“Data a new direction” consultation response from defenddigitalme

defenddigitalme is a call to action to protect children’s rights to privacy. We are teachers and parents who campaign for safe, fair and transparent data processing in education, in England, and beyond. Our director, Jen Persson, supported the Council of Europe Committee of Convention 108 during the writing and adoption of Guidelines on Children’s Data Protection in an Education Setting in 2019-20.[1]

---

1. Summary

1.1. Children merit specific protection with regard to their personal data

What does the UK want to put first: human flourishing or producing AI for profit? If the intention is to promote both, then we need a robust and consistent method of protecting human rights in a world of machine learning and automated decisions. The proposals in this consultation undermine that. We respond with a particular regard to the impact on children and within educational settings.

This Consultation mentions children only 7 times in 146 pages and fails to engage with the impact these changes will have on them in any substantial way. They are mentioned in passing with respect to the Age Appropriate Design Code, with regard to child sexual exploitation, keeping the ICO complaints process open for children, and four times with regard to scrapping the legitimate interests balancing test. It fails to register where it will have disproportionate impact on children, such as having no consistent standards and approach to the duty of a Data Protection Officer [in a school], or reintroducing a fee regime for subject access requests.

There is no mention of children in the impact assessment. This is despite the fact that children merit special attention, and how data is controlled by them and on their behalf is particularly complex, due to the nature of their capacity which changes over time, and the role of legal guardians.

The GDPR recognises that 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. (Recital 38). Data protection by design and default (Article 25) means that *“measures [that] shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons.”* The right to privacy is also enshrined in Article 8 of the ECHR. And Scotland is set to become the first country in the UK to directly incorporate the United Nations Convention on the Rights of the Child (UNCRC) into domestic law. Under the UNCRC Article 16: “No child shall be subjected to arbitrary or unlawful interference with his or her privacy.” As per Article 16(2), “The child has the right to the protection of the law against such interference.”

States have obligations towards children’s rights. General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights sets out:[2]

> *“The realisation of children’s rights is not an automatic consequence of economic growth and business enterprises can also negatively impact children’s rights,”* and *“States should require businesses to undertake child-rights due diligence.” (3)(62)*

The proposals fail to take account of these issues and the consultation would benefit from a full Child Rights Impact Assessment.

[1] The Committee of Convention 108 adopted Guidelines on Children’s Data Protection in Education Settings in Nov. 2020 https://www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting-

[2] UNCRC General comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights https://www.refworld.org/docid/51ef9cd24.html

1.2. Public engagement has not been carried out with children

By denying children any meaningful way to participate in this consultation, as much as no impact assessment of its implications for them, the Department perpetuates the problem and Lupton and Williamson's conclusions in their work on the datafied child (2017),[3] that in many approaches to the datafication and dataveillance of children fail to offer, "opportunities to participate in matters that affect their wellbeing and enable them to play an active part in society. There remains little evidence that specific instruments to safeguard children's rights in relation to dataveillance have been developed or implemented, and further attention needs to be paid to these issues."

We encourage the consultation to consider our recent report, *The Words We Use in Data Policy: Putting People Back in the Picture* (September 2021).[4] Just as debate on data in UK policy often steers towards misrepresentation of personal data as something 'depersonalised', it also dehumanises the involvement of people in the process. This consultation fails to address what is actually needed in the UK, the infrastructure to create connection between individuals (the public), and the institutions and/or industry that process their personal data.

Across 10 years of public engagement people consistently ask for the same red lines about commercial re-use and anonymisation and to have consent choices respected in the processing of their personal data, across the UK (see Annex I), and young people are little different from adults. At a workshop as part of our research, youth participants discussed what data means to them and three key themes developed: (1) Misrepresentation (2) Power hierarchies and abuses of power and (3) Agency and control over what data used 'in your best interests' may mean. The participants agreed that being misrepresented by data has damaging consequences, and they feel it is incredibly important to have control over your data to have control over how you are represented and ultimately, control over your life and flourishing into adulthood.

Children are hardly included in the National Data Strategy either. In fact, it only mentions children twice: once in section 6.1.4, where children aren't even in focus, but rather they are creators of behavioural data through the "monitoring and reporting of online harms" and the focus is "deriving value" from that. The second mention in is section 6.2.1, which discusses how data can help prevent child abuse. Children are framed in the strategy as a vulnerable subset of society in need of protection but even that, should be monetised by Safety Tech companies.

