Public Law Project

Public Law Project House of Commons Report stage briefing on the Data Protection and Digital Information Bill

November 2023

Summary and Recommendations

1. **The Data Protection and Digital Information 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 affecting 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. Automated decision-making is also on the rise. Personal data is fed into and trains automated, algorithmic and artificial intelligence (AI) systems, which are now used to make decisions that would traditionally have been made by human beings: decisions about education, health and social care, immigration, and welfare 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 – resulting in a corresponding lack of transparency in how high-impact data driven decisions are being made. Such opaqueness makes it difficult to prevent unfair decisions being made in the first place and limits the ability to hold decision makers accountable for those decisions.

3. The Prime Minister has spoken extensively in recent weeks and months about the transformative power of AI, and the risks attendant on this transformation; he has set out his intention to make the UK "a global leader in safe AI".[1] This intention, however, is undermined by this Bill. **Data is what powers AI – it is used to build and train AI systems and forms the raw material by which AI systems derive insights and produce relevant outputs**. For that reason, **a robust data protection framework is essential to ensuring the safe development and use of AI.** Protections which ensure that individuals can get information about how their data is being used, that safeguard them from solely automated decision-making in instances where the decision has significant effects, and requires data controllers to thoroughly assess the impact of data protection risks of a project, are all essential to understanding and assessing the operation and impact of AI systems. It is difficult to feel confident in the Government's promises to mitigate the risks posed by the AI revolution, given that it is simultaneously trying to weaken each of these vital protections.

4. 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 rather than seeking to achieve a healthy balance between the two. **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.**

5. This briefing for Report stage in the House of Commons identifies a series of issues with the

[1] Prime Minister's speech on AI: 26 October 2023, https://www.gov.uk/government/speeches/prime-ministers-speech-on-ai-26-october-2023.

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 can both protect and access their data in future.**

PLP therefore recommends:

- **Clause 8 (vexatious or excessive requests by data subjects) 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 12 (automated decision-making) should be amended so that it does not weaken existing protections around automated decision-making.**
- **Clause 18 (assessment of high risk processing) should be removed from the Bill: it means impact assessments are only required for 'high risk processing'.**
- **Clauses 5 (lawfulness of processing) and 6 (the purpose limitation) should be removed from the Bill: these are broad and unspecified powers which would allow the Secretary of State to amend the UK GDPR via statutory instrument, without scrutiny by Parliament.**
- **Clause 114 (power to make consequential amendments) 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.**

Clause 8: Reduced access to personal data and knowledge about how it is used

6. Transparency around government use of personal data has intrinsic value; people have a right to know how their data is being used and how it influences the way they are governed. Transparency has consequential value, too. It facilitates democratic consensus-building about the appropriate use of data and new technologies, and it is a prerequisite for holding government (and other influential entities) to account when things go wrong.[2] However, Clause 8 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 8:

A data subject is someone who can be identified, directly or indirectly, by personal data such as a

[2] 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/.

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 ("Subject Access Requests"). 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 8 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 from 'manifestly unfounded or excessive' 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 8 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")'. The very fact that the recipient holds data relating to the sender means that there is some form of relationship between them (e.g. employer/employee, service provider/service user).

Third, the weakening of an individual's right to obtain information about how their data is being collected, used or shared is particularly troubling given the simultaneous effect of the provisions in Clause 10, which would mean data subjects are less likely to be informed about how their data is being used for additional purposes, other than those for which it was originally collected in cases where the additional purposes are for 'scientific or historical research', 'archiving in the public interest' or 'statistical purposes'. Together, the two clauses mean that an individual is less likely to be *proactively* told about how their data is being used, whilst it is harder to access information about their data when requested.

At Committee stage, the Minister claimed that the new parameters 'are not intended to be reasons for refusal' but rather are to 'give greater clarity than there has previously been'.[3] However, as raised by Dr Jeni Tennison in her oral evidence to the Committee, the Impact Assessment for the Bill indicates that a significant proportion of the savings predicted would come from lighter burdens on organisations in dealing with Subject Access Requests as a result of this Clause.[4] This suggests that while the Government claims that this clause is a 'clarification', it is in fact intended to weaken obligations on controllers, and correspondingly weaken the rights of data subjects.

