Public
Law
Project

Public Law Project House of Commons second reading briefing on the Data Protection and Digital Information (No.2) Bill

13 APRIL 2023

Summary and Recommendations

1. **The Data Protection and Digital Information (No.2) Bill would weaken important data protection rights and safeguards, making it more difficult for people to know how their data is being used, how decisions about them are being made, and weakening requirements on those who process data to consider the rights and interests of those their actions will affect.**

2. We live in an increasingly data-driven world. Social media giants, insurance companies and governments collect and process personal data on an ever-increasing scale. Relatedly, automated decision-making is also on the rise. Personal data is fed into automated systems, which are now used to make decisions that would traditionally have been made by human beings: decisions about immigration, welfare benefits, and policing, to name a few. While the use of big data and automated decision-making tools can result in quicker and more consistent outcomes, there is currently a lack of transparency and accountability in how they operate. As a consequence of this opacity and lack of protections, and because such decision-making can have huge consequences on people's lives, these systems carry a very real risk of discrimination and harm.

3. This Bill would mean sweeping changes to data protection law, including both the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR) - changes which prioritise economic growth and innovation over rights-protection, transparency and accountability. **While the Bill does not outright remove any of the current protections in data protection law, it weakens many of them to the extent that they will struggle to achieve their original purposes.**

4. This briefing for second reading in the House of Commons identifies a series of issues with the Bill regarding transparency, accountability and the wider context of increased delegated powers, including the deficiency in Parliamentary scrutiny they create. **PLP continues to be concerned that many of the proposals set out in the Bill will undermine how effectively people, especially those who are vulnerable or marginalised, can both protect and access their data in future.**

   PLP therefore recommends:

   - **That Members use the second reading to highlight the risks this Bill proposes to data protection provisions and the impact of this for marginalised groups who are often subject to increased scrutiny and decision-making by algorithmic technology.**
   - **That Members use the second reading to highlight the disconnect between the newly released UK Government AI White Paper, which states that the UK wishes to be 'world-leading' in its approach to AI regulation, and the simultaneous weakening of the existing protections and safeguards around the use of automated decision-making in UK law via the DPDI Bill.**
   - **Clause 7 should be removed from the Bill: it significantly limits people's ability to access information about how their personal data is being collected and used.**
   - **Clause 9 should be removed from the Bill: it curtails the right of the data subject to be informed about how their data is used.**
   - **Clause 11 should be removed, and Article 22 retained as a prohibition on solely automated decision-making.**

- **Changes to Clause 17 that mean impact assessments are only required for 'high risk processing' should be removed from the Bill.**

- **That Members question why Clauses 5 and 6 of the Bill contain broad and unspecified powers for the Secretary of State to amend the UK GDPR via statutory instrument, without scrutiny by Parliament.**

- **Clause 106 should be narrowed to allow ministers to make provisions that are consequential on the Act only where necessary, as recommended by the Delegated Powers and Regulatory Reform Committee.**

Introduction: A data protection shortfall

5. Currently there is insufficient protection, overcollection, and overprocessing of data by government bodies. While the increase in data collection will affect all of our lives, it has long been recognised that the effect will not effect us all equally. Already marginalised groups – such as those arriving by small boats from France, and individuals in the welfare system – are at a greater risk of harm from the surge in data collection, processing and by use of automated decision making by government. Last year, the Justice and Home Affairs Committee published its report, 'Technology Rules? The advent of new technologies in the justice system' (March 2022), which offers examples of data-based decision-making, including some provided by Public Law Project - such as the Home Office's sham marriage algorithm, which helps determine whether an intended marriage should be investigated as a 'sham' (para. 127). The Committee stressed that without transparency, there is no accountability for when things go wrong. It has been recognised that the surge in data collection, processing, and use of automated systems by government does not affect all communities equally. Professor Karen Yeung highlighted that risk assessment tools are not being developed to "identify insider trading or who is going to commit the next kind of corporate fraud… we are turning it into prediction tools about poor people."

6. The watering down of rights protections proposed by this Bill poses additional risks for us all but more so for marginalised groups, as they are often the individuals who are subject to increased surveillance, scrutiny and decision-making by algorithmic technology. Without robust data protections, unfair, disproportionate and unlawful practices could leave marginalised individuals exposed to even higher levels of intrusive data collection and processing, exposing them to significant harm.