While there is a commitment to deliver the National Data Strategy through collaboration and "in a way that builds public trust," this consultation offers nothing to describe how that will be achieved or sustained through actions to support children and their families in processing their personal data.

Business needs a level playing field to come from government to interpret the standards that meet their duty to fairness in the data protection sense of principle 1, not conflation with equality of outcomes. Fairness needs tools for communication, "measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means."

---

[3] Williamson and Lupton (2017) The datafied child: The dataveillance of children and implications for their rights https://journals.sagepub.com/doi/abs/10.1177/1461444816686328

[4] defenddigitalme (2021) The Words We Use in Data Policy: Putting People Back in the Picture https://defenddigitalme.org/research/words-data-policy/ A look at national data policy with young people's views on how data is talked about and used

The single point in the consultation that would build a useful starting point here is a tool on 'Transparency mechanisms for algorithms' (paras 288-290). In addition reports are needed to facilitate easy access to know what data is held, not as the proposals suggest, adding barriers to exercising data rights. These proposals will result in a regime that push even more of the risks of data processing back to us, the people, and away from companies, but increasing their reputational risk.

2. Three Key Issues

2.1. Artificial intelligence. The majority of protections around AI are individual and consent based and fail children. Consent is made invalid by the imbalance of power between an authority and data subject. Children cannot consent to what they cannot fully understand and extra protections should be obligatory, not the proposals which will weaken protection from "mutant algorithms".[5] This is not solved by outsourcing obligations to Data Intermediaries for example. According to Michael Sanders, Chief Executive of the What Works for Children's Social Care in September 2020, as regards machine learning in children's social care, now is the time to stop and think, not 'move fast and break things'.[6] "With the global coronavirus pandemic, everything has been changed, all our data scrambled to the point of uselessness in any case."

There are serious issues with the use of AI in education (AIEd) in the UK, which range from concerns around misselling to platforms designed to influence children's mental health. Some of AIEd's risks are reflected in the views of 1225 parents with children aged 18 and under polled by YouGov and commissioned by Nesta in 2019. 61% of parents anticipate that AI will be fairly or very important to the classroom of the near future. However, many are fairly or very concerned about consequences of determinism (77%), accountability (77%) and privacy and security (73%).

Reducing data protection in the area of automated decision making and Article 22 with make those concerns worse and could make adoption less trusted and supported by parents. This will affect learning with and about AI in schools and have short and long term effects on the training and development of a future workforce.

While footnote 44 of the Impact Assessment quotes the number of ICO cases that resulted in "No infringement" or "No infringement with advice given" this standalone number does not tell the whole story. Some of those cases in 2020 were companies and AI, about which parents had complaints in the handling of their child's data at school.

Case study A: ClassCharts Parents that objected to a school introduction of ClassCharts in 2019 brought their concerns to us. They were upset because the school had not consulted on its introduction and had only the information on the company website and data protection impact assessment to understand how their children's data was being used. As part of investigation the ICO revealed that the company did not use AI at all after which in 2020 the company removed previous statements from its website[7] that being "driven by Artificial Intelligence" was its unique selling point. "NQTs, supply & cover teachers will love how our AI engine automatically suggests seating plans

[5] BBC (2020) A-levels and GCSEs: Boris Johnson blames 'mutant algorithm' for exam fiasco https://www.bbc.co.uk/news/education-53923279

[6] Sanders, M. (2020) Machine Learning; Now is a time to stop and think https://whatworks-csc.org.uk/blog/machine-learning-now-is-a-time-to-stop-and-think/

[7] https://web.archive.org/web/20190929221230/https://www.classcharts.com/

optimised for learning & behaviour," they claimed. The product was mis-described for years to schools and is still widely used in the education sector today. The ICO never published its findings.

