Written evidence submitted by the 5Rights Foundation (DPDIB15)

Data Protection and Digital Information Bill (No.2)

House of Commons Public Bill Committee
Written evidence submission

About 5Rights Foundation

5Rights develops new policy, creates innovative frameworks, develops technical standards, publishes research, challenges received narratives and ensures that children's rights and needs are recognised and prioritised in the digital world. While 5Rights works exclusively on behalf of and with children and young people under 18, our solutions and strategies are relevant to many other communities.

Our focus is on implementable change and our work is cited and used widely around the world. We work with governments, inter-governmental institutions, professional associations, academics, businesses, and children, so that digital products and services can impact positively on the lived experiences of young people.

At second reading, the 5Rights Foundation welcomed Minister Scully's commitment to preserving the status of the Age Appropriate Design Code (AADC) in recognition of its central role in the protection of children's data online.

> "We are committed to protecting children and young people online. The bill maintains the high standards of data protection that our citizens expect and organisations will still have to abide by our ***Age-appropriate design code***. Any breach of our data protection laws will result in enforcement action by the Information Commissioner's Office.[1]"
> *Minister Paul Scully, House of Commons, 17 April* 2023

5Rights is delighted by this commitment from the despatch box but in order for the Ministers words to remain true some other issues in the bill need to be considered.

The proposed changes to UK GDPR and the amendments to interpretations and principles around what constitutes personal data (clause 1), research and statistical purposes (Clause 2), Lawfulness of Processing (Clause 5) and the Purpose Limitation (Clause 6), undermine data protection upon which the Code depends.

---

[1] Data Protection and Digital Information Bill No.2, Second reading, House of Commons, Minister Scully, link

This submission sets out the key principles of the code, its domestic and international impact, and how the changes to UK GDPR risks undermining children's data protection.

Children's special data protections and the Age Appropriate Design Code

The Age Appropriate Design Code (AADC)[2] is the UK's regulatory code for child data protection. Brought in by the Data protection Act 2018, it is a statutory code of practice which translates the law into 15 standards enforced by the ICO. it is the global gold standard in children's data protection and was the first statutory code of its kind in the world. It is binding on all services – including apps, online games, social media - 'likely to be accessed by children'.

Despite its beginnings in UK law, it has reframed protection for children globally by raising the age of online protections for children to the age of 18 (per the UN Convention on the Rights of the Child) rather than the standard 13, and by placing duties on services to consider the best interests of children, their differing ages, capacities, and development needs in developing their services. All companies *likely to be accessed* by children must be safe and privacy preserving by design and default ensuring that companies offer children privacy-by-design. Importantly it made the connection between privacy and safety.

Impact of the Age Appropriate Design Code

The Code has made the UK world-leading on the issue of children's data protection. Since coming into law in September 2020, the AADC has inspired other countries to follow suit, and there are now similar codes in Ireland[3], the Netherlands[4] and in California[5] - the home of big tech. Its international impact is growing still, and it has been introduced in Maryland[6], Minnesota[7], Nevada[8] and New Mexico[9]. Similar codes are currently being considered in Turkey, Argentina, and Indonesia.

Following the introduction of the Code, companies have made significant changes that have transformed the experiences of children online for the better.

- Meta – one of the largest social media companies in the world - has introduced a number of positive measures to it key services, Facebook and Instagram. Instagram stopped private messaging from unknown adults to children, and it has partnered with Yoti to introduce new age assurance measures. Instagram has also introduced 'positive nudges' for teen users who repeatedly view the same type of content, encouraging them to try something different[10]. Across

---

[2] Age Appropriate Design Code, ICO, link
[3] The Fundamentals for a Child-Oriented Approach to Data Processing, link
[4] Code for Children's Rights, link
[5] The California Age-Appropriate Design Code Act, link
[6] Maryland: Bill on online children's data introduced to Senate, link
[7] Minnesota Kid's Code, link
[8] Nevada Kid's Code, link
[9] New Mexico Kid's Code, link
[10] New Tools and Resources for Parents and Teens in VR and on Instagram, Instagram, link

both services, Meta updated its privacy policy to make it more accessible and clearer, and set up a privacy centre for users to control who can see what they share across services, and what data is collected on them and the adverts they see.

- Google turned location History off, without the option to switch it on, for all under 18s globally. Google has also updated it terms to prevent advertisers targeting under 18s based on their age, gender, or interests. They have also developed easy-to-understand materials[11].
- TikTok sets all users accounts under the age of 16 to private by default[12] and turns off the setting 'Suggest your account to others', which shows profile recommendations in the For You page, off by default for users under 16. Users under the age of 16 do not have access to direct messaging. When someone aged 16-17 joins TikTok, their direct messaging setting will now be set to 'No One' by default[13]. They have also turned off notifications for under 15's at 9pm and under 17 at 10pm.
- Microsoft Edge, a web browser, has launched a 'Kids Mode'. There are two modes available, one for kids aged 5 to 8 and another for 9 to 12[14].
- Roblox now does not show targeted advertising to children or track them for that purpose, and partners with third-party advertising companies to serve contextual advertising and cap the frequency of advertising to children[15].

