## Defend Digital Me Briefing: the Data Protection and Digital Information Bill (No. 2)

This Bill fundamentally refocuses the essential nature of the UK data protection regime. It moves away from today's rights-based regulation, which prioritises seven key data protection principles framed by accountability as an overarching premise, towards a business-centric one, in which accountability is downgraded as part of its deregulation aims. This leaves people, including children, less protected.

> ***"Successful sustainable innovation is dependent on building and maintaining public trust."***
>
> The Centre for Data Ethics and Innovation Review into bias in algorithmic decision-making (2020).[1]

Every time the Bill is described as "reducing the compliance burden on businesses" substitute "stripping today's data protection safeguards from children." Now is the wrong time for downgrading data rules if the UK is serious about becoming a "tech super power".[2] Regulation is going in the wrong direction by reducing safeguards against data misuse while the sensitivity of our personal data collected and the automated methods for its use and abuse at speed and scale go up.

> *"Genesis Market had **80 million sets of credentials and digital fingerprints up for sale, with the NCA calling it "an enormous enabler of fraud".** Genesis Market sold login details, IP addresses and other data that made up victims' "digital fingerprints"."*
>
> (BBC News, April 5, 2023)

The paradox could not be more stark if one remembers the DCMS motto of the Online Safety Bill on the one hand, *making the UK the world's 'safest' place to go online*, rendered pointless if on the other hand, this Bill increases their digital risk with lifetime impact in an increasingly digitised world.

> *"inappropriate data processing practices by e-learning platforms, opaque automated decision-making and misuse of learning analytics, risk undermining data protection and privacy rights. In the case of children and youth, this can have **significant and long-term social, economic and professional consequences**, and fail to account for their evolving capacities."*
>
> (Resolution from the 2018 International Conference of Data Protection and Privacy Commissioners.)[3]

**Note: Data Protection law does not stand alone.** It does not by itself overrule the fundamental right to privacy enshrined in human rights law and it sits alongside communications law, the common law of confidentiality, and the administrative law that governs the actions of public authorities. According to well-established rules a public authority must possess the power to carry out what it intends to do. If not, its action is "ultra vires", i.e. beyond its lawful powers. It is also necessary that the power be exercised for the purpose for which it was created or be "reasonably incidental" to the defined purpose. Data protection law that governs data processing by public authorities lays over the top of administrative law to manage but not dictate that data processing beyond what is permitted in the primary legislation at the point of collection under the powers of the public authority.

---

[1] The 2020 CDEI Review into bias in algorithmic decision-making (p6)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/957259/Review_into_bias_in_algorithmic_decision-making.pdf

[2] DSIT (March 2023) International Technology Strategy to guide the UK to becoming a tech superpower by 2030.
https://www.gov.uk/government/news/plans-to-make-uk-an-international-technology-superpower-launched

[3] https://edps.europa.eu/sites/default/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf

Data regulation is necessary to protect people from being dehumanised, turned into data,[4] and treated simply as numbers. No government can revoke our fundamental human right to privacy, as recognised in international instruments; even if a government might like to exchange that right for the promotion of economic aims, or to misuse the data rights of the many to hunt out the few in the current Hostile Environment. But if we cannot *exercise* our rights and the law is not *enforced*, they exist only on paper, not realised in practice.

The overhaul of the data protection regime that would be brought about by the DPDI Bill (No.2) is however neither necessary nor desirable, given that so much capacity has already been recently invested in the Data Protection Act 2018. The Bill as currently drafted will introduce retrogressive and undesirable changes, including fundamental changes to the lawful basis for processing data:

- Changes to lawful basis (legitimate interests) (clause 5)
- Changes to purpose limitation[5] (clause 6)
- And further changes aimed at reducing transparency, accountability and rights-protection.

The seriousness of the proposed changes above to the current Article 5 of the GDPR must not be underestimated. These changes put together systemically undermine the principles which lie at the heart of data protection law. The current law sets out seven key principles[6]:

  - Lawfulness, fairness and transparency
  - Purpose limitation
  - Data minimisation
  - Accuracy
  - Storage limitation
  - Integrity and confidentiality (security)
  - Accountability

These principles are set out right at the start of the legislation, and inform everything that follows. They embody the spirit of the general data protection rights based regime. As such, there are narrow and limited exceptions to these general principles. But the new Bill changes this, seeking to normalise these exceptions and heralding a broad shift away from the essential nature of data protection law and its core underpinning.

Compliance with the spirit of these key principles is the fundamental building block for good data protection practice and changes are far more sweeping than might be understood by reading only individual changes to certain provisions. It is also key to compliance with the detailed provisions of the UK GDPR and therefore to the perception of the overall adequacy of the UK regime as a whole.

“Accountability is more than simple compliance with the rules - it implies a culture change,” said the much missed EDPS Giovanni Buttarelli in 2016. The new Bill will be a backwards step to undo that,

[4] See the Defend Digital Me report (2021) The Words We Use in Data Policy: Putting People Back in the Picture https://defenddigitalme.org/research/words-data-policy/
[5] Working Party 29 Opinion 03/2013 on purpose limitation https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf
[6] The universal seven key data protection principles (ICO) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

"quantum shift in emphasis on who is responsible for ensuring that our right to data protection is fully respected". Instead of a Data Protection Officer, the Bill introduces a second-rate version, a senior accountable owner. Instead of a consistent method of identifying and managing risk, through Data Protection Impact Assessment, scrapping it will create confusion of how it should be done. Anything that amends the fundamental principle of the GDPR, accountability, threatens adequacy.

Failure to comply with the principles is recognised as increasing the seriousness of any infringements of today's law. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. However, fines are always discretional. The concept that breaching the principles is most serious, is not.

If new legislation is unavoidable, it should be an opportunity to make some valuable additions to the existing data protection regime, such as introducing protections for the personal data of deceased children. It must not undermine the core principles and essence of the current law.

If this is all about simplification of the regime for business, why is the UK choosing to maintain two parallel frameworks, the UK Data Protection Bill and the UK GDPR, when one not both would be easier to continue to work in tandem with the EU GDPR and the Council of Europe Convention 108?

