KC Legal Opinion

Defend Digital Me commissioned and are placing into the public domain a Legal Opinion by Stephen Cragg KC of Doughty Street Chambers relating to the Data Protection and Digital Information Bill (2023).

This Opinion (a) summarises the main legal arguments and analysis; (b) provides a more detailed explanation of the Bill; and (c) lays out the legal opinion in full. In summary he found:-

- **The proposed change to the definition of 'personal data' in the Bill has the potential to mean that some data currently defined as 'personal' will in future be excluded from protections in the DPA 2018 and UK GDPR**. In particular there is potential for the definition of 'personal data' to change depending on who is processing data, and the Bill removes the need for a data controller to have an ongoing duty to consider whether retained data has become 'personal data'.
- The terms 'scientific research' and 'scientific research purposes' would now be defined by clause 2 of the Bill to mean **'any research that can *reasonably* be described a scientific, whether publicly or privately funded and whether carried out as a commercial or non-commercial activity**'.
- **Loosening of requirements on purpose limitation** will assist commercial and non-commercial organisations involved in research and re-using personal data obtained from third parties, but will do nothing to increase protection for individual data subjects.
- **A list of 'legitimate interests' has been elevated to a position where the fundamental rights of data subjects (including children) can effectively be ignored** where the processing of personal data is concerned. The Secretary of State can add to this list without the need for primary legislation, bypassing important Parliamentary controls. Business friendly interests, such as direct marketing, are now listed, without provisos, as interests which may be seen as 'legitimate' giving succour to commercial organisations, but **no added protection to the personal data of individuals.**
- **The powers of the Information Commissioner are diluted** in a way which provides less protection to data subjects, but much more power to the government to restrict and interfere with the role of the Commissioner.

"*Overall the Bill is a significant shift away from a rights-based regime towards a set of market standards which treats data a product, raising concerns that the UK is moving away from international benchmarks and standards.*"

"*If the new definition of personal data is enacted, that will also, of course, mean that fewer data of children will be protected under the new law.*"

"*The best way to protect children's data is by the retention or introduction of specific safeguards in legislation. However, there is no doubt in my mind that, additionally, such a code of practice as previously advocated for by DDM would be a useful tool for ensuring that special care is taken when the processing of the personal data of children within the education and social care systems (especially) is under consideration.*"

Download the new legal opinion on the Data Protection and Digital Information (DPDI) Bill by Stephen Cragg KC [pdf. 282 KB] from: https://defenddigitalme.org/2023/11/27/new-legal-opinion-on-the-data-protection-and-digital-information-bill/

The Defend Digital Me View of the Bill

Defend Digital Me is calling for the Data Protection and Digital Information Bill to be withdrawn. In March 2023, Defend Digital Me, as part of a coalition of 25 further civil society organisations, already wrote to the Secretary of State for Science, Innovation and Technology, Michelle Donelan MP, calling for the Data Protection and Digital Information (DPDI) Bill to be dropped. The signatories included trade unions as well as human rights, healthcare, racial justice, migrants rights, workers' rights and criminal justice organisations. We share concerns that the government's proposals will seriously weaken data protection rights in the UK, and will particularly harm people from marginalised communities.

This under-scrutinised Bill makes significant and substantive changes to the safeguards in place for the protection of everyone, including children, in the digital environment.

This Bill upends the principles of necessity and proportionality and data minimisation. It touches on and negatively affects every one of the seven foundational principles of data protection law.

It will make our personal data more available for commercial benefit, while putting our personal privacy at risk. In particular **Defend Digital Me believes it means that children will find it much harder to exercise their own rights to manage their personal data once they become adults**, when for example, consent was given by a parent.

One of the respected constitutional law scholars of the 20th century, the late **Paul Freund**, memorably said that the U.S. Supreme Court "should never be influenced by the weather of the day but inevitably they will be influenced by the climate of the era."

In the view of Defend Digital Me, this Bill is the perfect storm of a post-Brexit, post-pandemic economy, and Home Office "Hostile Environment".