PLP recommends that this Clause be removed from the Bill (see Clause 8, Amendment 1 in

[3] Sir John Whittingdale's comments in Public Bill Committee on 16 May 2023, House of Commons Official Report Public Bill Committee (Bill 265), https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf, at column 114 and 113 respectively.
[4] Dr Jeni Tennison's comments in Public Bill Committee on 10 May, House of Commons Official Report Public Bill Committee (Bill 265), https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf, at column 28; Impact Assessment for the Data Protection and Digital Information Bill, https://publications.parliament.uk/pa/bills/cbill/58-03/0265/DataProtectionandDigitalInformationBillImpactAssessment.pdf, para 147.

Appendix). If this amendment is not accepted, PLP recommends an alternative amendment (see Clause 8, Amendment 2 in Appendix) requiring the provision of reasons detailing why the request is considered vexatious or excessive.

Subject Access Requests: a case study

Catt v. the United Kingdom[5]

Mr Catt was a 94 year old peace activist who had been a regular attendee at public demonstrations since 1948.

In 2010, as the result of a subject access request, Mr Catt learned that the police had collected and retained his personal data, which included his political views, on an "extremism database". This was despite the fact that Mr Catt had never been convicted of any offense, had no violent history and was someone for whom violent criminality was viewed as being "a very remote prospect indeed".

The case raised significant concerns about the power of police to surveil peaceful protesters and individuals in public places and retain personal information about them, as well as the potential chilling effect on legitimate public protest.

In 2019, the European Court of Human Rights determined that the retention of his data on the database amounted to an interference with Mr Catt's Article 8 rights to privacy.

The case demonstrates that existing Subject Access Request provisions, and the ability they confer on individuals to obtain the information held on them are vital to identifying unlawful use of data, and the dangers of placing additional barriers to their use.

Clause 12: Reduced protections against solely automated decision-making

10. Automated decision-making is increasingly used by Government departments in a range of high-stakes contexts, including about education, health and social care, immigration, and welfare as well as by private actors in contexts such as financial services. The particular risks and problems that arise in relation to solely automated decision-making are well-accepted.[6] Human oversight can help to guard against a machine's errors, mitigate risks such as encoded bias and ensure that there are robust and rational reasons behind a

[5] Catt v United Kingdom (43514/15) (2019) 69 E.H.R.R. 7.

[6] Information Commissioner's Office, Guidance on 'What is automated individual decision-making and profiling?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/automated-decision-making-and-profiling/what-is-automated-individual-decision-making-and-profiling/#id4.

decision.[7]

11. The Government data consultation response acknowledges that, for respondents, 'the right to human review of an automated decision was a key safeguard'.[8] Despite the government acknowledging the importance of human review in an automated decision, if implemented, Clause 12 would reverse the presumption against solely automated decision making, permitting solely automated decision-making in a much wider range of contexts.

The problem with Clause 12:

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 12, in reversing the presumption against solely automated decision making, would mean that solely automated decision-making would be allowed, unless it is a 'significant decision' and is based on special categories of personal data[9] - 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 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.[10]

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.[11] Whether a decision to include someone on a database meets the threshold of a significant decision is simply not known leading to uncertainty for both decision makers and data subjects.

---

[7] Tatiana Kazim, 'Human oversight is crucial for automated decision-making. So why is it being reduced?' in Prospect magazine (December 2021), https://www.prospectmagazine.co.uk/politics/38195/human-oversight-is-crucial-for-automated-decision-making.-so-why-is-it-being-reduced.

[8] Department for Digital, Culture, Media and Sport, Data: a new direction - government response to consultation (23 June 2022), Rights in relation to automated decision-making and profiling (Article 22), https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation.

[9] 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.

[10] For more information about the Dutch use of the SyRi system and its use of innocuous datasets, see Netherlands Helsinki Committee, Bring Human Rights Home: A Story from the Netherlands, https://www.nhc.nl/bring-human-rights-home-a-story-from-the-netherlands/; Lighthouse Reports, The Algorithm Addiction, https://www.lighthousereports.com/investigation/the-algorithm-addiction/.

[11] Big Brother Watch, 'Poverty Panopticon: the hidden algorithms shaping Britain's welfare state' (20 July 2021), https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/Poverty-Panopticon.pdf.

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 the restrictions on automated decision-making in Clause 12 new Article 22B apply to all categories of personal data, not just 'sensitive personal data'. PLP has drafted an amendment to this effect (see Clause 12, Amendment 1 in Appendix).