Parliamentarians will wish to be mindful of these risks as the Bill weakens existing data protection provisions which benefit us all and which are of particular importance to already marginalised groups.

Clause 7 and 9: Reduced access to personal data and knowledge about how it is used

7. Transparency around government use of big data and automated decision-making tools has intrinsic value; people have a right to know how they are being governed. Transparency has consequential value, too. It facilitates democratic consensus-building about the appropriate use of new technologies, and it is a prerequisite for holding government (and other influential entities) to account when things

go wrong.[1] However, Clauses 7 and 9 would seriously limit people's ability to access information about how their personal data is being collected and used. This includes limiting access to information about automated decision-making processes to which they are subject.

The problem with Clause 7:

A data subject is someone who can be identified, directly or indirectly, by personal data such as a name, an ID number, location data, or information relating to their physical, economic, cultural or social identity.

Under existing laws, data subjects have a right to request confirmation as to whether their personal data is being processed by a controller, to access that personal data, and to obtain information about how it is being processed as per Article 15 of the UK GDPR. Section 53 of the DPA and Article 12 of the UK GDPR state that a controller can only refuse a request from a data subject if it is 'manifestly unfounded or excessive'.

There are three main ways in which Clause 7 significantly limits people's ability to access information about how their personal data is being collected and used:

First, it would lower the threshold for refusing a request to 'vexatious or excessive'. This is an inappropriately low threshold given the nature of a data subject access request, namely, a request by an individual for their own data.

Second, Clause 7 would insert a new, mandatory list of considerations for deciding whether a request is vexatious or excessive. This includes vague considerations such as 'the relationship between the person making the request (the "sender") and the person receiving it (the "recipient")'.

Third, the proposed changes to Article 12 and section 53 are potentially open to a very wide interpretation – while examples of what might be a vexatious request are provided, what amounts to excessive is completely unchartered legal terrain and could be relied upon more often by public bodies to refuse data subject access requests – thereby unfairly limiting people's access to their own data.

PLP recommends that this Clause be removed from the Bill.

The problem with Clause 9:

Currently, data subjects have a right to be informed about the collection and use of their personal data enshrined in Articles 13 and 14 of the UK GDPR. Clause 9 would seriously restrict this right and should be resisted.

Sometimes, a data controller will want to use personal data for additional purposes, other than those

[1] Public Law Project has conducted comparative and theoretical research on algorithmic transparency. See 'Executable versions: an argument for compulsory disclosure, Part One' (3 August 2022), Digital Constitutionalist, available at https://digi-con.org/executable-versions-part-one/.

for which it was originally collected. Under Article 13(3), a data subject has a right to know about this. PLP strongly opposes the inclusion of Clause 9 in the Bill because it would place new limitations on this right in cases where the additional purposes are for 'scientific or historical research', 'archiving in the public interest' or 'statistical purposes'. These terms are very vague and open to wide interpretation. Scientific research is defined as 'any research that can reasonably be described as scientific, whether publicly or privately funded, including processing for the purposes of technological development or demonstration, fundamental research or applied research'. This could enable private companies carte blanche to use personal data for the purposes of developing new products without needing to inform the data subject.

The effect of such changes to Article 13 are likely to mean that data subjects are less likely to receive information about the processing of their personal data for purposes other than those for which it was collected.

Therefore, PLP recommends that Clause 9 is removed from the Bill.

Clause 11: Reduced protections against solely automated decision-making

8. Automated decision-making is increasingly used in a range of high-stakes contexts, including immigration, policing, and welfare benefits. The particular risks and problems that arise in relation to solely automated decision-making are well-accepted. It is not only that human oversight can help to guard against a machine's mistakes and mitigate risks such an encoded bias; there is also a concern about human dignity, and a sense that decisions about human beings should not be made solely on the basis of a data profile.

9. The Government data consultation response acknowledges that, for respondents, 'the right to human review of an automated decision was a key safeguard'. PLP has written about the importance of the prohibition on solely automated decision-making for Prospect magazine: 'Human oversight is crucial for automated decision-making. So why is it being reduced?' (6 December 2021). Despite the government acknowledging the importance of human review in an automated decision, if implemented, Clause 11 would mean that solely automated decision-making is permitted in a wider range of contexts.