These are just some of thousands of changes which together have seen the biggest redesign of digital services for any social purpose. It has been noted around the world and data privacy for children now forms public policy, including in the US where it was part of President Biden's State of the Union Speech[16] and in California where Governor Newsom signed the California AADC into law with a fanfare[17].

Data Protection and the Digital Information Bill No.2

The following clauses in the bill risk watering down the protections offered by the AADC and damage the march to a global standard of data protection for children which in turn undermines our efforts to make the online world safer for children.

Clause 1: Information relating to an identifiable living individual

Clause 1 amends section 3 'terms relating to the processing of personal data' of the DPA 2018 and inserts a new section 3A. This would narrow the definition of personal data by restricting the circumstances in which a living person can be 'identified' - one of the two tests of whether information is 'personal data'.

New section 3A would insert two knew cases for where a person is 'identifiable' which both appear to rest strongly on the judgement of individuals and could insert a great

---

[11] Giving kids and teens a safer experience online, Google, link
[12] Teen privacy and safety settings, TikTok, link
[13] Furthering our safety and privacy commitments for teens on TikTok, link
[14] Learn more about Kids Mode in Microsoft Edge, link
[15] Roblox Will Ban All Advertising Aimed at Children Under 13 With New Standards, Roblox, link
[16] President Biden's State of the Union Address 2023, link
[17] Governor Newsom Signs First-in-Nation Bill Protecting Children's Online Data and Privacy, link

deal of subjectivity into the assessment of whether data is personal. For example, 'reasonably knowing' if the person is 'likely to be identifiable' could rely on the technological knowledge of the individual processing the data to know whether there is technology which could make the person identifiable. With the pace of technological development, and the challenges keeping up with the latest capabilities, this could lead to differing outcomes depending on who has made that judgement.

The key impact means more data would fall outside the current data protection framework. This includes children's personal data.

It is essential that there is no watering down of the underlying principle of what constitutes personal data in relation to children.

Clause 2: Meaning of research and statistical purposes

Clause 2 would broaden the definition of what constitutes data processing for scientific research to include research that is carried out as a commercial activity. In effect this could make it easier for companies to use personal data in product development. Broadening the definition of data processing for scientific research could lead to poor uses of children's data which purports to be in their best interest – particularly in EdTech.

EdTech is a nascent industry which has the potential to be hugely beneficial for children. However, the way it is currently used does not always provide a safe and secure environment for children, or their data. A report from Human Rights Watch which reviewed 164 EdTech products found 89% of them had engaged in data practices that put children's rights at risk, undermined or actively violated them. Researchers found instances of companies monitoring children without their consent and knowledge, harvesting children's data (including information on what they do, who they are, where they live or study) to the extent that the only way to protect themselves from this would have been to throw "the device away in the trash"[18] [19].

Further research by the Digital Futures Commission found that Google and ClassDojo were collecting children's educational data and processing and profiting from that data for advertising and other commercial purposes. Where teachers had shared external links in Google Classroom, children were taken out of this protected environment and into third party tracking zones[20].

These examples demonstrate how even in perceived positive uses of children's data, they can be made vulnerable to commercial exploitation.

It is disappointing that the bill fails to actively facilitate access to data by independent researchers. This puts a key objective of the bill – to drive scientific research - at serious risk. Independent researchers have in accessing this data means to study how technology works and can impacts children (both positively and negatively). Thanks to

---

[18] Governments Harm Children's Rights in Online Learning, Human Rights Watch, link
[19] Children's Rights Violations by Governments that Endorsed Online Learning During the Covid-19 Pandemic, link
[20] Digital Futures Commission, link

whistle-blowers such as Frances Haugen, we now know that Facebook was aware that its platform was impacting the mental health of children having kept internal research secret for two years that suggested its Instagram app made body image issues worse for teenage girls[21]. However, if tech companies do not have to, or cannot easily, pass on internal data to researchers, it prevents researchers from understanding the harms this technology has, and how these services can be improved for children. The General Comment 25 on children's rights in relation to the digital environment states, "regularly updated data and research are crucial to understanding the implications of the digital environment for children's lives, evaluating its impact on their rights and assessing the effectiveness of State interventions. States parties should ensure the collection of robust, comprehensive data that is adequately resourced.[22]"

The bill should not allow children's personal data to be used for commercial purposes without a high level of protection and only ever in their best interests.

The bill should extend the protections of the AADC to all EdTech.

The bill could usefully bring forward a framework that facilitates independent researchers access to data to support research and build the evidence base on the impact of digital services on children.

Clause 5: Lawfulness of processing

Clause 5 introduces the concept of a 'recognised legitimate interest (RLI)'. This is a class of legitimate interests where processing data would be automatically lawful, provided it is necessary to meet the legitimate interest test. Currently, processors in the private sector must balance their legitimate interest to process the data, against the privacy interests of the data subject.

