Automated individual decision making, including profiling

1. Recital 71 "such measure should not concern a child".[1]

Current amendment 74A, page 7, line 11, at end insert "( ) This section does not apply in respect of a child."

A new amendment might be positioned. either within Chapter 2, Lawfulness of processing, after the clause 8, Child's consent in relation to information society services, alternatively after the current clause 13, automated decision making safeguards

page 5, line 11, at end insert "()
OR
page 8, line 1, at end insert "()

Automated individual decision making, including profiling

Controllers and processors must not carry out solely automated processing, including profiling, that produces legal or similar significant effects (as defined in GDPR Article 22(1)) in respect of a child."

There is a risk that the current position of amendment 74A could mean its interpretation that the safeguards in clause 13 should not apply, and cause confusion or potentially remove safeguards for children if subjected to solely automated decision making.

The intent to protect children will likely be lost in practice if not made explicit. This recital is vital if we are to properly protect children from aggressive marketing including geolocators profiling children's movements and behaviours[2], without understanding or regulation. Concerns that children's data for fraud and crime prevention or similar would be negatively affected, should be allayed as it does not preclude processing, only that it should not be "solely automated". These caveats are also outlined in Recital 71.

The ICO also notes in their documentation on profiling and automated decision making that children need particular protection with regard to their personal data. "*Controllers must not carry out solely automated processing, including profiling, that produces legal or similar significant effects (as defined in Article 22(1)) in respect of a child.*"[3]

Why the Safeguards in Clause 13 p 7 of the bill (GDPR 22 (2)(b) are insufficient and inappropriate for children

Note while Article 22 (2)(a) has exemptions for (a) contract, (b) the Union law with safeguards, and (c) based on explicit consent, recital 71 acknowledges this, and yet is still explicit that, "such measure should not concern a child". Safeguards are therefore considered insufficient in GDPR, as similarly outlined in CM/Rec (2010)13 adopted by the Committee of Ministers of the Council of Europe, and in recent UNICEF discussion papers.

If this article were explicit on the Bill, it would remove the need for data controllers and processors to understand recital 71 and 38 or goodwill that "such a measure should not

[1] https://gdpr-info.eu/recitals/no-71/

[2] Child safety smartwatches 'easy' to hack, watchdog says http://www.bbc.co.uk/news/technology-41652742 and Report #WatchOut https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf

[3] p23 https://ico.org.uk/media/about-the-ico/consultations/2013894/ico-feedback-request-profiling-and-automated-decision-making.pdf

concern a child". It is better than amendment 74A because 74A assumes data controllers understand therefore why GDPR Article 22 safeguards should not be required.

A minor *can* enter into a contract. However, the law also assumes that a minor cannot understand the implications of a contract. So, whatever caveat is drafted into the contract, he or she will remain protected to the disadvantage of the other party.

Further, a contract with a minor is voidable. That means they are able to cancel any contract at any time before reaching the age of 18 and for a reasonable period after that time. The Bill reduces the age of parental verification down to 13.

Minors 13-18 still need protections from these effects. A minor cannot adequately provide an agreement or consent to automated profiling if they are unable to see or understand the mechanism behind it or appreciate the implications of legal or similar significant effects.

Many of the most powerful protections for children under GDPR are not in articles, but stated as intent in recitals, and stem for the principles in recital 38:.

GDPR Recital 38: "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child."*

2. UNICEF discussion paper on privacy and freedom of expression: Oct 2017[4] and The Convention on the Rights of the Child (CRC)

When contextualizing children's right to privacy among their other rights, best interests and evolving capacities, however, "it becomes evident that children's privacy differs both in scope and application from adults' privacy."[5]

"While there is now a widely accepted public imperative to protect children from harm, abuse and violence online, there has been comparatively little consideration of how to empower children as active digital rights-holders."

"While behavioural advertising provides a way for companies to offer consumers greater convenience, this brings a concomitant risk to users' privacy as behavioural profiling incentivizes the collection of increasingly larger amounts of personal data."

3. Council of Europe Recommendation CM/Rec (2010)13 adopted by the Committee of Ministers on 23 November 2010

The Internet of the future will therefore not just connect human beings with one another but will also interlink smart devices (an Internet of things) that surround people in their everyday lives and accompany them as they move around and carry out their daily activities. In this world of "ambient intelligence", objects will constantly monitor and analyse the behaviour of

[4] https://www.unicef.org/csr/ict_paper-series.html

[5] PRIVACY, PROTECTION OF PERSONAL INFORMATION AND REPUTATION United Nations Children's Fund (UNICEF) March 2017. https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

human beings around them, probably without their knowledge, so as to interact with them in a dynamic way."[6]

"Principle 3.5 recommends that, in principle, the profiling of persons who cannot freely express their consent be forbidden, especially, for example, adults with incapacity and children, within the meaning of the United Nations' Convention on the Rights of the Child".[7]

"Considering that the profiling of children may have serious consequences for them throughout their life, and given that they are unable, on their own behalf, to give their free, specific and informed consent ***when personal data are collected for profiling purposes, specific and appropriate measures for the protection of children are necessary*** *to take account of the best interests of the child and the development of their personality in accordance with the United Nations Convention on the Rights of the Child."*

4. If Article 8, reduces the age at which a commercial company can collect, and exploit a child's personal data without parental oversight, it is therefore necessary for additional protections on the face of the Bill.