## 12 ways the Bill will reduce transparency, accountability, and safeguards for children's rights

**The Bill as currently drafted would:**

1. Create differences between the UK definition of legitimate interests and the GDPR as a legal basis for lawful data processing
    a. Remove the explicit mention of children's fundamental rights and freedoms from the current definition for the newly defined list of legitimate interests
    b. Remove the explicit current mention of protection of rights and freedoms.
    c. Remove the safeguards of a balancing test on which necessity and proportionality tests rest, pulling the rug out from under current basic data protection principles.
2. Change the purpose limitation principle in ways that will dramatically reduce the trust in what was agreed about how your data could be used by others at the time of collection.
3. Research definitions are reframed (Part 1, clause 2 (4)(a)) to permit any and all commercial product development ("technological development") and together with customer data about individuals becoming state property as a minable resource (Part 3) this will mean children and adults becoming non-stop data mining cows for companies to profit from without our ability to object if defined as commercial 'research'.
4. Allow for intra-group transmission of personal data for 'internal administrative purposes'. (Part 1, clause 5(4)). Existing law already permits what is necessary, and this vaguely defined change would surely enable companies with thousands of affiliated companies to profit from children's data without external visibility once distributed at scale 'inside' the network.
5. Reduce accountability by making it more difficult for people, including children, to access copies of their own data. (Part 1, clause 7)

6. Reduce public trust in data handling through transparency by making it more difficult for people, including children, to know when their data is being processed for new purposes or has been passed on to third parties. (Part 1, clause 9)
7. Weaken protections against harm from solely automated decision-making. (Part 1, clause 11)
8. Remove a vital safeguard against unlawful and harmful data processing, by reducing the requirement to have a Data Protection Impact Assessment (DPIA). (Part 1, clause 17).
9. Reduce enforcement of rights and increase risk of lack of deterrent effect by weakening ICO as an independent regulator and oversight body. (Part 1, clause 27 and 28, and Part 5)
10. Pave the way for powers to permit unlimited 24/7 365 days a year, for registered political campaign groups of any kind, to send unsolicited digital, email, and print direct marketing to teenagers (age 14+) across all of the UK (Part 4, Clause 83).
11. Reduce the accountability of companies to know what data they hold, how they process it and show where it goes and why in reduced record keeping requirements (ROPA).
12. Part 5, Clause 104 abolishes The Office of Commissioner for the Retention and Use of Biometric Material. Current oversight of biometrics in schools does not fall under the oversight of the Biometrics Commissioner who has nonetheless been a passionate supporter of change – while the ICO has supported the status quo with better process around use, not better protection for children from use. Why has the government refused this oversight?[7]

[7] https://hansard.parliament.uk/Lords/2022-12-12/debates/225551A8-EA02-4D2B-B2F2-6692BD174935/Children'SPrivateInformationDataProtectionLaw#contribution-B395CADB-CFE3-4137-92D6-5D74D07B074E

| Part and Clause No. | Subject | Specific topic | Current position | Proposed new position | Threats to data adequacy |
|---|---|---|---|---|---|
| Part 1, clause 6, and Schedule 2 | Purpose limitation | Further processing of data, in ways that are incompatible with the original purpose for which it was collected. | One of the key principles contained in Article 5 of the EU GDPR is purpose limitation. Before data processing starts, there must be a specific, well-defined purpose for it. Generally speaking, there can be no further processing of data in a way that is incompatible with the original purpose. As things currently stand, this essential principle is reflected in the UK GDPR but will be undermined despite no proven need. | The new Bill seriously undermines purpose limitation by creating a new set of conditions under which the processing of personal data for a new purpose is to be treated as processing in a manner compatible with the original purpose.<br><br>The list of new conditions is long and the language used is vague which is open for future changes without oversight.<br><br>Further, the Secretary of State is given new, and its Henry VIII powers to amend Annex 2 by regulation. | These changes seriously undermine one of the fundamental seven principles of data protection, and risk rendering the principle of purpose limitation virtually obsolete. |
| Part 1, clause 5, and Schedule 1 | Legitimate interests | Permitting data processing for a much wider range of 'recognized legitimate | Currently, data processing is permitted in a narrow range of clearly defined | Clause 5 would introduce a new legal basis for data processing (Article 6(1)(ea), namely, where “processing is | To a large extent, Article 6(1)(ea) replicates the wording of Article 6(1)(f) but it is notable that, here, |

| | | | | | |
|---|---|---|---|---|---|
| | | interests', without any explicit need to consider the fundamental rights and freedoms of children, consider the fundamental rights and freedoms of people more generally, or conduct a balancing test. | circumstances one of which is where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child." (Article 6(1)(f) of the UK GDPR). | necessary for the purposes of a recognised legitimate interest".<br><br>The set of 'recognised legitimate interests' for the purposes of Article 6(1)(ea) would be set out in a new Annex 1 and would include, for example, 'protecting national security', 'safeguarding public security' and 'investigation and prevention of crime'. | the 'balancing test' featured in Article 6(1)(f) is stripped out (though the "necessity" test is retained) and there is no mention whatsoever of the rights and freedoms of data subjects or of children. In this sense, Article 6(1)(ea) is a chopped-off version of the Article 6(1)(f).<br><br>It is also highly concerning that the Secretary of State would have open-ended Henry VIII powers to amend Annex 1 at will (under clause 5(6)) and, instead of an obligation to not override children's rights and freedoms, she must now only have a lesser "regard to" them (clause 5(7)). |
| | | Balancing test no longer required in certain broad topics | Today an "interest" must be sufficiently clearly articulated to allow the balancing test to be carried out | | Effects on assessment of necessity and proportionality |

| | | | | | |
|---|---|---|---|---|---|
| | | | against the interests and fundamental rights of the data subject. This is not optional. | | |
| | | Legal basis added in Annexe 1 | | | The effect on the fundamental 7 principles of data protection |
| | | Legal basis added in Annexe 1 | In the context of new Article 7(f), the controller can process the data, subject to conditions and safeguards, as long as the data subject has not objected. In this sense, the right to object can rather be considered as a specific form of opt-out. | No Right to Object will be offered or honoured. | |
| Part 4, Clause 83 | Legitimate interests for political purposes | Direct marketing for "the purposes of democratic engagement (from age 14+) | This is currently banned and should remain so. | The change would permit unlimited unsolicited political and other registered campaign groups direct marketing at teens 14+ across the UK. | Threat to the fundamental 7 principles of data protection and purpose incompatibility |
| Part 1, Clause 5(4) | Intra-group transmission of personal data for internal administrative purposes | This is already possible today where there is a legitimate necessity, but there must be informed processing. | This will mean invisible "daisy chains" sometimes with thousands of 'intra group' businesses that could seek to justify onward use within large | Can a child be expected to know that a school app to support them in choosing library books is in fact part of a multinational chain, funded by private equity based in the | This change is unnecessary as what is already necessary and proportionate is permitted in existing law. The shift |

| | | | | | |
|---|---|---|---|---|---|
| | | This change would remove that obligation. | corporations that becomes impossible to understand. | Cayman Islands? Where are the limits of what is reasonable “intra group” transmission? | away from rights is away from GDPR alignment. |
| Part 1, Clause 2 | Meaning of research and statistical purposes | The Bill will fundamentally undermine the professional status of research if it goes ahead with proposed changes. The definition of ‘research’ will become more amateur, more commercial, and more exploitative. The new definition will expand the permitted uses of data that attract the data processing research exemptions granted today, including for example offering either the need for informed processing, or to offer people a Right to Object. | Education data can include highly sensitive data from children that they do not know is collected and do not get told on reaching adulthood, about adoption, child protection, sexual orientation and religion in student records – there are currently no restrictions or protections for people finding this data used in unexpected ways in either “the public interest” or for commercial re-use. Why make this even more explicitly “acceptable” when instead, people want asked especially with a right to object to commercial re-use? | The result of activity that can, “reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity” will see our children routinely become lab rats for trialling new products, and their personal data used to create for-profit products, all without consent or even being properly informed and without ethical oversight, as has already been the case to-date without adequate enforcement across the sector when the aim is “to maximise the value of this rich dataset”.[8] | Any divergence from what is considered historic, scientific or public interest research purposes will threaten adequacy. |