Case study B: Mental health prediction A second case, in which the ICO took no formal action, was with an AI company operating in schools with thousands of children. Steer Education Ltd claims its product AS Tracking works by tracking the steering biases which are developing in the mind of a student. Concerns voiced by parents and in our complaint included that there was no transparent way that children, staff or parents can independently validate any company claims, and that it is excessive for a school to "curate a unique 10 year record of a child's social-emotional development, monitoring their wellbeing through adolescence." They were concerned a company could influence their child's mental health or make some sort of assessment about it, without parents being able to understand it fully, and that the data collected included highly sensitive information such as 'recently bereaved', with a welfare plan, heavily committed, gifted, and nationality. In February 2020, defenddigitalme was told the Office of the Information Commissioner had:

> *"made enquiries with STEER, and....found that it is likely that STEER and the schools using their services are in contravention of the UK General Data Protection Regulations (UK GDPR) or Data Protection Act 2018 (DPA18). I can confirm that this finding means that I partially uphold the concerns you raised around Article 5(1)(a), Article 5(1)(b), Article 9, and Article 35 of the UK GDPR."*

There was no enforcement action published.

Case study C: safety tech CEO claimed at the SafetyTech launch event in March 2021[8], he could

> *"probably talk for about five days about all the mistakes that we've made along the way. I'll never forget our CFO and I we were called into a meeting with our lawyers …and we told them about how our technology worked and one of the things we were doing is we were intercepting incoming messages without the authority of the person that had sent it in the first place …of course the lawyers said to Ted and I, you realise you could go to prison for doing that… I don't think i've ever broken out in such a sweat in my whole life so we realised that* ***this is a complex landscape*** *and* ***legislation is different depending where you are around the world, and you really need to be alert to that."***

This highlights that different legislation in different places adds complexity whereas being aligned (for example with the GDPR) keeps things simpler for international business.

Other AI tools used in education profile children and claim to be able to identify signs of extremism and terrorism. There is no independent evidence of efficacy of the intended purposes, goals or error rates, or assessment of the chilling effect on the developing child. Such tools can have lifelong lasting consequences for children and need far stronger, not weaker protections than exist today in law. Removing Article 22 protections or accountability for such intrusive, high risk tools, would be wrong.

2.2. Accountability. The Data Protection Officer is the responsible adult in authority, that should be a layer of protection for children in educational settings or other institutions or commercial business, protections from bad product procurement through expert risk assessment, the go-to person for questions for parents avoiding confusion within schools for thousands of organisations in a

[8] SafetyTech launch, March 2021 https://www.youtube.com/watch?v=l4FAeSQ0IZc

consistent way. Abandoning accountability in the DPO, abandoning protections in daisy-chaining the legal basis for data processing without further assessment, abandoning the key GDPR principle of accountability, fundamentally damages the role of data protection, and threatens future adequacy.

2.3. Children and the balancing tests in the legitimate interests basis for lawful processing.
The positive reference to children in the consultation fails to set out any thinking on its implications. Para 60 suggests the balancing test could be maintained for use of children's data, irrespective of whether the data was being processed in connection with an activity on the Legitimate Interests (LI) list, shifting from 'in particular' of the UK GDPR Article 6(1)(f) to only. This shift could mean a hard requirement. How does the consultation propose defining "children's data"? Is the data subject under 18 at the point of collection? Does the personal data collected from a child forever stay "children's data"? Or does data move out of scope for the LI balancing test requirement as the person reaches 18? Will mixed datasets be required to have a balancing test or not? Or just for the children in it? Will it apply to the personal data of deceased children? If not, why not?

This proposal should not proceed. The balancing test should remain as it is today for processing under legitimate interests, for all data, irrespective of the data subject's age.

3. Recommendations in response to selected consultation questions

3.1 Chapter One

1.2 Not to weaken research definitions to give parity to commercial re-use of data (for example, research to turn children's data into a data product) with scientific research purposes, and public interest research.

1.2.10. Not to weaken people's rights to know what is being done with personal data under the Article 14(5)(b) exemption in Article 13. Do you think the government should take away your right to be told that they keep your data and who they give it to and why? This has gone badly for children.[9]

1.3 Not to broaden the legitimate interests definition to give parity to further processing of data for new purposes with public interest research. This Q1.3.2. also appears to suggest that redefining what could be "incompatible" purposes to be acceptable, and it will mean removing purpose limitations of data already collected. Perhaps they want to not be held in breach of the law for deciding your school records can be given away to commercial companies, like the DfE does today? This is a fundamental reshaping of the aims of data protection law and incompatible with Convention 108 and the GDPR.