Many academics and child's rights groups, worry that with respect to Article 8 and age verification, "GDPR will have the unintended consequence of generating many "under-age" users, misleading potential sexual abusers about the age of their intended victims or, worse, allowing them to claim a defence in these terms."[8]

The GDPR's provision for children is riddled with uncertainties.[9]

Clarity will help schools and universities apply the law with the due regard to privacy by design that GDPR Article 25 requires, as well as Recital 38 that children merit special protections as they are less aware of the risks, "creating personality or user profiles". Recital 71 should mean protection from profiling purposes. Clarity on this in explicit terms, will support developers of online information society services not hinder them.

5. Five case studies: Young people and schools often cannot see risk[10] and unintended consequences such large datasets, profiling and automated decision making have, even with consent or legal grounds for processing. Researchers and universities use data for predictive operational purposes, without transparency or protections from outcomes. Applied use is growing.

a. Profiling case study: Racially profiling students in University (Civitas Learning)[11]

Systems show all students' past five years of attainment data to 'predict' vulnerability to future 'low achievement'. Uses top ten 'predictors' (factors that range from failing one module to country of birth, gender, age, ethnicity - and many other factors recorded and available to all academic staff to see). Academic staff can use filters to pull up 'at risk' students by ethnicity or country of birth or anything else - and we get the student name, personal email, student ID, ability to add in more personal data. Staff are told to use this data to tailor our approach to students - ie you are Muslim or black or foreign and data

---

[6] The Council of Europe The protection of individuals with regard to automatic processing of personal data in the context of profiling p23 para 27 https://rm.coe.int/16807096c3

[7] ibid p47 para 120

[8] http://blogs.lse.ac.uk/mediapolicyproject/2017/02/09/online-challenges-to-childrens-privacy-protection-and-participation-what-can-we-expect-from-the-gdpr/

[9] http://blogs.lse.ac.uk/mediapolicyproject/2016/12/12/the-gdpr-using-evidence-to-unpack-the-implications-for-children-online/

[10] V-Tech was a very public breach affecting hundreds of thousands of UK children http://www.bbc.co.uk/news/technology-34963686 and Edmodo a large breach in schools.

[11] Blog https://www.mynsu.co.uk/blogs/blog/tallykerr/2017/08/02/Learning-Analytics/

shows you are in danger of getting a poor degree. Academics are concerned about data security if hundreds of academic staff have access and complicity in racial profiling of entire student populations in teaching and pastoral practice.

b.The University of Cambridge Institute of Criminology: profiling in research

Research has its own exemptions. But as a case study, these researchers were given identifying national pupil data in 2013 for use until April 2019, to predict pupil exclusion for London schoolchildren. This is ongoing (as listed in the third party register of identifying pupil data releases). Yet there is no quality check for data accuracy or effect. **Adding "young offender" as a code on pupils named records for life, to be collected from January 2018 (SI 807/2017) for the first time therefore a significant change.** What oversight will there be of data used in research, and without small numbers suppression?

c. Profiling case study: Predictive policing research and operational support

Identifying pupil data was requested by UCL researchers working in conjunction with operational police forces, to use in predictive policing research. (also Third party register)[12] Again, how might offender and reasons for exclusion like 'theft, violence, drugs' all which are not criminal convictions, but last forever, and may not even be accurate but are a Head's best ascription (consider the teens who may take the exclusion for their friend). This was rejected, but on what basis, and what might be today, may not be tomorrow. It is reminiscent of the MOD requests for targeting career marketing[13]. It is only a matter of time for scope creep to mean all sorts of profiling and algorithms run on pupil data that we cannot understand, and as yet, no one is questioning the desired outcomes, bias in training data or output. What kind of school and society will we hope to see as a result?

d. Behaviour. In classrooms today automated profiling is being sold to schools as a way to track pupils 24/7 even to design seating plans. These are not transparent on cost, benefit and security risk.

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

- that create persistent and permanent behavioural records,
- that claim to use AI and machine learning to profile that behaviour and claim to identify how pupils interact, and using AI to automatically generate seating plans.
- Mandatory web monitoring[14] imposed by school is compulsory and profiles children's keyword use and internet activity 365 days a year 24/7[15] even personal Bring-Your-Own-Devices, in private time, at home and in holidays
- 95% of children referred to Prevent require no action is taken - what is the error rate, false flags and what happens to those children's records recorded in error? Risk aversion in people means over reliance on automated profiling.[16]

e. Biometrics, RFID and CCTV[17] are commonly used to profile children without transparency or choice in education, in public space and in their private time.

