Response to Working Party 29 Guidelines on Automated individual Decision-making and Profiling for purposes of Regulation 2016/679

"The sensitivity of digitized pupil and student data should not be underestimated"
International Working Group on Data Protection in Telecommunications
Working Paper on e-Learning Platforms (April 2017)[1]

Summary

Given that "such a measure should not concern a child" is only in a recital, there is a need for data controllers and processors to understand recital 71 and 38 with a degree of interpretation. However, little attention is paid to the rights or specific profiling experiences of the child. We believe that much clearer guidance on children and profiling and automated decision-making are needed in practice.

Under the GDPR, individuals have the right not to be subject to decisions based solely on automated processing of their personal data, including profiling, which produces (i) legal effects concerning them; or (ii) a similarly significant effect. The GDPR does not define either 'legal effects' or 'similarly significant effects.' Where in practice does predictive scoring of attainment by third party companies fit and on what basis? Sold to schools, some Heads post scores on staff room walls and target interventions with a handful children who will raise or lower the school's overall performance outcome.

Baroness Ludford was one of many peers to point out difficulties in the House of Lords during the Second Reading of the UK Data Protection Bill, on October 10 2017[2]

"We may need seriously to look at the lack of definition of "substantial public interest" as a basis for processing sensitive data, or even of public interest….There is also concern that the safeguards for profiling and other forms of automated decision-making in the Bill are not strong enough to reflect the provisions of Article 22 of the GDPR. There is no mention of "similar effects" to a legal decision, which is the wording in the regulation, or of remedies such as the right of complaint or judicial redress."

Claims of public interest from the State can be far reaching, and well beyond reasonable expectations and the original purpose of data collection at local and national level. Our research into school census expansion plans[3] to collect nationality data in 2016 revealed an agreement for monthly handovers of up to 1,500 children's national pupil data for immigration enforcement. This impinges on fundamental rights to privacy and the basic data protection principles of purposes limitation and fairness.

Commercial products are widespread in schools and higher education bodies are increasingly buying AI solutions, sold as ways of reducing workload and increasing efficiency through reduced admin. time. The resulting rapid transfers of pupil data to commercial third parties, have no oversight. If processing should not routinely concern a child, there will need to be change and very strong codes of practice and enforcement in England, to respect the intent of the GDPR, this WP29 guidance, and CoE Principle 3.5,[4] "*profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the UNCRC.*"

When contextualizing children's right to privacy among their other rights, best interests and evolving capacities however, "i*t becomes evident that children's privacy differs both in scope and application from adults' privacy.*"[5]

[1] Working Party 29 Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools) http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf
[2] http://hansard.parliament.uk/Lords/2017-10-10/debates/22188EC1-6BAB-4F06-BE64-5831ABAF78E2/DataProtectionBill(HL)
[3] 2016 school census in England http://defenddigitalme.com/wp-content/uploads/2017/08/Briefing_pupildata_BorderForce_Nationality.pdf
[4] CM/Rec (2010)13 adopted by the Committee of Ministers on 23 November 2010
[5] Privacy, Protection of Personal Information and Reputation - United Nations Children's Fund (UNICEF) (2017) https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

Recommendations

1. Commissioner registration should be obligatory without exemptions, for processing of;
    a. personal data used in automated decision making, in particular for children,
    b. for the purposes of GDPR Article 9 (1) and (4) (Processing special categories of personal data) including “data concerning health” with the meaning of Article 4(15);
    c. data processing concerning the profiling children

2. IV. B(5), V. and III.B. More guidance is needed regards “Article 6(1) (e) – necessary for the performance of a task carried out in the public interest or exercise of official authority; “*might be an appropriate basis for public sector profiling in certain circumstances*.” On what constitutes necessary use, and significant effect. Profiling and automated decision-making with little meaningful ‘human intervention’ are applied routinely in state education in England. These bodies will use this legal basis for most data processing, and where there is no parental oversight or consent. The case studies that follow outline why this is significant.

3. V. The Working Party’s guidance should give clearer guidance on minimum expected safeguards appropriate to a child’s maturity based on capacity not age, with regard to GDPR Article 22 (2)(b) and Article 23 on automated individual decision-making including profiling. Guidance should suggest controller practice reflect the rights of the child where it involves profiling and decision-making, particularly in processing sensitive personal data. Controllers must have particular regard to the rights of the child and their ability, with regard to 9 (2)(c) and 9 (2)(e) and right to be treated in a manner consistent with the promotion of the child's sense of dignity and worth; consistent with the UNCRC, and a child’s best interests.