[8] Children’s Private Information: Data Protection Law Volume 826: debated on Monday 12 December 2022 https://hansard.parliament.uk/Lords/2022-12-12/debates/225551A8-EA02-4D2B-B2F2-6692BD174935/Children’SPrivateInformationDataProtectionLaw#contribution-06D4244D-EE40-4831-A66E-A409E9BDE3B2

| | | | | | |
|---|---|---|---|---|---|
| Part 3, clauses 61-77 | Customer data | "Business data" | | This "includes a power to require suppliers and others to provide customers with customer data and business data." This is a vast power to require data about customers' and your behaviours, purchases, services and anything the Secretary of State demands for the state under the Henry VIII powers. | According to the government's own impact analysis[9], this could give rise to unlawful interferences with ECHR Article 8 rights and Article 1 of Protocol 1 and, in relation to enforcement of the regulations, Article 6. This also seems to conflict with the foreseeable purpose limitation at the point of collection, as well as fundamental principles of data minimisation and necessity. |
| Part 1, clauses 27-33, and Part 5 | Information Commissioner's Office | Restructuring the regulatory authority and reducing its independence. | | Clause 27 introduces a statutory framework of objectives for the Information Commission. This list of considerations is clearly weighted in favour of business interests and the interests of | This weakening of the regulator is extremely concerning as it would create more space for bad actors to act with impunity, using and abusing the personal data |

[9]https://web.archive.org/web/20230404085753/https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum

| | | | | | |
|---|---|---|---|---|---|
| | | | | government, and includes nothing about the protection of the rights of citizens generally or children specifically.<br><br>Clause 28 would give the Secretary of State new powers to influence Information Commissioners in the exercise of their functions. | of people in general and children in particular. In a context where data abuses are already going unchecked, this is clearly a step in the wrong direction. |
| Part 1, clause 15 | Record keeping requirements (ROPA) | | The ROPA is also the place where today the controller or processor shall document the assessment as well as the safeguards referred to in the second subparagraph of paragraph 1 of Article 49 of the GDPR. | By making this optional in the absence of any future adequacy decision there will be no place to record the appropriate safeguards required. | Threat to accountability principle, the key overarching framework of the entire GDPR data protection regime |
| Part 1, clause 17 | Data Protection Impact Assessments | Replacing the requirement to undertake a DPIA with weakened 'assessments of high risk processing'. | DPIAs, currently required under Article 35 of the UK GDPR, are a vital safeguard, helping to protect individuals against unlawful or | Under clause 17 of the Bill, the minimum requirements of an assessment would be lowered. The data controller would no longer be required to give a systematic description of the | This would make for a much more light-touch form of assessment and would put children at risk of more frequent and DPIAs, if properly carried out, can offer some |

| | | | | | |
|---|---|---|---|---|---|
| | | | discriminatory data processing systems. Importantly, they can help organisations to identify risks and mitigate them before a system is deployed. | processing operations and purposes. Instead, they would simply be required to summarise the purposes of the processing. The data controller would no longer be required to conduct a proportionality assessment, asking themselves whether the objective of the measure is sufficiently important to justify the limitation of a protected right; whether the measure is rationally connected to the objective; whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective; and whether, on balance, the measure is justified. Instead, they would only be required to consider whether the processing is necessary for the stated purposes. more serious privacy invasions. | protection and help to ensure that data controllers do not deploy rights-violating data systems; but if the requirement to undertake a DPIA is watered down, we are likely to see an increase in rights violations. |

| | | | | | |
|---|---|---|---|---|---|
| Part 1, clause 7 | Subject Access Requests | Lowering the threshold for refusing a subject access request, thereby making it more difficult for people to access their own data | Currently, individuals, including children, have the rights of access under Article 15 of the UK GDPR to find out whether and how their personal data is being processed and to obtain a copy of that personal data. Under section 53 of the DPA 2018 and Article 12 of the UK GDPR, a data controller is allowed to refuse a request only if it is 'manifestly excessive or unfounded'. | New Clause 7 of the Bill would lower this threshold, allowing a data controller to refuse a request if they consider it is 'vexatious or excessive'. There would also be a new list of considerations for deciding if a request meets this threshold, and the vague language used to frame these considerations creates a risk that the provision will be unfairly relied upon to refuse legitimate requests. | These changes will make it harder for people to get copies of their own personal data – which may include data about their movements and location, their biometric information, or treatment by a care provider – and to understand how it is being used. Not only would this undermine people's dignity, it would also reduce accountability: if a person does not know how their data is being used, they cannot challenge unlawful or unfair practices. |
| Part 1, clause 9 | Right to know | Diminishing a data subject's right to know how personal data is being processed in cases where that data has been passed on to a third party. | Today's Articles 13 and 14 of the UK GDPR are designed (a) to ensure that people have sufficient information about who is processing their personal data and why and (b) to ensure that people are aware of their data rights. Article | Under the new Bill, clause 9 would expand this list of exemptions to include situations where providing information would involve 'disproportionate effort' and 'is likely to seriously impair the achievement of the objectives of the processing'. | This clause is open to very broad interpretation by a data controller and would severely restrict the right to know. It would make it much more likely that a child's personal data will be passed on to a third party and processed |

| | | | | | |
|---|---|---|---|---|---|
| | | | 14 of the UK GDPR, in particular, provides data subjects with rights to know how their personal data is being processed in cases where that data has been passed on to a third party. Article 14(5) sets out some exemptions to the right to know, i.e. situations where information need not be provided. | | without the child's knowledge. |
| Part 1, clause 11 | Automated decision making | Weakening safeguards against solely automated decision-making | Currently, people have a right under Article 22 not to be subjected to solely automated decision-making that would have legal or similarly significant effects. Article 22 is an important safeguard. Especially while the 'AI revolution' is still in its infancy, having a 'human in the loop' helps to ensure fair and | Clause 11 would remove this right, except in respect of decisions involving 'special categories' of personal data. | Article 22 already requires a decision to have legal or similarly significant effects before human involvement in the decision-making process is required. It is unnecessary and potentially harmful to add the additional requirement that the decision must also involve special categories of personal data. This change is likely to lead to an increase in risky and potentially rights-violating |

| | | | | | |
|---|---|---|---|---|---|
| | | | accountable decision-making. | | uses of new AI technologies. |
| Part 5, Clause 104 | The Office of Commissioner for the Retention and Use of Biometric Material is abolished | The current oversight of biometrics in schools does not fall under the oversight of the Biometrics Commissioner who has nonetheless been a passionate supporter of change – while the ICO has supported the status quo with better process around use, not better protection from use. | | The new obligation on the ICO to recognise and account for how its regulatory activity could impact on competition and innovation and economic growth may be in conflict with its statutory duty to regulate and protect humans' rights, not business interests. | Other countries have banned or found unlawful the use of facial recognition in schools – Sweden, France, Bulgaria and Poland took action on fingerprints. The ICO only suggested it was "likely" unlawful in 2022, and created a 'how to guide' and case study instead. |

## Making it more difficult for people, including children, to know when their data is being processed for new purposes or has been passed on to third parties.