1.4.4 Agree the legitimate interests balancing test should be maintained for children's data, irrespective of whether the data is being processed for one of the listed activities because the legitimate interests balancing test should be maintained for processing all personal data, regardless of age. (See above **2.3. Age and data)**

1.5.1 The consultation conflates the data protection principle of 'fairness' telling people what you will do with personal data at the point of collection, with a whole lot of other ideas on being fair i.e. not being discriminatory. This is not the intention of the data protection principle of 'fairness'. AI has no special case here.

[9] Betting firms use data from Department for Education Learner Records Service: BBC Papers January 19, 2020 https://www.youtube.com/watch?v=oWrKFZ-S0l0&t=1s

1.5.5 No change is required to existing law unless you are trying to make what is currently unlawful, lawful. That requires more discussion than this consultation permits.

1.5.10-12 No change is required to existing law, which already permits this bias monitoring purposes. The risk is far greater that this change would be used to excessively process sensitive data and protected characteristics. There is also a conflation of "outcome fairness" with equality. (See **The Legal Education Foundation** explainer.[10]

1.5.17 Disagree strongly with the Taskforce on Innovation, Growth and Regulatory Reform's recommendation that Article 22 of UK GDPR should be removed. (See exams 2020).In particular in relation to sensitive personal data, this can be where safeguards are most needed to maintain public trust.

1.5.19 Revealing the purposes and training data behind algorithms, as well as looking at their impacts should be done already today, as part of risk assessment and fair processing. No change is needed in law to permit it.

1.5.5 Disagree that the Government should permit organisations to use personal data more freely, for the purpose of training and testing AI. Any responsible work is already permitted with existing lawful bases for doing so. This could only result in more exploitation of children's personal data to turn into products.

1.6 Data minimisation and anonymisation should be encouraged, but not by rewording the definition of what counts as minimised. Government could start with its own administration of public admin datasets in processes to address excessive data retention by weeding and destruction; and aggregation and anonymisation.

3.2 Chapter Two

2.2.5 Disagree strongly with removing the existing requirements to designate a data protection officer (DPO). Children need a clear go-to person for concerns. This can be a shared service today and does not put disproportionate demands on any business that wants to handle personal data well.

2.2.8 Disagree with proposal to remove the requirement for organisations to undertake a data protection impact assessment. This would encourage the lowest common denominator based on worst practice if organisations were able to adopt different approaches to identify risk. The DPIA already has flexibility how it is done according to organisational needs and its data processes. It would mean the bad actors could hide bad practice more easily and disproportionately disadvantage good actors without common incentives to 'do the right thing'. In fact, the DPIA should include where appropriate a child rights impact assessment[11], to take into account situations of acute power imbalance for example.

2.2.9 Disagree strongly with proposals to remove the requirement for prior consultation with the ICO so it is no longer mandatory and organisations would not face any direct penalties for failing to consult the ICO in advance of carrying out the processing. Disagree with proposals to remove record

---

10 The Legal Education Foundation (2021) https://thelegaleducationfoundation.org/articles/leading-barristers-warn-that-government-proposals-to-reform-uk-data-protection-law-may-lead-to-unintentional-breaches-of-the-equality-act-2010

11 UNICEF Child Rights Impact Assessment https://www.unicef.org.uk/wp-content/uploads/2017/09/Unicef-UK-CRIA-comparative-review_FOR-PUBLICATION.pdf

keeping requirements under Article 30. (See the ICO audit of Department for Education why both need to be kept and perhaps the accountability they are hoping to avoid in future.)[12]

2.2.11 Since most organisations will process some personal data routinely, the requirement to keep a record and know what data you process and why, supports the need to be able to provide this in Articles 13/14, rather than duplication, (as per paras 176/77) you cannot do the latter without having done the first. There is no need for duplication of the same processing information. ROPA is necessary and should not be scrapped.

2.2.18 Does removing the obligation to have a data responsible officer at public authorities intend to remove any duty to be accountable for the authority's data processing? If not, any change here would only be on paper and create confusion, unless something substantial is intended to change. All public authorities that process personal data need to have someone accountable for it. To carry out risk assessment. To be a 'go to' internally and externally for questions. To avoid internal confusion and potential duplication if each department had to perform the tasks rather than have a single designated person. Appointing a data protection officer allows for great flexibility according to the types of processing done and need not be onerous. As is already widely done today in state schools, this role can be provided as a shared service and not even be in-house. No need to change the law.