4. V. Recommendations are needed on expected standards for processing and profiling the genetic, biometric and data concerning health of a deceased data subject, especially a child;[6]

5. III. D (1). Articles 13(2) (f) and 14(2) (g) - Right to be informed: Recommendations should be clearer where parental authorisation[7] is obtained. In particular, where the processing involves profiling-based decision making, for example on tracking walls and children[8] when under the age of Article 8(1). Processing for the purposes of both (a) profiling and (b) making a decision based on the profile generated, must be made clear to the data subject, however there is no consideration given to make this transparent to a parent when it is they, not the subject that has to accept the terms and conditions of use. Guidance should also include a requirement to notify the maturing subject of ongoing retention -- on an annual basis, when processing has been based on parental consent, so as to be able to make their own decision later in life.

6. Guidance is further needed where profiling ascertains information about the data subject’s surrounding attributes, activity or behaviours rather than personal data, outwith Article 4(4), to obtain knowledge about the individual, when the subject of surveillance is a child. There is little known about the use of millimetre microwave technology, for example, which are not processing the biometrics of a body but come into contact or pass through it, to collect data on attributes which are hard to classify as personal, yet could hardly be more invasive.[9]

[6] pursuant to the derogation available in Recital 27 of the GDPR which regards genomics and the potential effect on children's lives from decisions by other family members should be given the highest regard

[7] Lievens, E. and Milkaité, I. Ghent University https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355

[8] https://www.ivir.nl/publicaties/download/EDPL_2017_03.pdf

[9] Electromagnetic radiation scanners use Ultra-Wide Band (UWB) 75-110 GHz, used on crowds to detect potential concealed weapons being carried by individuals. In use by police forces in the UK. (Biometrics-in-Schools, Pippa King, 2017) See also https://www.intellihub.com/millimeter-microwaves-anti-terror-artificial-intelligence-scanning-in-public/ and http://www.radiophysicssolutions.com/industry/security/schools use in schools

Profiling Case Studies

The range of ways in which children are profiled in school-wide applications using children's personal data from school records, often including biometrics, behaviour, photographs as well as sensitive special needs and ethnicity personal data, are not transparent to pupils and parents in England.

Profiling case study: Web monitoring and filtering

In England web monitoring and filtering includes profiling through keyword logging and real-time screen recording of all Internet use, both in school and at home, 365 days a year on school provided laptops or software installed on personal items in bring-your-own-device, as a result of statutory guidance introduced in September 2016 on 'safeguarding in schools'.

[10]Monitoring systems[11], are using artificial intelligence in schools to "*continuously build a profile of all users, allowing the system to accurately interpret between a one-off event or a consistent pattern of behaviour.*" In our research of over 400 schools in England, we are yet to find one policy that makes any mention of the supplier name, or what policy there is on monitoring, keywords of third party access, and retention, error rate, or course of redress. Companies monitor 24/7 every day of the year, including on parent-bought school-use Chromebook purchase schemes, or BYOD bring-your-own-device. Each may potentially may each be affecting the lives of "half a million students and staff in the UK" without oversight or awareness of their accuracy, accountability, or otherwise inside black-box decision-making which is often trusted without openness to human question.

"throughout the year, the behaviours we detect are not confined to the school bell starting in the morning and ringing in the afternoon, clearly; it is 24/7 and it is every day of the year. Lots of our incidents are escalated through activity on evenings, weekends and school holidays. Invariably, although the volume decreases, for example, during the six-week school holiday."[12]

While there is human involvement *after* the automated-decision, we have been told that where teachers are risk averse, and cannot see the algorithm to understand any discrimination bias or error, it is known that children have been wrongly flagged through using keywords such as 'cliffs' and 'black rhino''. Children and families have no course of redress to have their profile corrected, or deleted, now marked as at risk of suicide, or gang membership. There is no oversight who may view and retain this. The guidance does not address sufficiently what rights a child has to refuse this type of profiling. Digital agreements to 'consent' to school monitoring are compulsory and must be signed by both parents and child. These consent policies are not valid, yet parents and pupils are obliged to comply.