Today's Articles 13 and 14 of the UK GDPR are designed (a) to ensure that people have sufficient information about who is processing their personal data and why and (b) to ensure that people are aware of their data rights, including the right of access under Article 15 (we discuss Article 15 in more detail below). Article 14 of the UK GDPR, in particular, provides data subjects with rights to know how their personal data is being processed in cases where that data has been passed on to a third party. Article 14(5) sets out some exemptions to the right to know, i.e. situations where information need not be provided.

Under the new Bill, clause 9 would expand this list of exemptions to include situations where providing information would involve 'disproportionate effort' and 'is likely to seriously impair the achievement of the objectives of the processing'. This clause is open to very broad interpretation by a data controller and would severely restrict the right to know. It would make it much more likely that a child's personal data will be passed on to a third party and processed without the child's knowledge.

## Making it more difficult for people, including children, to access data about themselves

Currently, individuals, including children, have the rights of access under Article 15 of the UK GDPR to find out whether and how their personal data is being processed and to obtain a copy of that personal data. Under section 53 of the DPA 2018 and Article 12 of the UK GDPR, a data controller is allowed to refuse a request only if it is 'manifestly excessive or unfounded'.

New Clause 7 of the Bill would lower this threshold, allowing a data controller to refuse a request if they consider it is 'vexatious or excessive'. There would also be a new list of considerations for deciding if a request meets this threshold, and the vague language used to frame these considerations creates a risk that the provision will be unfairly relied upon to refuse legitimate requests. These changes will make it harder for people to get copies of their own personal data – which may include data about their movements and location, their biometric information, or treatment by a care provider – and to understand how it is being used. Not only would this undermine people's dignity, it would also reduce accountability: if a person does not know how their data is being used, they cannot challenge unlawful or unfair practices.

## Case study: named records show sensitive data on abuse and children in care

**The Department for Education** knows the individual named details, with highly detailed sensitive categories of abuse, including home address of 2,538,656 distinct Children in Need / Looked After Child (LAC) records (going back to 2006), who are able to be matched at the DfE to a home address information via other sources included in the National Pupil Database. [source DfE FOI 28, September 2022] The NPD is a database of over 23 million individual named records.

In the entirety of the 23 million+ database, as at 8 September 2022, there are [only] **70** individuals flagged for shielding in total (i.e. extra safeguards.) This includes both current and former pupils. Are these politicians children, celebrities, children under police protection schemes or CIN / LAC children? Making a Subject Access Request is very challenging and returns a lot of data in codes that need looking up and comparison with tables available on the Internet, unusable for child.

### Case study: equality monitoring data identifies students' sexual orientation and religion

Higher Education applicants who have submitted their sexual orientation and religious affiliation as part of equality monitoring since 2012, have not had their data only kept as statistics, but it has been added into their named national school pupil records. The declared sexual orientation of 3,213,683 students is now kept on their identifying record in the National Pupil Database. [Source DfE][10]

**The religious affiliation of 3,572,489 people** is held on their named records. Why is this data collected, retained and above all **"linked"** with individually named, *highly* detailed lifelong school records, at all? Why is it not only collected and kept as stand-alone statistics to achieve the same aims? Our research in 2018 showed 69% of parents asked did not know the database existed.

There is an opportunity in the Data Protection and Digital Information Bill before Parliament in summer 2023 to right this wrong. And for example, the Higher Education and Research Act 2017 might be amended to reference only statistical data in a number of places where it demands data sharing on "equality of opportunity" in connection with access to and participation in higher education provided by English higher education providers.

### Case study: are you or your family in the named National Pupil Database?

**Are you or your family state educated or have you taken state exams since 2012? Millions of former and current school pupils and students do not know that they have a national pupil record controlled by the Department of Education and re-used for commercial purposes, as well as journalists, think tanks, charities, the police, Home Office for immigration enforcement, and public interest researchers.**

In November 2019, the ICO wrote[11] to our Director with initial remarks ahead of an ICO audit it carried out in 2020.

*"Our view is that the DfE is failing to comply fully with its data protection obligations. Primarily in the areas of transparency and accountability, where there are far reaching issues, impacting a huge number of individuals in a variety of ways,"* and that the DfE, *"was failing to fully comply with the GDPR because many parents and pupils are "either entirely unaware of the school census and the inclusion of that information in the national pupil database or are not aware of the nuances within the data collection, such as which data is compulsory and which is optional".*

[10] https://defenddigitalme.org/2023/04/02/does-your-national-school-record-reveal-your-sexual-orientation/
[11] Letter from the ICO to Jen Persson (November 2019)
https://defenddigitalme.org/wp-content/uploads/2023/04/ABC-ICO-decision_Redacted.pdf

October 2020**:** the ICO released a short executive summary from the DfE compulsory audit[12] in response to our case made in June 2019 and complaints by Liberty. Among its 139 findings, it identified that, "The DfE are not providing sufficient privacy information to data subjects as required by Articles 12, 13 and 14 of the GDPR," and that "The DfE are reliant on third parties to provide privacy information on their behalf however, this often results in insufficient information being provided and in some cases none at all which means that the DfE are not fulfilling the first principle of the GDPR, outlined in Article 5(l)(a), that data shall be processed lawfully, fairly and in a transparent manner."

In April 2023 we have seen no progress on communications to children and families of pupils in school today, nor the millions of people who are in the database but have already left state education settings.

## Risk assessment: the burden of risk assessment is pushed from data controller to the person, the "data subject" even where that person is a child

DPIAs, currently required under Article 35 of the UK GDPR, are a vital safeguard, helping to protect individuals against unlawful or discriminatory data processing systems. Importantly, they can help organisations to identify risks and mitigate them before a system is deployed.

Under clause 17 of the Bill, the minimum requirements of an assessment would be lowered.

The data controller would no longer be required to give a systematic description of the processing operations and purposes. Instead, they would simply be required to summarise the purposes of the processing. The data controller would no longer be required to conduct a proportionality assessment, asking themselves whether the objective of the measure is sufficiently important to justify the limitation of a protected right; whether the measure is rationally connected to the objective; whether a less intrusive measure could have been used without unacceptably compromising the achievement of the objective; and whether, on balance, the measure is justified. Instead, they would only be required to consider whether the processing is necessary for the stated purposes. This would make for a much more light-touch form of assessment and would put children at risk of more frequent and more serious privacy invasions.

Under the existing data protection regime, children are subjected to rights-violating data collection and processing by the UK state.

For example, the National Pupil Database (NPD) contains named and sensitive personal data relating to more than 20 million individuals. It includes information such as whether a child is pregnant, has social, emotional or mental health needs, or is attending a young offender institute. Yet parents and children are usually unaware that such data is being collected and held; data is retained indefinitely; and of its re-uses. We have calculated that between March 2012 to June 2021 there have been over 2,000 releases containing sensitive, personal or confidential data at pupil level.[13]

[12] ICO summary of the DfE Audit (March 2020)
https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2618384/department-for-education-audit-executive-summary-v1_0.pdf
[13] More information about the NPD is available on Defend Digital Me's website
https://defenddigitalme.org/my-school-records/national-pupil-data/

DPIAs, if properly carried out, can offer some protection and help to ensure that data controllers do not deploy rights-violating data systems; but if the requirement to undertake a DPIA is watered down, we are likely to see an increase in rights violations.