2.3.4 Disagree there is a case for re-introducing a fee for processing subject access requests (any charges would disproportionately affect children). (See the Met Police Gangs Matrix where it played vital role in transparency for children and young people).[13]

2.4.9 Nothing should weaken today's protections for children from advertising. They need strengthened and all targeted advertising based on profiling children should end. Weakening this would inevitably mean families could be bombarded with even more ads from school for all the companies that engage with children through education and would be detrimental.

3.3 Chapter Three

3.2.4 Today's mechanisms to protect transfers abroad are inadequate because they are not enforced. New enforcement of existing law would be welcome.

3.3.3 The proposals for reverse transfers must not create loopholes to enable data washing of personal data collected unlawfully abroad, to then receive a special exemption status.

3.5 Repetitive use of derogations is currently restricted by the UK GDPR recitals and in European Union regulatory guidance because special cases, are special for a reason. Making them routine removes that recognition and should not be done. This is simply saying we'll routinely weaken the protections placed on this by the EU and therefore is a risk to adequacy.

3.4 Chapter Four

4.3 Nothing should weaken protections for children in their personal data used across public services. Nothing in Data Protection (DP) law prevented data sharing with a lawful basis in the pandemic. DP law has explicit exemptions for such situations and we should not normalise weaker

---

12 ICO audit of Department for Education (published October 7, 2020) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/statement-on-the-outcome-of-the-ico-s-compulsory-audit-of-the-department-for-education/

13 ICO enforcement of the Met Police Gangs Matrix https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-finds-metropolitan-police-service-s-gangs-matrix-breached-data-protection-laws/

governance for convenience in times that fall outside pandemic emergency situation. Not all private bodies are equal and not every processor engaged with a public task should be given the same legal basis as the controller. Nothing today prevents processing by third-party organisations / private organisations that process on behalf of the public sector. Why a change in law is needed is not set out. What is does appear to seek to do is make what is unlawful today, lawful (see case study DeepMind and the 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/).

4.4. Good consistent definitions will matter, but agree with introducing compulsory transparency reporting on the use of algorithms in decision-making for public authorities, government departments and government contractors using public data. In addition clear routes for redress are required to contest automated decision making and request a human-made decision. Plus a ban is needed on automated decision making based on children's biometrics, AI in emotional and affective technology; i.e. not only a register of what is being done, but what should not be done is needed.

4.4.8 We disagree change is needed in the ways proposed. The police already has Part 3 of the UK DPA 2018 exclusively for law enforcement. These changes must not weaken protections for people on biometrics which is a growing area of concern and a growing risk for public trust in the police. It appears to suggest an increase in powers for police when their adoption of biometrics is a free-for-all. The police adoption of emerging technologies[14] means data from immigration and biometrics databases and national police databases are being merged, but without any new protections or independent oversight. Para. 302 is mistaken to seek to pursue an ambition to align more closely the commercial, law enforcement and national security processing frameworks because the public has consistently, over ten years (see list below), reflected a stronger level of trust (albeit not even distributed across the population) between processing for purposes in the public interest by state bodies, and by commercial companies. Watering down "who is the police" is detrimental to public trust and an increasingly blurred line between public and private actors. See also our submission to the Justice and Home Affairs Committee Inquiry New technologies and the application of the law.[15]

3.5 Chapter Five

5.2 Any changes to the governance of the ICO should strengthen their powers and independence, not reduce it. The push towards the ICO having to take on not only the existing duty to 'take account of economic growth' under the Deregulation Act 2015, but yet another new duty ' to have regards to competition' is all about business not data protection for people and respect for our human rights. Greater enforcement is needed today, not even more 'business-friendly' approaches if business is to be seen to be trustworthy and to protect the reputation of good actors by removing the bad.

5.6 That the complainant must attempt to resolve their complaint directly with the relevant data controller before lodging a complaint with the ICO: This is not needed and is already routine practice. Where it fails is where people do not know about the processing that affects them. Do you know who's got your personal confidential school records given away by the Department for Education for commercial re-use since 2012? In addition group representation should be adopted by the UK akin to Article 80(2) of the GDPR.