A West Cheshire school required tagging pupils' movements around the campus[18]. In a trial of up to three years, ending in February 2013, pupils at West Cheshire College wore tags that allowed

---

[12] Third party register of identifying pupil data use http://defenddigitalme.com/2017/10/who-got-your-pupils-personal-and-school-data-in-2017/

[13] Schools Week – MoD requests sensitive pupil data… by mistake Schools Week Army recruiter considers appeal to access pupil data

[14] https://schoolsweek.co.uk/mandatory-web-monitoring-in-schools-opens-a-slippery-can-of-worms/

[15] Hansard, Mark Donkersley http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/communications-committee/children-and-the-internet/oral/41158.html "it is 24/7 and it is every day of the year, evenings, weekends and school holidays"

[16] http://www.bbc.co.uk/news/uk-41927937

[17] School move to install cameras in pupils' toilets divides parents http://www.bbc.co.uk/news/av/uk-england-birmingham-41845809/school-move-to-install-cameras-in-pupils-toilets-divides-parents

[18] Wendy Grossman, Guardian Nov 2013 https://www.theguardian.com/technology/2013/nov/19/college-rfid-chip-tracking-pupils-invasion-privacy

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 "the technology did not enhance current systems or business operations" and the college became concerned about rising costs to maintain the system.

6. Page 126 line 8, Schedule 2, Para 4 3(a) would remove the rights of Article 13 (2) (f) to understand that their data are subject to such profiling and automated decision making if used in "immigration purposes". It must be clear, such measures should not concern a child. Page 126, line 10, Para 4 (3)(b) regards article 14(1) to (4) means that the right to rectification in GDPR article 14 (2)(c) would be removed.

Given the error rate of recent Home Office interventions and well documented letters sent in error - even to a newborn baby. The erroneous letter from the NHS trust stated Violet Vipulananthan Horne, who was born in the UK and has two British parents, would need to pay for treatment she had received at a London hospital, because she was not "ordinarily resident" in the UK.[19]

This secrecy is exemplified in the DfE current approach as regards national pupil data. The DfE refuses Subject Access Requests, *contrary* to the usual recommendations of the Office of the Information Commissioner. They would perhaps prefer we have no ability to ask what data are held, and to whom they have been given, and it seems are unwilling to promote transparency and permit National Pupil Database subject access rights. How much harder will it be for parents to prove a child's innocence when the system assumes they are in guilty, and our rights to be informed, to understand and rectify have been removed?

Reference: pupil data use in immigration enforcement [download Briefing.pdf 713 KB]

National School Records were used in secret and nationality added to the data collected while Ministers told the public and parliament, these data would not be passed to the Home Office. We know that up to 1,500 individual pupils' home address and school address may be made available to the Home Office on a monthly basis in an ongoing agreement in place since July 2015. In November 2016, defenddigitalme and other human rights organisations were told that the DfE "might be minded to remove nationality from the algorithm [used by the DfE to match children to provide home and school address for up to 5 years, for the Home Office searches]."

On October 5, the DfE confirmed to Sky News that information obtained from the National Pupil Database was used since 2015 to contact families **to "regularise their stay or remove them".**[20]

7. Smart Toys

Breaches in education are very real and these can include data used for profiling[21]. Growing predictive uses of children's data including biometrics from smart toys and things like smart watches[22].Child smartwatches may profile children's habits and movements, but may not be safe, according to recent report by the Norwegian Consumer Council. *None of the watches "handle data privacy and security particularly well," the researchers found. It was commonly impossible for a user to delete information from the app. And deleting an account only stopped the app from collecting more information -- it did nothing about the data already stored. Only one watch, the Tinitell, required a parent's consent to set up the app to track a child." The fact that a parent has consented to the use of the tool or toy, does not protect the child from commercial exploitation of their data, or misuse.*

---

[19] The Independent 19 Sept 2017, NHS letter demands eight-day-old baby provide identity documents http://www.independent.co.uk/news/uk/home-news/nhs-letter-newborn-baby-eight-day-old-identity-documents-free-healthcare-right-violet-nik-horne-a7955211.html

[20] Sky News 5 October 2017 http://news.sky.com/story/school-census-boycott-over-child-deportation-fear-11067557

[21] 77 Million Accounts, Students, Teachers, Parents Stolen http://www.ibtimes.com/edmodo-hacked-77-million-accounts-students-teachers-parents-stolen-education-social-2540073

[22] Child safety smartwatches 'easy' to hack, watchdog says http://www.bbc.co.uk/news/technology-41652742 and Report #WatchOut https://fil.forbrukerradet.no/wp-content/uploads/2017/10/watchout-rapport-october-2017.pdf