### Case study: Department for Education 2020

**In 2020, the Information Commissioner's Office found that the Department of Education does not always carry out a DPIA when it ought to, or else not at an early enough stage.[14] If anything, the requirement to undertake a DPIA should be strengthened, not weakened.**

In 2022, the Department for Education told schools at the launch of a new national data collection that they had consulted with the ICO but it was untrue. The communications and documents that the Information Commissioner's Office ("ICO") subsequently released in response to our Freedom of Information Request[15] in July, show that at that time, and when the data collection started, the DfE had not in fact worked with the ICO on its DPIA, contrary to the DfE's initial communication to schools (which the ICO subsequently asked it to edit /retract). Nor had the DfE had a Data Protection Impact Assessment ("DPIA") signed off before processing began, as required by law. The ICO asked the Department to pause the high risk data collection, and carry out the risk assessment. The Department declined to pause.[16]

This was a full two years after the ICO audit that found exactly this failure to carry out necessary risk assessment at the correct time in the process of new data processing among 139 failings. One may ask what lessons were learned, and how would anyone know since it remains unpublished in full?[17]

### Automated decision making: weaker protections when the computer says no

> *"artificial intelligence powered systems whose decisions cannot be explained raise fundamental questions of accountability not only for privacy and data protection law but also liability in the event of errors and harm."*

Artificial intelligence (AI) is the number one technology priority in the UK's International Tech Strategy and all five priorities are underpinned by number 6, Data. Automated decision-making systems, powered by personal data, are increasingly used by public bodies in a range of high-impact contexts, including education. For example, some schools in the UK now use emotion recognition systems, which assess the mood of the students in the classroom in real-time and recommend interventions to the teacher.[18] Automated decision-making at scale is a relatively new phenomenon

[14] The 2020 Executive Summary of ICO's audit of the Department for Education https://defenddigitalme.org/wp-content/uploads/2021/10/department-for-education-audit-executive-summary-marked-up-by-DDM-Jan-2021.pdf
[15] https://www.whatdotheyknow.com/request/prior_consultation_article_364#incoming-2086686
[16] DfE failure to carry out DPIA on high risk new daily attendance data collection (2022) trialhttps://defenddigitalme.org/2022/09/16/news-challenging-the-department-for-education-on-excessive-pupil-data-collection/
[17] Children's Private Information: Data Protection Law Volume 826: debated on Monday 12 December 2022 https://hansard.parliament.uk/Lords/2022-12-12/debates/225551A8-EA02-4D2B-B2F2-6692BD174935/Children'SPrivateInformationDataProtectionLaw#contribution-ABA3A1C9-FF6A-4F35-B9DC-F9894E5E4575
[18] See Stephanie Hare, 'Face up to it – this surveillance of kids in school is creepy' (2022, The Guardian, https://www.theguardian.com/commentisfree/2022/may/08/face-up-to-it-this-surveillance-of-kids-in-schools-is-creepy, with reference to Defend Digital Me's report, 'The State of Biometrics 2022', available at https://defenddigitalme.org/research/state-biometrics-2022/.

and, as such, presents a high risk of error and unfairness. The A-levels algorithm, scrapped due to the unfairness it would have produced, is just one example.[19]

> *"Emphasising the importance of trust, since strong data protection and privacy safeguards help to build individuals' trust in how their data is processed, which encourages data sharing and thereby promotes innovation."*[20]

Currently, people have a right under Article 22 not to be subjected to *solely* automated decision-making that would have legal or similarly significant effects. This means that a human must be involved in the decision-making process; significant decisions cannot be taken by a computer alone. Article 22 is an important safeguard. Especially while the 'AI revolution' is still in its infancy, having a 'human in the loop' is important - not only to help mitigate the risks of automated decision-making, but also for reasons of human dignity. There is a widespread sense that important decisions about human beings should involve some element of human judgement.

Yet clause 11 would remove this right, except in respect of decisions involving 'special categories' of personal data. Article 22 already requires a decision to have legal or similarly significant effects before human involvement in the decision-making process is required. It is unnecessary and potentially harmful to add the additional requirement that the decision must also involve special categories of personal data. This is absurd one one remembers that in the Convention 108 there is a prohibition on processing sensitive data except with dedicated, narrow exemptions.

### Case study: biometrics in schools

In October 2021, there was public outcry when schools in Scotland adopted facial recognition for routine canteen cashless payment systems. Download our briefing including the court and regulatory action in other countries including bans on biometrics in schools.[21] Read about the 2021 debates in the Scottish Parliament on October 28th and the House of Lords on November 4th here; and the joint-action with Big Brother Watch and media coverage here. In March 2023 the Welsh Senedd backed a call for legislation over the use of biometric data in schools led by Sarah Murphy, member for Bridgend. Now is the time to strengthen, not weaken biometrics oversight and include education.

*"Despite repeated requests from the Biometrics and Surveillance Camera Commissioner to have legal oversight of the ethical use of that technology in schools, the Government have refused to agree. Why is this loophole still there, and when will it be closed?"*

Lord Scriven, December 2022, The House of Lords

### Enforcement becomes less likely and less of a deterrent for bad actors (Part 1, clauses 27 and 28, and Part 5)

The new Bill fundamentally changes the constitution of the data protection regulator.

---

[19] See, for example, Will Bedingfield 'Everything that went wrong with the botched A-Levels algorithm' (19 August 2020, Wired), available at https://www.wired.co.uk/article/alevel-exam-algorithm.
[20] International Conference of Data Protection and Privacy Commissioners. (2018). Declaration on Ethics and Data Protection in Artificial Intelligence.
https://edps.europa.eu/sites/default/files/publication/icdppc-40th_ai-declaration_adopted_en_0.pdf
[21] Defend Digital Me Briefing on biometrics in UK schools April 2023
https://defenddigitalme.org/wp-content/uploads/2023/04/Biometrics-in-schools-briefing-2-April-2023.pdf

Under Part 5 of the Bill, ICO would be restructured. Instead of a single Information Commissioner, there would be an Information Commission with an independent board and chief executive. More concerningly, the Bill would, under Part 1, clause 27, introduce a statutory framework of objectives for the Information Commission. In carrying out their functions, Information Commissioners would be required to have regard to: '(a) the desirability of promoting innovation; (b) the desirability of promoting competition; (c) the importance of the prevention, investigation, detection and prosecution of criminal offences; (d) the need to safeguard public security and national security.' This list of considerations is clearly weighted in favour of business interests and the interests of government, and includes nothing about the protection of the rights of citizens generally or children specifically. Already, the government relies on vaguely formulated arguments about 'national security' and 'crime prevention' to avoid being transparent and accountable in their practices of data collection and use. These new provisions would likely mean that Information Commissioners give even more weight to such arguments without safeguards in place.