---

[14] Wired (2018) UK police are now using fingerprint scanners on the streets to identify people in less than a minute The system being used by West Yorkshire Police searches the 12 million fingerprint records kept in the UK's criminal and immigration database https://www.wired.co.uk/article/uk-police-handheld-fingerprint-scanner-database-biometric-security

[15] defenddigitalme (2021) Submission to the JHA Committee enquiry into emerging technologies and policing https://defenddigitalme.org/wp-content/uploads/2021/11/Submission-to-the-Justice-and-Home-Affairs-Committee-Inquiry-New-technologies-and-the-application-of-the-law-%E2%80%94-defend-digital-me.pdf

5.8 The role of the Biometrics Commissioner should not be moved under the ICO and any changes should reflect his own response.[16] Data Protection is about ensuring the free flow of data in a standardised governance framework. The oversight for emerging technology is about more than just data. People also have rights to privacy, as well as data protection. Children have rights embodied in the UNCRC that speak to human dignity, and the ability to fully develop and flourish into adulthood without undue interference. The government seems to have forgotten all this in the consultation.

3.5.1 The proposed changes to the role of the ICO and the Biometrics Commissioner

The role of the Biometrics Commissioner should not be moved under the ICO and any changes should reflect his own response https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response. Data Protection is about ensuring the free flow of data in a standardised governance framework. The oversight for emerging technology is about more than just data. People also have rights to privacy, as well as data protection. Children have rights embodied in the UNCRC that speak to human dignity, and the ability to fully develop and flourish into adulthood without undue interference. The government seems to have forgotten all this in the consultation.

When Ayrshire schools adopted facial recognition in September the public outcry, criticism by Scotland's First Minister in parliament, and in a debate by members of the House of Lords, and widespread criticism in media shows how sensitive the subject is. It is not adequate to have treated as a matter of data processing and protection and should not be within the ICO role of enforcement needed in this same subject. (See https://defenddigitalme.org/2021/11/04/biometrics-in-schools/)[17]

The EU decisions against using facial recognition (biometrics) in schools were acknowledged by the UK Information Commissioner in their June 2021 report, page 22, 'The use of live facial recognition technology in public places.'[18] but has to date not taken enforcement action to end the unnecessary and disproportionate use of biometrics in schools. The Commissioner Fraser Sampson has by contrast objected[19] saying, "if there is a less intrusive way, that should be used."

In his own words, "*Both [The Biometrics Commissioner and the Surveillance Camera Commissioner] functions are about much more than upholding data rights. Proposing their absorption by the ICO is to misunderstand the specific nature and importance of both."*[20]

The ICO, when asked (FOI request, July 2021) about biometrics in schools and consent, processing, complaints and any action taken by the ICO, responded: "*We cannot report on the background of complainants or whether their complaints relate to consent and biometric data. This is because we do not need to routinely report on this type of information for our business purposes.*[21]"

"Business purposes" must not become the benchmark for whether or not the ICO has fulfilled its tasks necessary to its duties.

---

[16] Biometrics Commissioner https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response

17 See biometrics in schools outcry in September 2021 https://defenddigitalme.org/2021/11/04/biometrics-in-schools/

[18] The Information Commissioner (June 2021) 'The use of live facial recognition technology in public places.' https://ico.org.uk/media/2619985/ico-opinion-the-use-of-lfr-in-public-places-20210618.pdf

[19] FT (October 2021) Facial recognition arrives in UK school canteens https://www.ft.com/content/af08fe55-39f3-4894-9b2f-4115732395b9

[20] Biometrics Commissioner (October 2021) Response to the proposals from the DCMS Data A New Direction https://www.gov.uk/government/publications/data-a-new-direction-commissioners-response/press-release

[21] FOI request to the ICO https://www.whatdotheyknow.com/request/biometric_data_in_education#incoming-1846830

3.5.2 Biometrics in schools is a global issue and yet the UK lags behind taking action.

3.5.2.1 Sweden: Facial recognition and consent (2020)

Sweden issued its first fine under GDPR[22] as a result of its case. The key finding was that consent was not a valid legal basis given the imbalance of power between the data subject and the controller.