Data protection law is not something that should be driven by the political weather of the day. An ever-increasing volume of data about us in an increasingly automated world demands greater efforts towards upholding protection and power to the people whose lives are affected by its use and abuse.

There is no reason that makes it necessary to change today's law to make current data practices less safe, less fair and less transparent to the people whose lives are recorded in their digital activity, their likes and habits, and whose data footprints are already tracked across the globe by thousands of third parties, vying for our online attention.

This Bill gives more power to data users and takes it away from the people who the data are about. It will not only weaken protections by enabling more personal data to be excluded from protection using research exemptions, but make vast amounts of processing fall outwith the definition of personal data entirely over time -- relabelling the data doesn't change the nature of the data or its sensitivity or its threat model. It also restricts access to see what is done to our digital-selves through interferences with our private and family life, and with fewer routes to remedy and redress when things go wrong. This Bill takes the UK in not only a new, but completely wrong direction.

The Bill must be dropped.

Given our remit in the education and children's sector, we considered the effects on children in particular. In our 2021 report, The Words We Use in Data Policy: Putting People Back in the Picture, we explained that if the government wishes to simplify the law, it should not be rewriting another version of one part of our Data Protection law, at all, but first, fixing all of the failed transposition of the 1995 Directive implemented in the UK through the 1998 Data Protection Act which came into force on March 1, 2000 and repealed the Data Protection Act 1984. The European Commission found that about one-third of all of the 1995 Directive's provisions had not been fully or properly transposed in the UK law. The Commission (after a long delay during which this was not resolved) started infringement proceedings over this mis-transposition, but did not pursue this further and the matter ended unresolved with Brexit. This Bill is an attempt to take us back in time. The GDPR came into being recognising the risks of emerging technologies and their implications for human rights, and that what had gone before was not enough to meet growing public outcry over data misuses. The UK government should be consolidating the two amended laws (the UK-GDPR and the Data Protection Act 2018) into one, comprehensive piece of data protection law -- not redrafting new complex layers.

Children's protection and recognition of needs are missing

This Bill contradicts the wide acceptance of today's position in recital 38 of the GDPR that, "*Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing ...*". Instead it says marketing should become a formally recognised legitimised interest that *outweighs* the rights and freedoms of individuals. This fails to understand the adTech ecosystem and real-time biding mechanisms behind the scenes of today's online marketing activities every nano-second of every day wherever we go and whatever we do. It fails to recognise children, as well as adults, should be protected from the undue influence those systems can have on our autonomy, agency and choices we make. Including weakening of protections of data repurposing for political persuasion which is so desperately in need of protection when it comes to mis-- and disinformation, to uphold democratic aims.

Children's ability to exercise the right to rectification and erasure are removed

Recital 65 of the GDPR today will become near impossible to exercise for children later in life, if in future personal data is no longer personal some way down the line. [A] "*data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes the law. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.*" How is anyone supposed to exercise this right if the redefinition of personal data changes the nature of its status over time, and later in life the former child can no longer exercise rights they should have been able to exercise at the point of collection, but were incapable of doing so?

Safeguards for children from profiling

The Bill contradicts the spirit of Recital 71, which states that children should have the right not to be subject to a decision, "*which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing* and which produces legal effects concerning him or her ***or similarly significantly affects him or her*[...]*...In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision*."**

When it comes to political opinion and data for political purposes, we have had no answer to the question what the safeguards are for teenagers? These would be required by Article 6 of the Convention 108.

The desire to use the UK population as a resource to exploit by the private sector to build data products in the short-term, and with even less oversight and fewer controls, will come at the cost of long-term risks and harms to people through greater exposure of their digital footprint and identity. The effects can last a lifetime.

Data protection is a Gatekeeper to Access Digital Identity

This bill is a disaster for the public, in particular for children and the immediate and future security of UK identity as a national asset and as a national security gatekeeper -- weakening the protections around personal data and ID are a threat not only to individuals but the State. Its soft wording seems like insignificant changes but then, if so, why change it at all? In fact this Bill brings in substantive and significant change to the UK data protection regime. The UK will diverge from existing data protection law, become a lone-rider in a new wild west of data washing by data hoarders around the world. It risks the interoperability of common high standards of personal data flows across borders.