Further, Part 1, clause 28 would give the Secretary of State new powers to influence Information Commissioners in the exercise of their functions. Under clause 28, the Secretary of State would be empowered to set 'strategic priorities' for data protection, to which Information Commissioners 'must have regard… when carrying out functions under the data protection legislation'. When the statement of strategic priorities is published, Information Commissioners would be required to explain in writing how they will have regard to the statement and publish a copy of that explanation. Again, this seriously weakens the independence of the regulator and makes it more likely that interests of government will be given undue weight, at the expense of the rights and interests of ordinary people.

This weakening of the regulator is extremely concerning as it would create more space for bad actors to act with impunity, using and abusing the personal data of people in general and children in particular. In a context where data abuses are already going unchecked, this is clearly a step in the wrong direction.

## Purpose limitation: changes mean less protection and more surprises

One of the key principles contained in Article 5 of the EU GDPR is purpose limitation. Before data processing starts, there must be a specific, well-defined purpose for it. Generally speaking, there can be no further processing of data in a way that is incompatible with the original purpose (though the EU GDPR foresees some limited exceptions to this rule for archiving purposes in the public interest, scientific or historical research purposes and statistical purposes).[22] This principle is foundational and indispensable to an adequate data protection regime.

As things currently stand, this essential principle is reflected in the UK GDPR.

However, the new Bill seriously loosens purpose limitation by creating a new set of conditions under which the processing of personal data for a new purpose is to be treated as processing in a manner

[22] See the Handbook on European Data Protection Law (2018 edition), page 122, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_en.pdf.

compatible with the original purpose. These conditions would be set out in a new Annex 2 and would include situations where the processing is 'necessary' for the purposes of 'protecting public security', 'responding to an emergency' or 'protecting the vital interests of the data subject or another individual'.

The list of new conditions is long and the language used is sometimes vague. Further, and even more concerningly, the Secretary of State is given new Henry VIII powers to amend Annex 2 by regulation. These changes seriously undermine one of the essential principles of data protection law. They come close to making purpose limitation obsolete in UK data protection law and put the UK at risk of an inadequacy decision. The Secretary of State could seek to make uses justifiable with unrestricted compatibility in Annex 2, and by changing initial purposes ('purpose limitation') in the UK GDPR in Article 5(1)(b) to the purposes for which the controller collected the data.

The processing of data must be foreseen by law. The new clause is in direct contradiction of the obligations under the EU GDPR and as such, directly incompatible with an adequacy decision.

> *"In this respect, it is useful to recall the Working Party's Opinion on purpose limitation, where it is specifically stated that 'when an organisation specifically wants to analyse or predict the personal preferences, behaviour and attitudes of individual customers, which will subsequently inform 'measures or decisions' that are taken with regard to those customers ....free, specific, informed and unambiguous 'opt-in' consent would almost always be required, otherwise further use cannot be considered compatible. Importantly, such consent should be required, for example, for tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research." (Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. European Commission, 9 April 2014, Page 47)*

## Legitimate interests: a loosening of the definition of 'legitimate' meaning in law, towards a layman's definition of justifiable according to our own criteria

Currently, under Article 6 of the UK GDPR, data processing is lawful only in a narrow and clearly defined set of circumstances. This includes, amongst other things, where "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child" (Article 6(1)(f)).

Clause 5(2) of the Bill would insert a new Article 6(1)(ea) and, in so doing, would create a range of new circumstances under which data processing is lawful, namely, where "processing is necessary for the purposes of a recognised legitimate interest". To a large extent, this replicates the wording of Article 6(1)(f) but it is notable that, here, the 'balancing test' featured in Article 6(1)(f) is stripped out (though the "necessity" test is retained) and there is no mention whatsoever of the rights and freedoms of data subjects or of children. In this sense, Article 6(1)(ea) is a chopped-off version of the Article 6(1)(f) with the safeguards for rights removed.

The set of 'recognised legitimate interests' for the purposes of Article 6(1)(ea) would be set out in a new Annex 1 and would include, for example, 'protecting national security', 'safeguarding public security' and 'investigation and prevention of crime'. It is highly concerning that the Secretary of State would have open-ended Henry VIII powers to amend Annex 1 at will (under clause 5(6)) and, instead of an obligation to not override children's rights and freedoms, she must now only have a lesser "regard to" them (clause 5(7)).

In addition, clause 5 of the Bill also sets out situations where data processing is for a 'legitimate interest' for the purposes of Article 6(1)(f). Staggeringly, the legitimate interests basis is broadened to explicitly permit intra-group transmission for ill-defined "internal administrative purposes". Again, that would now be without a balancing test and without an obligation to consider and justify against children's fundamental rights and freedoms.

These changes are highly problematic. Under EU data protection law, a legitimate interest is not to be read as akin to the layman's definition of 'justified' but rather must be 'acceptable under the law'.

And it is not enough for it to be lawful (i.e. in accordance with applicable national and international law); but it must also

- be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific); and
- represent a real and present interest (i.e. not be speculative).[23]

The EU GDPR requires the general principle that public authorities, as a rule, should only process data in performance of their tasks if they have appropriate authorisation by law to do so, and that is not created by the data protection basis or conditions around legitimate interests. Adherence to this principle is particularly important- and clearly required by the case law of the European Court of Human Rights - in cases where the privacy of the data subjects is at stake and the activities of the public authority would interfere with such privacy.

Data protection law is not permissive of itself, and can only follow on from the primary legislation that enables the statutory gateway for data flow at the point of collection with a proportionate legitimate aim pursued in law, which is necessary in a democratic society.

The new 'recognised legitimate interests' in Annex 1 flout these crucial principles, and put the UK at risk of an inadequacy decision and/or an adverse finding by the European Court of Human Rights.

### Legitimate interests: cutting the balancing test hinders necessity and proportionality tests

Today, the legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party, may provide a legal basis for processing, but it is conditional that the interests or the fundamental rights and freedoms of the data subject are not overriding, ***taking into consideration the reasonable expectations of data subjects based on their***

[23]ICO legitimate interests basis https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/

***relationship with the controller. By undoing today's purpose limitation the likelihood is that uses will be unexpected and go beyond those of the data subject (the person whose data it is about).***

In the context of fundamental rights, such as the right to the protection of personal data, proportionality is key for any limitation on these rights. More specifically, proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right. In other words, the limitation on the right must be justified. Safeguards accompanying a measure can support the justification of a measure. If the balancing test is scrapped, there is no basis for the assessment of proportionality which inhibits the determination of necessity. Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. Necessity is also fundamental when assessing the lawfulness of the processing of personal data. Without the balancing test there is nothing to determine lawfulness.

The new Bill permits what is explicitly forbidden in the EU GDPR under legitimate interests[24] and therefore is a direct challenge to adequacy

> *"It also suggests it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering."*

### *Legitimate interests also requires an opt out*

In today's law, to safeguard on the less rigid basis of legitimate interests which can tip the balance of power in favour of the data controller, the self-determination of the data subject to come into play by enabling a right to object.

The Bill's list of reasons in Annex 1 simply override both the data subjects fundamental rights and freedoms and also removes their right to object. In the context of Article 7(f), the controller can process the data, subject to conditions and safeguards, as long as the data subject has not objected.

"In this sense, the right to object can rather be considered as a specific form of opt-out."