3.5.2.2 France: Courts and authorities find facial recognition is not necessary and proportionate

A French court canceled[23] a decision in 2020 by the South-Est Region of France (Provence-Alpes-Côte d'Azur – PACA) to undertake a series of tests using facial recognition at the entrance of two High schools considering that this would be illegal.

3.5.2.3 New York State: Facial recognition and other biometrics (2020)

All biometric technology was suspended in New York State schools until July 2022[24] and Florida banned biometrics in schools in 2014 already.

3.5.2.4 Poland: Biometrics: fingerprints (2020)

In 2020 a school in Poland was fined and banned from using biometric fingerprint technology[25] in the school canteen.

3.5.2.5 Scotland: North Ayrshire (October 2021)

North Ayrshire put its rollout on pause, on October 22nd, 2021 a week after it began the rollout.

3.5.2.6 The Ada Lovelace Institute public participation workshops and poll numbers

The Ada Lovelace Institute's 2019 call for a moratorium on biometric technologies like facial recognition was followed by a survey of public attitudes towards facial recognition, published in the report *Beyond Face Value*.[26] The survey showed that not only did the majority of the UK public want greater limitations on the use of facial recognition, but that a deeper understanding of public perspectives was needed to inform what would be considered as socially acceptable for these technologies. They commissioned a nationally representative survey of 4,109 adults, undertaken in partnership with YouGov and revealed the majority are opposed to its use in schools (67%).[27]

According to their public poll of 4,109 adults in 2019, nearly half the public (46%) want the right to opt out of the use of facial recognition technology. This figure is higher for people from minority ethnic groups (56%), for whom the technology is less accurate.

Their recommendations included developing more comprehensive legislation and regulation for biometric technologies, establishing minimum standards and an independent, authoritative body to provide robust oversight. The proposed Commissioners / ICO changes would not address all of this.

---

[22]BBC (2019) Facial recognition: School ID checks lead to GDPR fine. https://www.bbc.co.uk/news/technology-49489154

[23] Christakis, (2020). First Ever Decision of a French Court Applying GDPR to Facial Recognition https://ai-regulation.com/first-decision-ever-of-a-french-court-applying-gdpr-to-facial-recognition/

[24] NY State schools ban https://www.nysenate.gov/legislation/bills/2019/a6787 and EPIC https://epic.org/2020/12/new-york-enacts-law-suspending.html

[25] Poland (2020) Fine for processing students' fingerprints imposed on a school https://edpb.europa.eu/news/national-news/2020/fine-processing-students-fingerprints-imposed-school_en

[26] Ada Lovelace Institute report on public attitudes to facial recognition (2019) https://www.adalovelaceinstitute.org/report/beyond-face-value-public-attitudes-to-facial-recognition-technology/

[27] Ada Lovelace Institute https://www.adalovelaceinstitute.org/report/citizens-biometrics-council/

4. Conclusion

Children's voice should matter in this consultation but is absent. Plans to restructure data protection law, must that prioritise human flourishing in a vision of society that means living with the outcomes of machine learning and increasingly automated decision making in the public and private sectors.

Many digital products on the UK market, adopted widely in education, some of them even promoted by the DCMS, are highly intrusive by design. They require accordingly high levels of risk assessment, a competent data protection officer to assess due diligence and compliance over a product life cycle, and consistent standards of quality and application.

As the Safety Tech CEO in our case study C said, this is a complex (AI) landscape, around the world and legislation that differs makes it harder for companies that need to be alert to that.

These proposals are short sighted. Divergence in the data protection laws between Member States of the EU was what led to the GDPR because it was bad for business, as we set out in our report *The Words We Use in Data Policy: Putting People Back in the Picture* (September 2021).[28] While we may have left the EU it would be folly to think that creating a duplicate system will serve any useful purpose for business. It will damage the industry that it targets as its main beneficiary, Artificial Intelligence, through loss of public confidence and trust in what will be viewed as a second-class system. In all likelihood in the short term, while companies may cut costs by cutting corners on good practice, it will not serve their interests through loss of reputational risk and harm from other bad actors in the same sector. Nor will changes serve their customers or users, including children, to whom they have obligations. It might well serve as a platform to benefit other countries, as the majority of VC comes from China and the US that could buy out successful AI start ups. The impact assessment included no consideration of this or of potential long term risks to UK users' data security or economic sustainability. (Case study: story of edTech company Edmodo's data breach, including 2 million UK pupils and teachers, followed by its 2018 buyout[29] by Chinese-owned NetDragon.)

