, 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 (2018) (40th International Conference of Data Protection and Privacy Commissioners 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, (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. (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, (UK) 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

Monahan, T. and Torres, R (2009) Schools Under Surveillance: Cultures of Control in Public Education (Critical Issues in Crime and Society) Rutgers University Press, ISBN: 081354680X

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

Nemorin,S. (2017) University College London, Affective capture in digital school spaces and the modulation of student subjectivities. Emotion, Space and Society, ISSN 1755-458 http://eprints.lse.ac.uk/83298/

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. (2010) The Royal Academy of Engineering, 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. (2019) Gaggle CEO, Education Week, 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 de-personalized learning and win the right to opt out (2019) https://www.studentprivacymatters.org/ kansas-students-join-the-rebellion-vs-summit-and-depersonalized-learning/

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

Pegg, McIntyre (2018) The Guardian, https://www.theguardian.com/society/2018/sep/16/child-abuse-algorithms-from-science-fiction-to-cost-cutting-reality (accessed February 2020)

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

Poland DPA first decision and fine under the General Data Protection regulation https://uodo.gov.pl/en/553/1009 concerning the lack of fair processing to data subjects, citing disproportionate effort, as well as the unlawful processing of personal data collected from publicly available sources, at scale.

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. (2018) University of Western Australia, 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

Privacy International Report — How Apps on Android Share Data with Facebook (even if you don't have a Facebook account. (2018) https://privacyinternational.org/sites/default/files/2018-12/How%20Apps%20on%20Android%20Share%20Data%20with%20Facebook%20-%20Privacy%20International%202018.pdf

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

Regan, P and Steeves, V. (2019) Education, privacy, and big data algorithms: Taking the persons out of personalized learning https://doi.org/10.5210/fm.v24i11.10094

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)

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., (2019) Monash University, Australia, What are the acceptable limits of school data? The case of the Florida 'school safety 'database 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, (2016) Shadow of the smart machine: Will machine learning end? https://www.nesta.org.uk/blog/shadow-smart-machine-will-machine-learning-end (accessed September 2019)

Southgate et al., (2019) Artificial Intelligence and Emerging Technologies in Schools, commissioned by the Australian Government https://docs-edu.govcms.gov.au/system/files/doc/other/aiet_final_report_august_2019.pdf

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

Steeves, V., Associate Professor, Department of Criminology, Faculty of Social Sciences. The Interdisciplinary Research Laboratory on the Rights of the Child (IRLRC) and Young Canadians in a Wired World, Phase III: Life Online https://mediasmarts.ca/ycww/life-online

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. (2015) Discussion on conformity https://www.youtube.com/watch?v=QHLh485SJXc at CPDP panel, Bentham goes to school: surveillance and student privacy in the classroom.

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

Tucker, W and Vance, A. (2016) School Surveillance: The Consequences for Equity and Privacy. Education Leaders Report (4), National Association of State Boards of Education,. 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)

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.

Veale, M. (2019). A Critical Take on the Policy Recommendations of the EU High-Level Expert Group on Artificial Intelligence. https://doi.org/10.31228/osf.io/dvx4f

Who Knows What About Me (2017) Children's Commissioner, 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

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

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

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