The problem with Clause 11:

Currently, Sections 49 and 50 DPA and Article 22 of the UK GDPR provide a right not to be subject to a decision based solely on automated processing, with some narrow exemptions.

Clause 11 would mean that solely automated decision-making would be allowed, unless it is a 'significant decision' and it is based on particular types of personal data[2] - in which case, specified conditions must be met. The conditions are that the automated decision-making is required or authorised by law or the data subject has explicitly consented. As part of this change, solely

[2] The special categories of personal data under Article 9(1) are those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

automated decisions that do not involve ‘sensitive personal data’ are now permissible. Automated decisions can have significant effects on people’s lives without involving sensitive personal data. Examples include decisions concerning access to financial products, educational decisions like the A-level algorithm scandal, or the SyRI case in the Netherlands where innocuous datasets such as household water usage were used to accuse individuals of benefit fraud.

It is also unclear what will meet the threshold of a ‘significant decision’. The Charity Big Brother Watch has identified Local Authorities which use predictive models to identify children deemed at high risk of committing crimes and to include them on a database. Would a decision to include someone on a database meet the threshold of a significant decision?

The impact of Clause 11:

These changes would mean that solely automated decision-making is permitted in a much wider range of contexts. It is especially concerning given that many high-impact algorithmic decisions do not involve processing of special categories of personal data which is a narrow and specific category.

Further, the proposed changes would mean that Article 22 will no longer be cast as a right not to be subject to solely automated decision-making, but rather as a restriction on solely automated decision-making.

PLP recommends that Article 22 is retained as a prohibition on solely automated decision-making and that Clause 11 is removed from the Bill.

Clause 17: Watered-down impact assessments

10. Data Protection Impact Assessments (DPIAs) are currently required under Article 35 of the UK GDPR and are essential for ensuring that organisations do not deploy – and individuals are not subjected to – systems that may lead to unlawful, rights-violating or discriminatory outcomes. The Government data consultation response noted that '[t]he majority of respondents agreed that data protection impact assessments requirements are helpful in identifying and mitigating risk and disagreed with the proposal to remove the requirement' to undertake them. However, under Clause 17, the requirement to perform an assessment would be seriously diluted.

The problem with Clause 17:

Under Clause 17, the minimum requirements of an impact assessment would be lowered. Instead of a systematic description of the processing operations and purposes, the controller would only be required to summarise the purposes of the processing. This would mean that limited consideration is given to how the processing works and the risks this might pose.

Instead of a proportionality assessment, under this provision, the controller would only be required to consider whether the processing is necessary for the stated purposes. Proportionality is the legal test for deciding whether an infringement on human rights (including the right not to be discriminated against) is justified and lawful. By limiting assessment requirements to include only whether the processing is necessary – not whether it is proportionate – Clause 17 dilutes the important safeguard of DPIAs.

Bridges, a 2020 challenge to South Wales Police's (SWP's) use of automated facial recognition (AFR) technology, demonstrates the importance of DPIAs in ensuring that policies properly assess the risks to the rights of individuals and therefore comply with the law.

In this case, the Court of Appeal found that because SWP's DPIA was written on the basis that Article 8 of the European Convention on Human Rights was not infringed by its use of AFR technology, when in fact it was, the DPIA was not compliant and thus its policy was unlawful.

It is worrying, therefore, that the requirement to thoroughly consider the risks to the rights and freedoms of data subjects, and the proportionality of processing is to be watered down by Clause 17. Without rigorous risk and impact analysis, disproportionate and therefore discriminatory processing could be carried out, before the possibility of harm is evaluated and mitigated.

PLP do not consider these changes necessary or desirable, and they should be removed from the Bill.

Clause 5, 6, 11 and 106: increased delegated powers mean less Parliamentary scrutiny

11. The Bill contains a number of wide delegated powers giving the Secretary of State the power to amend the UK GDPR via statutory instrument. The Government has said that the UK GDPR's key elements remain sound and that it wants to continue to offer a high level of protection for the public's data[3] but this is no guarantee against significant reforms being brought in through a process which eludes parliamentary scrutiny. Proposed changes to the UK GDPR should be contained on the face of the Bill where they can be debated and scrutinised properly via the primary legislation process. As it stands, key provisions of the UK GDPR are to be subsequently amended via statutory instrument, an inappropriate legislative process that affords much less scrutiny and debate, if debates are held at all.