The opinion of the Working Party 29 2(2009) noted, "I*t 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. Legislators, political leaders and educational organisations should, in their respective areas of competence, take effective measures to address these issues.*"

Since the introduction of schools 'statutory guidance,' and the Investigatory Powers Act 2016[13] children in England are commonly under surveillance,profiled online and off, in both public and private space and time. Web monitoring can mean their Internet use, or that of other people may be recorded in any room in their house, at any time of day. Some providers have known security vulnerabilities.[14]

[10] Safeguarding-in-Schools statutory guidance https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
[11] Smoothwall Visigo AI Classroom monitoring software https://kb.smoothwall.net/Content/general/Introducing_Visigo.htm
[12] Mark Donkersley, Managing Director, e-Safe Systems Limited, Parliamentary Select Committee October 2016
[13] The Investigatory Powers Act 2016 http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted
[14] Impero Education vulnerabiities https://lizardhq.rum.supply/2015/08/04/impero-2.html

Profiling case study: Apps integrated with school information management systems

Schools use commercial apps which use children's personal data to create profiles

- that create persistent behavioural records[15]
- that claim to use AI and machine learning to profile that behaviour and claim to automatically generate seating plans based on how children influence one another.
- for administration such as homework communications and tracking, or sickness tracking, and cashless payment systems that store parents' financial details and child's personal profile.
- Biometric data in library, print, locker and canteen service use based on fingerprints, profile children's biometric data and children's activity down to the nth degree, even to what they buy and its nutritional content. Records of 'consumption' which are actually records of spend, are sent to parents. At what point of maturity should a child have the right not to be profiled for parental oversight, and where does well-being stretch beyond necessity, into curiosity?

There is no oversight or accountability for the ethical or privacy effects of education technology in use in UK state schools. Many of these commercial apps are free to schools, but offer premium in-app paid services to parents and pupils over time, or other secondary services such as private tutoring.

School-wide seamless integration with the pupil information management systems, means that children's personal data are sent to a range of commercial third party providers to create profiles *before* the parent and pupil have been informed, and without any choice or ability to say no. The providers - such as cashless payment systems - create activation codes for parent sign-in. The data transfer has already taken place, before parents have any opportunity to refuse to use the scheme. They profile purchasing, attainment, equipment use, building access times, sickness or behaviour.

Profiling of attainment, behaviour and biometrics are routine and part of everyday delivery of education in England. Parents and pupils are given no choice and are rarely offered privacy policies of classroom providers or apps, even on request. Rights to correction, data minimization and to be informed about retention policies or deletion are missing as a rule, rather than exception.

Profiling case study: Health and physical tracking in schools

Sports researchers recently carried out a study[16] of teenagers at school and found fitness trackers and health apps and devices may not be positive health promotion tools. Wearing the device made some pupils lose confidence in their physical ability. Others said the device made them feel fat and uncomfortable with their peers.Their reasons for taking part in physical activity also changed. For example, more pupils reported taking part in physical activity because they felt pressurised.

Profiling case study: identity and physical tracking using biometrics in schools

A West Cheshire school required tagging pupils' movements around the campus in 2013. In a trial of up to three years, pupils at West Cheshire College wore tags that allowed them to be tracked in detail throughout the college's three campuses. *"The technology was introduced with the aim of assessing how it could be used for self-marking class attendance registers, safeguarding purposes, and to improve the physical management of the buildings.*" It was discontinued in February 2013, when a review showed that "t*he technology did not enhance current systems or business operations*" and the college became concerned about rising costs to maintain the system. This case study was brought

[15] ClassDojo poses data protection concerns for parents, Williamson, B. and Rutherford, A. Stirling University (2017)
[16] The Motivational Impact of Wearable Healthy Lifestyle Technologies: A Self-determination Perspective on Fitbits With Adolescents, Kerner, C. and Goodyear, V. Brunel University London (2017) http://www.tandfonline.com/doi/full/10.1080/19325037.2017.1343161

into the public domain through Freedom-of-Information and research work in 2012-13 by Pippa King, Biometrics-in-Schools[17] and there is no duty to have public consultation and rarely any meaningful consent processes or opt-out alternatives on use of such measures. Use of biometric technologies continues to expand. More recently, Ed-Tech start-up SCM Secure, has reportedly deployed its biometric palm vein solution at two childcare facilities in Oxford, UK.[18]