The RLI's are listed in Annex 1 as - national security and defence, emergencies, crime, **safeguarding vulnerable individuals** (vulnerable individuals include anyone under the age of 18) and democratic engagement. The clause makes allowances for the list to be amended by the Secretary of State, although she must have regard to "where relevant, the need to provide children with special protection with regard to their personal data."

While the Secretary of State must have regard for children's special protections if she is to amend this list – the bill text qualifies this with "where relevant". Children must always receive special protections as per Recital 38 of GDPR. Clause 5 would introduce language that would make children's protections contingent on where the Secretary of State deems these protections to apply. This would introduce a loophole in the bill and could seriously undermine protections for children's data[23].

---

[21] Facebook aware of Instagram's harmful effect on teenage girls, leak reveals, Guardian, link
[22] General comment No. 25 (2021) on children's rights in relation to the digital environment, link
[23] "Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.", Recital 38, GDPR, link

Secondly, an automatic lawful basis for the processing of data on the basis of safeguarding vulnerable people (e.g. children) could lead to inconsistency in outcomes, especially where there appear to be differing views on what constitutes safeguarding by officials. A recent investigation by Liberty Investigates and the Observer found Sussex Police had advised officers to collect the contents of unaccompanied child refugee's phones. When questioned about this the Home Office said "the downloading of phones or devices in the possession of any child does not form a routine part of the safeguarding process"[24].

All children's data must be considered 'special' and 'individual'. There must be no additions to 'legitimate processing' that would result in routine access to or processing of children's data.

Clause 6: Purpose limitation

Clause 6 amends article 5 of GDPR on the principles relating to the processing of personal data. The second principle of article 5 protects individuals' data from being re-used beyond the purpose for which it was originally given or collected, where the further 'use' would not be compatible with its original purpose – the purpose limitation. This bill would:

- Amend article 5 to limit the rules around further processing to only apply to the controller who originally collected the data.
- Introduce new Article 8A which introduces new conditions or objectives for where further processing is automatically compatible with the original purpose. Annex 2 provides a list of conditions including the "safeguarding of vulnerable individuals" which includes children (anyone under the age of 18). Compatibility can also be demonstrated if processing meets one of the objectives listed in Article 23 - which includes 'important objectives of general public interest'. The bill gives the Secretary of State powers to amend this list.

Changes to purpose limitation represent a substantial weakening of this principle in the GDPR.

Introducing purposes which would be considered automatically 'compatible' with the original purpose and giving the Secretary of State significant powers in shaping these conditions, will permit the processing of personal data for further purposes which would otherwise have been incompatible. In the context of children's personal data, this is not acceptable.

Firstly, the condition that would grant further use on the basis of safeguarding vulnerable children could lead to poor outcomes for children – as outlined above there is inconsistency on the issue of safeguarding by public authorities.

Secondly, Secretary of State powers could enable government to use personal data for a different reason than for which it was collected for a potentially wide range of 'important objectives' in its economic or social policy. This vague and open-ended

[24] Fears grow over police collecting data from lone child refugees in UK, Observer, link

condition could allow for further processing of sensitive data which in the current hostile environment for families with children who have insecure immigration status, for example, could diminish trust in data sharing and push many families to hide from agencies which increase their vulnerability to trafficking and other harms[25].

The AADC is very clear that a child's data should be used only for the stated purpose, and only to the extent that children could reasonably be said to understand that purpose. Nothing in the bill should result in a downgrade of purpose limitation in relation to children's data.

Recommendation

5Rights welcomes measures which make compliance with data privacy clearer.

Children's data must be treated with the highest levels of privacy and with their best interests front and centre. As set out in Recital 38 of GDPR, "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."

It is essential that there is no watering down of the underlying principle of what constitutes personal data in relation to children.

The bill should not allow children's personal data to be used for commercial purposes without a high level of protection.

The bill should extend the protections of the AADC to all EdTech.

The bill could usefully bring forward a framework that facilitates independent researchers access to data to support research and build the evidence base on the impact of digital services on children.

All children's data must be considered 'special' and 'individual'. There must be no additions to legitimate processing that would result in routine access to or processing of children's data.

The AADC is very clear that a child's data should be used only for the stated purpose, and only to the extent that children could reasonably be said to understand that purpose. Nothing in the bill should result in a downgrade of purpose limitation in relation to children's data.

In order to make Minister Scully's commitment to children meaningful, the AADC must be enshrined on the face of the bill and nothing should be allowed to undermine its provisions.

---

[25] An argument for better data about children, Leon Feinstein, link

We further recommend that the Government commission's an independent legal opinion on how the bill in its current form lessens and or upholds the AADC so that it is clear to parliamentarians what is at stake.

Privacy is at the heart of a fair and safe online world for young people, we thank the committee for their efforts in keeping it that way.

May 2023