The problem with these Clauses:

Clause 5

The UK GDPR contains a finite set of lawful bases on which personal data can be processed. The protections provided by the UK GDPR currently could be easily undermined if the situations in which a data processor can lawfully process data were too numerous.

Clause 5(2((b) of the Bill adds a provision allowing personal data to be processed on the basis of a recognized legitimate interest and Clause 5(4), along with Schedule 1, sets out the conditions which must be met if processing is to be considered necessary for the purposes of a recognized legitimate interest. Clause 5(4) further makes provision for the Secretary of State via statutory instrument to add to or vary those conditions.

[3] https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#:~:text=The%20government%20launched%20its%20consultation,the%20UK's%20National%20Data%20Strategy.

Clause 6

Clause 6(5) of the Bill inserts Article 8A which allows the Secretary of State via statutory instrument to add other conditions in which further processing of personal data, beyond the original purpose for which the data was collected, is lawful.

If there are other circumstances in which the Government thinks it should be lawful to process personal data, or carry out further processing beyond the original purpose, those should be contained within the Bill, rather than left to ministers to determine at a later date without scrutiny.

Clause 11

The UK GDPR treats a solely automated decision as one without 'meaningful human involvement'. The public is protected from being subject to solely automated decision-making where the decision has legal or 'similarly significant effects'. Clause 11(1) of the Bill inserts Article 22D(1) which allows the Secretary of State to make regulations which deem a decision to have involved meaningful human involvement, even if there was not active review by a human decision-maker. Article 22D(2) similarly allows the Secretary of State to make regulations to determine whether a decision made had a 'similarly significant effect' to a legal effect.[4]

For example, in summer 2021 there was the A-level algorithm grading scandal, which PLP wrote about for the UKCLA: 'Model students: why Ofqual has a legal duty to disclose the details of its model for calculating GCSE and A level grades' (July 2022). If something like this was to reoccur, under this new power a minister could lay regulations stating that the decision to use an algorithm in grading A-levels was not a decision with 'similarly significant effects'.

22D(4) also allows the Secretary of State to add or remove, via regulations, any of the listed safeguards for automated decision-making.

Furthermore, if the minister wishes to amend or remove safeguards on automated decision-making this should also be specified in the Bill not left to delegated legislation.

Clause 106

Clause 106 of the Bill is a widely drafted Henry VIII power that gives the Secretary of State the power to 'make provision that is consequential on any provision made by this Act'. The Delegated Powers and Regulatory Reform Committee have stated that powers which make consequential provision 'inherently lack a clear definition to its scope' and that consequential changes should 'therefore be restricted by some type of objective test of 'necessity'.[4] In the Bill, what is 'consequential' is left to the subjective judgment of ministers.

We recommend that Clause 106 is narrowed to allow ministers to make provisions that are consequential on the Act only where necessary.

[4] DPRRC (2017–19), 3rd Report, HL Paper 22, paras. 71, 72, 74.

Contact

Alex Sinclair
Research Fellow
a.sinclair@publiclawproject.org.uk

Mia Leslie
Research Fellow
m.leslie@publiclawproject.org.uk

Isabelle Agerbak
Policy and Parliamentary Lead
i.agerbak@publiclawproject.org.uk

Public Law Project is an independent national legal charity.

We are researchers, lawyers, trainers, and public law policy experts.

Our aim is to make sure state decision-making is fair and lawful and that anyone can hold the state to account.

For over 30 years we have represented and supported people marginalised through poverty, discrimination, or disadvantage when they have been affected by unlawful state decision-making.

Public Law Project contributes and responds to consultations, policy proposals, and legislation to ensure public law remedies, access to justice, and the rule of law are not undermined.

We provide evidence to inquiries, reviews, statutory bodies, and parliamentary committees in relation to our areas of expertise, and we publish independent research and guides to increase understanding of public law.

Public Law Project's research and publications are available at:

www.publiclawproject.org.uk/resources-search/