Our current UK data protection regime is *already* less strong than the GDPR intended. We did not make the derogations in 2018 that improved rights or added protections for people such as was available for group representation under Article 80(2), and instead made derogations that weakened rights, such as the controversial and contested immigration exemption.[30]

These proposals go against all of the concerns people have today about having too little control of the stories of our lives. Discrimination. Decisions made about us without us. How companies and organisations use our personal data for too much marketing, excessive policing, unfair algorithms. The UK must *not* reduce the protections we all need every day, going about our daily business.

November 19, 2021

---

[28] defenddigitalme (2021) p22 The Words We Use in Data Policy: Putting People Back in the Picture https://defenddigitalme.org/research/words-data-policy/ A look at national data policy with young people's views on how data is talked about and used

[29] EdSurge 92018) China's NetDragon to Acquire Edmodo for $137.5 Million https://www.edsurge.com/news/2018-04-09-china-s-netdragon-to-acquire-edmodo-for-137-5-million

30 Mission de Reya (2021) Data Protection Act immigration exemption is unlawful, rules Court of Appeal https://www.mishcon.com/news/data-protection-act-immigration-exemption-is-unlawful-rules-court-of-appeal

Annex 1

Public engagement demands better protections to uphold public trust

The 2010 study[31] with young people conducted by The Royal Academy of Engineering supported by three Research Councils and Wellcome, discussed attitudes towards privacy and the use of medical records and concluded: *These questions and concerns "**must be addressed by policy makers, regulators,** developers and engineers before progressing with the design, and implementation of record keeping systems and **the linking of any databases**."*

In 2014, the House of Commons Science and Technology Committee in their report, Responsible Use of Data[32], said "***the Government has a clear responsibility to explain to the public how personal data is being used**."*

The same Committee's Big Data Dilemma **2015-16** report (p9)[33] concluded "*data (some **collected many years before and no longer with a clear consent trail) […] is unsatisfactory left unaddressed by Government and without a clear public-policy position**.*"

Or see from 2014, The Royal Statistical Society and Ipsos Mori work on the data trust deficit with lessons for policymakers.[34]

2018 We commissioned Survation to poll 1,004 parents of children aged 5-18 in state education in England in February 2018. Over half said they have lost track of their child's digital footprint in education.[35]

2019 DotEveryone's work on Public Attitudes[36] shows people want to be in control of data.

2020 The ICO Annual Track survey results[37] show declining public trust on previous years.

There is also a growing body of literature to demonstrate what the **implications are being a 'data driven' society**, for the datafied child, as described by Deborah Lupton and Ben Williamson in their own research in 2017.[38]

The UK government and policy makers, are simply ignoring the inconvenient truth that legislation and governance frameworks such as the UN General Comment no 25 on Children in the Digital Environment, that exist today, demand people know what is done with data about them, and it must be applied to address children's right to be heard and to enable them to offer them strong privacy as well as data protection rights, and ways to exercise them.[39]

---

[31] https://www.raeng.org.uk/publications/reports/privacy-and-prejudice-views

[32] https://publications.parliament.uk/pa/cm201415/cmselect/cmsctech/245/245.pdf

[33] https://publications.parliament.uk/pa/cm201516/cmselect/cmsctech/468/468.pdf

[34] https://www.ipsos.com/ipsos-mori/en-uk/new-research-finds-data-trust-deficit-lessons-policymakers

[35] Survation (2018) https://www.survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/

[36] https://doteveryone.org.uk/report/peoplepowertech2020/

[37] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/08/annual-survey-gives-insight-into-peoples-information-rights-views/

[38] https://www.semanticscholar.org/paper/The-datafied-child%3A-The-dataveillance-of-children-Lupton-Williamson/28863b10f4674bec927e1f1486525cffdef2b3c3

[39] https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2fPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2f5F0vEG%2bcAAx34gC78FwvnmZXGFUl9nJBDpKR1dfKekJxW2w9nNryRsgArkTJgKelqeZwK9WXzMkZRZd37nLN1bFc2t