Further, it is impossible for a child to not make their face, 'manifestly public' (via CCTV or IPTV) as per GDPR Article 9 (2)(e) outside, and it is not uncommon for schools to install these in bathrooms.[19]

Profiling case study: Racially profiling students in University (Civitas Learning)

At some of England's universities, a system profiles university students' past five years of attainment data to 'predict' vulnerability to future 'low achievement' using factors that range from failing a module to country of birth, gender, age, ethnicity - and many other factors recorded and available to all academic staff to see. Staff can use filters to pull up 'at risk' students by ethnicity or country of birth for example, and see student names, personal email, student ID, and have the ability to edit. Staff are told to tailor their approach to students accordingly. Academics have spoken to us, concerned about data accuracy, bias, and security because hundreds of academic staff have access.There is concern over the risk of discrimination through the racial profiling of the entire student population, with weak 'consent' model that students feel pressured to accept but little understand. Jisc are seeking[20] to *'make the market' for UK learning analytics*, working with Civitas Learning. JISC[21] considers this an example where solely automated profiling [of young adults and other students] is positive, and would be "*a breach of privacy if all such notifications were reported to tutors for review; students have expressed a fear that such reports might influence their marks*" and assumes that human intervention is rare and therefore a good thing. From what we have been told the implementation, as described above, is rather different in practice and how they believe error or system error/bias could be identified without human intervention, and avid human discrimination with it, are impossible to see.

Child Rights to Privacy

Data protection best practice is not always aligned with the controller's notion of reasonable or ethical expectations of privacy. The default public interest position in the UK is for sharing of administrative data for secondary purposes is an opt-out, not opt-in mechanism, where one exists at all, even in health since the Care Act 2014, and Digital Economy Act 207. For children this is impossible where parents take decisions on their behalf which cannot be revoked, such as to the use of their heel-prick test at birth[22] which currently has a bundled consent process with direct care. This makes privacy a right that needs defended, rather than one that is respected by default. While the right to privacy is not an absolute right; it is not well balanced against other fundamental rights, in accordance with the principle of proportionality, or respecting fundamental freedoms in UK education or health for children.

Some academics[23] are pushing the boundaries of research and profiling, or what constitutes "public" on social media, open to children 13+ (Facebook) or 16+ (LinkedIn). The UK government is keen to promote edTech[24] in schools. To enable safe use of AI we need much stronger enforcement of

[17] Biometrics in Schools http://pippaking.blogspot.co.uk/p/home.html
[18] Palm readers infants http://www.biometricupdate.com/201710/scm-secure-deploys-biometric-palm-vein-solution-for-uk-child-care-facility
[19] The Guardian https://www.theguardian.com/education/2017/nov/02/secondary-school-cctv-pupil-toilet-areas-summerhill-surveillance
[20] JISC, Creating a collaborative, integrated learning analytics service (2016)
https://www.jisc.ac.uk/blog/creating-a-collaborative-integrated-learning-analytics-service-fit-for-the-sector-25-jul-2016
[21] JISC WP29 response
https://community.jisc.ac.uk/library/consultations/2017-article-29-guidelines-profiling-and-automated-decision-making
[22] NHS newborn screening http://defenddigitalme.com/wp-content/uploads/2016/09/DDM_Newborn_Screening_Consultation2509.pdf
[23] Using Twitter data for demographic research, Yildiz, D.,Munson, J. Vitali,A. Tinati, R. Holland, J (2017)
https://www.demographic-research.org/volumes/vol37/46/
[24] UK Digital Strategy 2017 https://www.gov.uk/government/publications/uk-digital-strategy/uk-digital-strategy

profiling responsibilities and rights. At the time of writing, we look set to lose protection in the Charter of Fundamental Rights.

Children in England need to know authorities will not only provide clarity and confidence to processors and controllers but that every child can expect their rights are enforced so they can entrust their digital identity to third parties at a time of future socio-political uncertainty, and technological advance.

About defenddigtalme

defenddigitalme is a non-profit, non-partisan, data privacy and digital rights campaign led by parents, to make all children's data safe, fair and transparent across the education sector in England.
The campaign is funded by a single annual grant awarded by the Joseph Rowntree Reform Trust Ltd. in April 2017. We hereby consent to the publication of personal data contained in this document.