### Direct marketing for the purposes of democratic engagement (age 14+)

*This clause in the Bill should be removed.*

When can an adult MP or election campaigner legitimately have contact with a teenager without consent? Schedule 1, Annexe 1 Clause 9(b) proposes that the legitimate interest for contacting children for the purposes of influencing democratic engagement should override the child's fundamental rights and freedoms to confidentiality of their personal data being processed for party political work. There is no opt-in nor opt-out. The Minister would only have to 'consider' the effect on children's privacy.

[24] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

It would mean relentless email from all the candidates of any of the parties on the Electoral Commission Register of parties. Should we enable the promotion of extremist images, messages, direct to every child's device at any time as long as it could be said to be within the candidates 'campaign for election" and profiling would be permitted as long as it was within activity labelled "to support or promote democratic engagement." Pernicious profiling and targeting of vulnerable teens encouraging participation in every polemic rally every day of the week. Is that what this intends?

The UK International Tech Strategy[25] that after all says, "Authoritarian regimes have an alternative vision of harnessing technology for their own ends." Everything in this Bill must protect against that.

Children should not be profiled and targeted for marketing 24/7 365 days a year by an unlimited number of parties (currently there are 642 registered parties (as of April 2023) and over 2,100 including those currently deregistered).[26] Untargeted marketing can continue as is to households.

If at all, this should be tied narrowly to the voting age and in a narrow time window. Therefore 9(b) children aged 14 and over, should be raised to 16, and would be restricted in practice in the UK at the time of writing to the Welsh voting franchise[27] where young people aged 14 and 15 are now able to register to vote and 16 and 17 year olds can now vote in Welsh Parliament (Senedd) elections and Local Government elections, and it should only be around that time period.

Sending unsolicited birthday cards[28] before any child's 18th birthday would remain *unnecessary* even with the current drafting, and therefore remain unlawful anywhere in the UK.

### Case study: The Home Office does not know the impact of the DfE Hostile Environment

**Over 23 million (former and current) school pupils and students' national pupil records are processed monthly for the purposes of the Home Office for immigration enforcement. Millions of families and children whose names will never be in the "looked for" lists will nonetheless have their records needlessly and disproportionately searched for this new purpose with no safeguards in place for errors or routes for redress. The personal data handed over if they do find a match, can include five years of past home and school addresses and more, even a sensitive "adopted from care" flag. When asked in 2020 via PQ92745,[29] the Home Office did not appear to know or even care about its impact of using pupil data, and in answer to FOI the DfE said it did not know either. They don't know what happens to the children, much less their data, despite that being an organisational duty to demonstrate accountability and records of processing under the UK GDPR.[30]**

---

[25] The UK's International Technology Strategy. (March 2023.). GOV.UK. Foreword from the Foreign Secretary. https://www.gov.uk/government/publications/uk-international-technology-strategy/the-uks-international-technology-strategy

[26] The Electoral Commission registers of Political Parties, Non-party campaigners & Referendum Participants as required under the Political Parties, Elections and Referendums Act 2000 https://search.electoralcommission.org.uk/Search/Registrations

[27] the data subject is aged 14 or over

[28] Mark Spencer MP (2016) On sending unsolicited birthday cards to children https://www.sherwoodconservatives.com/news/know-anyone-who-would-18th-birthday-card-their-mp

[29] Parliamentary question 92745 (2020) from Caroline Lucas MP to the Home Office https://questions-statements.parliament.uk/written-questions/detail/2020-09-21/92745

[30] Defend Digital Me calls for Home Office data processing accountability (2023) https://defenddigitalme.org/2023/03/21/call-for-action-from-the-uk-information-commissioner-to-uphold-childrens-rights-in-the-hostile-environment/

It is crucial to remember that we have already weakened the protections and safeguards that are required when using legitimate interests as a lawful basis in data protection law, by having removed the Charter of Fundamental Rights.

Since the Lisbon Treaty entered into force on 1 December 2009, the European Union Charter of Fundamental Rights ('the Charter') enshrines the protection of personal data as a fundamental right under Article 8 (In the ECHR), which is distinct from the respect for private and family life under Article 7. Article 8 lays down the requirement for a legitimate basis for the processing. In particular, it provides that personal data must be processed 'on the basis of the consent of the person concerned or some other legitimate basis laid down by law'. These provisions reinforce both the importance of the principle of lawfulness and the need for an adequate legal basis for the processing of personal data.[31]

The new *definition of legitimate interests in Annex 1, chops off the rights-parts of it in current law. Today's legitimate interests offers a legal basis for processing data in 6(1)(f), "necessary for the purposes of the legitimate interests pursued by the controller or by a third party* ***except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."***

*The new law cuts all that out, making it only necessary for the Secretary of State to have regard for rights and children when making changes, rather than the legal basis being unable to override their rights for very good reasons, as safeguards to prevent misuse and protect children.*

We are particularly concerned about how the weakening of existing safeguards will impact children and in particular through the explicit removal of them in the current wording of legitimate interests to the new 7(f) where they are cut out.

## Research purposes: changing the definition creates more exemptions

The Bill will fundamentally undermine the professional status of research if it goes ahead with proposed changes. The definition of 'research' will become more amateur, more commercial, and more exploitative. The new definition will expand the permitted uses of data that attract the data processing research exemptions granted today, including for example the need for consent or to offer people a Right to Object. The result of activity that can, "reasonably be described as scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity" will see our children routinely become lab rats for trialling new products without consent.

### Case study: Visible Classroom — an edTech product for teacher improvement that collects voice recordings from classrooms

[31] Opinion 06/2014 on the notion of legitimate interests of the data controller
under Article 7 of Directive 95/46/EC (2014) p.8
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

Children's personal data and findings from edTech 'research' projects are being used in the development of commercial products, and would no doubt meet the new definition. They are used as test subjects without consent. As Nesta explained[32] about one example project in 2015,

> *"Based on this work with teachers and students, Ai-Media UK has been able to develop 'The Visible Classroom' further into a refined product for supporting teacher professional development. What was a new technology not tried in schools in this format before, has become a product that can be rolled out to schools."*

*Despite some edTech and research projects claims to influence mental health, emotion or learning, there is no consistent ethics oversight of how these projects can be introduced into classrooms and that parents can opt out of, never mind opt in. Nonetheless the companies of academic institutions and researchers who might be defined as 'scientific' can come into schools, extract children's biometric (voice) data and take it away from which the company benefits with a product to sell, without any benefit for the children who have no choice. This particular product was found in the EEF trial to have had a negative effect on teaching and learning. A negative impact of two months reduction in learning was estimated for KS2 reading outcomes for students in Year 5.*

> *"Our trial of the Visible Classrooms intervention involved teachers of 7230 students from 86 schools. The independent evaluation found that pupils taught by teachers in intervention schools made, on average, one month less progress in KS2 reading and maths."*
>
> https://educationendowmentfoundation.org.uk/projects-and-evaluation/projects/the-visible-classroom-2015

Nearly 1 in 4 parents don't know if their child has been signed up to systems using personal data in school, according to a survey we commissioned by Survation in 2018.[33] Overall, of the 1,004 parents of children aged 5-18 in state education in England, only half (50%) of parents polled said that they have sufficient control of their child's digital footprint. Over a quarter (28%) said the amount of control is insufficient while 22% said "don't know".