Data protection is a gatekeeper to children's lives with lifelong consequences

In an apparent government u-turn on its recent obsession with children's online safety, the government is writing law now that will reduce children's digital protection. This runs contrary to everything anyone interested in the subject has recommended for a long time, including in the 2018 resolution from the International Conference of Data Protection and Privacy Commissioners:

> *"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."***

This is furthermore, a particular high-risk for genomic data captured without consent as a baby for which there is no need for change by actors who want to operate to the high standards of protection expected by the public, and for public interest research -- people who want this changed want to operate to lower standards, for example, by not having to tell the public broadly what they will do in advance (at the point of collection) or not giving people any choice of the purposes of re-uses to exclude, for example military or abortion research to which some object as a matter of conscience.

Genewatch UK agrees. Dr Helen Wallace, Director of GeneWatch UK has said alongside their briefing, "This is a short-sighted and extremely dangerous attempt to tear up existing safeguards for

people's DNA and genetic information. If passed, these changes will damage people's trust in health, research and police uses of their DNA, perhaps for generations".

The Bill should be scrapped: it makes our research regime more amateur and puts people at greater risk from harm and unwanted interference.

There is NO need to redraft the definitions of personal data nor the definition of research nor the boundaries of legitimate interests. **If those changes go ahead, it will not only weaken safeguards by enabling more personal data to be labelled as "exempt" under research exemptions, but swathes of personal data will be removed outwith the definition entirely -- that relabelling will not change the nature of the data or its sensitivity or its threat model when distributed** or used-- it only serves to enable more exploitation of the UK public by industries (domestic, international or otherwise) without the public's ability to object or be informed and express preferences over being used as AI training datasets without our permission as an example. Rebranding personal data as research data, simultaneously weakens its protections set around the qualifications of the people who are accredited and qualified to handle it in safe ways. It reduces recourse to redress from malicious and opaque reuses; with effects for state and border security as well as individuals, for example in the case of children's DNA and biometrics. Overall, it makes our research environment more amateur and increases the risk for public interest researchers that public trust will be lost in the nature of their work.

In the UK we have already lost the protections of fundamental rights post-Brexit, because the government made the choice not to carry them over from EU Charter of Fundamental Rights into UK law. That means in particular a weakening of the rules to uphold respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity. In a world in which automated and machine-led decision making affects us more and more at speed and scale, where we are at constant threat of identity theft and financial fraud. The Bill fails to think Big or think for the future. Instead the Bill means digital identity can only be a state accredited ID to exercise housing and employment rights, but makes the frameworks for protecting those identities far weaker. Data protection laws are used to uphold our human rights and are not supposed to be designed to become a gateway to fraud at speed and scale, and mass exploitation in secret.

References

1. The DPDI Bill page https://bills.parliament.uk/bills/3430/publications
2. Defend Digital Me Second Reading Briefing | Data Protection and Digital Information Bill (2) https://defenddigitalme.org/wp-content/uploads/2023/04/Defend-Digital-Me-Second-Reading-Briefing-Data-Protection-and-Digital-Information-Bill-2-v1.5-1642023.pdf
3. The Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108) https://rm.coe.int/1680078b37
4. Open Rights Group led-coalition letter (March 7, 2023) https://www.openrightsgroup.org/press-releases/26-civil-society-groups-call-on-government-to-scrap-data-protection-and-digital-information-dpdi-bill/
5. The 2018 resolution from the International Conference of Data Protection and Privacy Commissioners https://edps.europa.eu/sites/default/files/publication/icdppc-40th_dewg-resolution_adopted_en_0.pdf
6. Defend Digital Me edTech and pupil data Briefing: November 2023 (WIP) v.1.9
7. Defend Digital Me. (2021). The Words We Use in Data Policy https://defenddigitalme.org/research/words-data-policy/