[32] Making learning visible: First 'Technology in Education' evaluation published. The results of our Visible Classroom pilot: source https://www.nesta.org.uk/blog/making-learning-visible-first-technology-in-education-evaluation-published/ (https://web.archive.org/web/20190723002723/https://www.nesta.org.uk/blog/making-learning-visible-first-technology-in-education-evaluation-published/)

[33] Survation conducted the survey of 1,004 parents of children aged 5-18 in state education in England on behalf of defenddigitalme between 17th-20th February. Full tables can be found at https://survation.com/wp-content/uploads/2018/03/Defend-Digital-Me-Final-Tables-1.pdf https://www.survation.com/1-in-4-parents-dont-know-child-signed-systems-using-personal-data/

## Part 3: customer data and business data. Children can also be customers.

This "includes a power to require suppliers and others to provide customers with customer data and business data." This is a vast power to require data about customers' and your behaviours, purchases, services and anything the Secretary of State demands for the state under the Henry VIII powers. According to the government's own impact analysis[34], this could give rise to unlawful interferences with ECHR Article 8 rights and Article 1 of Protocol 1 and, in relation to enforcement of the regulations, Article 6. This also seems to conflict with the foreseeable purpose limitation at the point of collection, as well as fundamental principles of data minimisation and necessity.

## What is missing

### Our proposal 1: Promote the respect for data rights in emerging technology

The Internet-of-Things means that often "smart" gadgets are collecting and processing personal data in ways children do not see and cannot expect as there is no screen. The Bill makes no attempt to understand these emerging harms or how children should be given agency to control their own interactions, what is collected and what is not, and to whom it is sent onwards for what purposes.

> *"Internet-connected toys fail miserably when it comes to safeguarding basic consumer rights, security, and privacy. Join us in saying that we will not allow these companies to use our kids as guinea pigs for emerging technologies."*
>
> *Finn Myrstad, the Norwegian Consumer Council "Forbrukerradet", BEUC member.*

### Case study: Cayla doll

Through hardware hidden in the body of the manufacturers created a doll that can carry a conversation through artificial intelligence and natural language processing. But do parents understand that their child is now sending chat to companies and third parties not only for new product development but could be used in ways that are unexpected. It's effectively putting a listening device into homes that some will argue should then be monitored if the content seems suspicious to the receiving company. Where are the ethical boundaries and legal limits of this?

Anything the child tells the doll is transferred to the U.S.-based company Nuance Communications, who specialise in speech recognition technologies. The company reserves the right to share this information with other third parties, and to use speech data for a wide variety of purposes.

**Kids are also subject to hidden marketing.** The toys are embedded with pre-programmed phrases, where they endorse different commercial products. For example, Cayla will happily talk about how much she loves different Disney movies. Meanwhile, the app-provider has a commercial relationship with Disney.

[34]https://web.archive.org/web/20230404085753/https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum

## Our proposal 2: Make equality monitoring safe in HIgher Education

Today, the UK Department for Education holds lists of millions of people's names on record with their declared sexual orientation. Students who have submitted their sexual orientation and religious affiliation as part of equality monitoring when applying for Higher Education do not know that these data are added into their named, longitudinal, national pupil record.

We believe how these processes operate in practice in the higher education sector must change urgently.

> The declared sexual orientation of 3,213,683, broken down as below. The religious affiliation of 3,572,489 people is held (give or take some duplicates and issues in the data quality).

Why is this data collected, retained and above all "linked" with individually named, highly detailed school records at all? Why is it not only collected and kept as stand-alone statistics to achieve the same aims? How widely spread is it across the Office for Students, and Higher Education Funding bodies? Is data used to do anything meaningful given that the majority of categories are still substantially 'not provided' or 'refused'.

We believe that these records must be destroyed at named level; and at most, only statistical outputs should be processed, accessed, or retained, and no raw identifying data should be passed around at all from the point of collection. Dealing in data through downloads and distribution, increases risk to both people and institutions, and is long out of date practice. It's not necessary and can be done differently.

How many UK students will one day live and work in Uganda is not the only real question of potential for harm here.

There is an opportunity in the Data Protection and Digital Information Bill before Parliament in summer 2023 to right this wrong. And for example, the Higher Education and Research Act 2017 might be amended to reference only statistical data in a number of places where it demands data sharing on "equality of opportunity" in connection with access to and participation in higher education provided by English higher education providers.

## Our proposal 3: Restore the dignity of dead children (GDPR Recital 27)

The potential derogation for the protection of data for the deceased (Recital 27) was omitted in 2018, which many other countries[35] did include. It should be included now for the UK.

Without safeguards in data protection law for the personal data of the dead, we are enabling the misuse of personal data that can continue to affect the human dignity, safety, and privacy of the living. We are missing a solid foundation for the basis of a social contract for genomic sequencing at scale, issues around insurance, and its ethical considerations. Consider:

[35] Bird and Bird (no date) Personal data of deceased persons https://www.twobirds.com/en/capabilities/practices/privacy-and-data-protection/general-data-protection-regulation/gdpr-tracker/deceased-persons

- the new NHS database on dead children
- police abuse of dead children's identities[36]
- DNA used as standard practice in research, including for commercial research, without parental and child consent, (and what needs to change as we outlined to NHS England and Public Health England in 2016)[37]
- the national plans from the Government's Chief Medical Officer Dame Sally Davies "genomic dream" for population-wide genetic testing of "Generation Genome".
- the intentions of some in research to link genomic data and education data, longitudinal admin data from birth, through to HMRC earnings and DWP welfare payments and the implications for policy and society.

While some may argue that often children's data is connected to their parent's and therefore would be in the scope of data protection law, it may not always be the case. We should really be forward looking and include rights here for all that go beyond the *living* "natural persons", because our data does, and that may affect those who we leave behind. It is insufficient for researchers and others who wish to use data without restriction to object, because this merely pushes off the problem, increasing the risk of public rejection of 'hidden' plans later.

## Our proposal 4: Restore the rights of 9 million children in school today and the 15 million who have left school whose national records are controlled by the DfE (Right to Object)

The Right to Object is part of UK and EU GDPR today however it is not made possible at the Department for Education nor in schools, where a simple check-box on the 15 UK Schools Information Management Systems could enable the Right to Object (for example to commercial re-use of identifying pupil data for external purposes beyond the Department for Education). Pupil data is also health data, special educational needs, children's social care records including abuse, and now sexual orientation and religion from equality monitoring. If the DfE does not honour the Right to Object already in law, then only making the mechanism compulsory in providers may enable it.

---

## Annexe

**Opinion 03/2013 on Purpose Limitation (2013) Working Party 29**
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

**Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

**Other WP29 opinions and recommendations**
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm

[36] COPS. (2016). Spycops Stealing Dead Children's Identities. Campaign Opposing Police Surveillance. https://campaignopposingpolicesurveillance.com/2016/11/11/spycops-stealing-dead-childrens-id/
[37] DDM consultation response on the NHS Newborn Blood Spot Screening Programme 2017-18 https://defenddigitalme.org/wp-content/uploads/2016/09/DDM_Newborn_Screening_Consultation2509.pdf