PLP has also drafted an amendment (see Clause 12, Amendment 2 in Appendix) which would not only maintain the current level of protection, but improve it, so that public authorities which use automation even partially to make decisions must ensure that safeguards for the data subjects rights and freedoms are in place.

Clause 18: Watered-down impact assessments

12. 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.[12] However, under Clause 18, the requirement to perform an impact assessment would be seriously diluted.

The problem with Clause 18:

Under Clause 18, 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.

Currently, impact assessments are required to contain an assessment of both 'the necessity and proportionality' of the processing in relation to the purposes. Clause 18 refers instead to a requirement to assess whether the processing is 'necessary' for those purposes. We would welcome clarification that the term 'necessary' in this context is intended to retain the legal meaning of proportionality (in line with existing case law).

Retaining the requirement around assessing proportionality is important to avoid a reduction in the

[12] Department for Digital, Culture, Media and Sport, Data: a new direction - government response to consultation (23 June 2022), Removal of data protection impact assessments, https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation.

standards of impact assessments. We therefore recommend (see Clause 18, Amendment 1 in Appendix) retaining the previous wording that refers to both necessity and proportionality, to avoid ambiguity or the suggestion that the assessment requirement is to be watered down.

If our amendment is not adopted, we urge MPs to seek clarity that an assessment of proportionality is to be inferred within the requirement to assess whether the processing is necessary.

Without rigorous risk and impact analysis of how data processing might risk the rights of data subjects, disproportionate and discriminatory processing could be carried out, before the possibility of harm is thoroughly evaluated and mitigated. This would enable such processing to occur, and the impact would be felt by individuals. 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 18.

PLP do not consider these changes necessary or desirable, and they should be removed from the Bill. PLP has drafted an amendment which would maintain the current requirements for data protection impact assessments (see Clause 18, Amendment 1 in Appendix).

PLP has also drafted an amendment which would not only maintain the current requirements, but also introduce new obligations on public authorities to publish data protection impact assessments they carry out (see Clause 18, Amendment 2 in Appendix).

Data Protection Impact Assessments: a case-study

The *Bridges* case[13]

In 2017 and 2018, the South Wales Police Force piloted a new facial recognition software called AFR locate. They would mount CCTV cameras on police cars, and on posts and scan the face of anyone who passed into its field of view and compare them with digital images of persons on a watchlist. The software would then assign an estimated probability that the images were a match and refer likely matches to a reviewing officer. If the officer identified someone as a possible match, they would decide whether the person should be stopped and searched or arrested.

One person who passed through the facial scanner's field of view was Edward Bridges. He is a civil liberties campaigner in Cardiff. In the days preceding Christmas 2017, he visited a busy shopping centre where the police were trialing the software. And in March 2018, he attended a protest outside of the Cardiff Arms Fair. Edward Bridges, with the support of Liberty, challenged the use of this software and was successful on three grounds, one being that the DPIA, as required by section 64 DPA 2018, was inadequate because it was written on the basis that Article 8 was not infringed (when it was found to be).

[13] *R (Bridges) v CC South Wales* [2020] EWCA Civ 1058.

The Court of Appeal held that had the DPIA of the software been carried out correctly, then the police would have considered whether the discretion afforded to individual officers to interfere with individuals' privacy was so wide as to not be in accordance with the law and that that breached Article 8 of the ECHR. And, accordingly that the human rights violation might have been avoided. Specifically, the court held that the police had failed to properly envisage measures to address the risks arising from the unlawfully wide discretion being given to officers in its purported DPIA.

Clause 18 would water down the requirement to thoroughly consider the risks to the rights and freedoms of data subjects. The Bridges case demonstrates that existing DPIA requirements, when adhered to, can prevent the violation of individuals' fundamental rights by the State.

Clause 5, 6, 12 and 106: increased delegated powers mean less Parliamentary scrutiny

13. 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[14] but this is no guarantee against significant reforms being brought in through a process which eludes full 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 can 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 Clauses 5, 6, 12 and 106:

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 recognised 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 recognised legitimate interest. Clause 5(4) further makes provision for the Secretary of State via statutory instrument to add to or vary those conditions.

[14] Department for Digital, Culture, Media and Sport, Data: a new direction - government response to consultation (23 June 2022), 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 full Parliamentary scrutiny.

Clause 12

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 12(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.[15] 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'.

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

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.

PLP has drafted an amendment which would limit the Secretary of State's power, so that they may add safeguards, but cannot vary or remove those in the new Article 22D as they stand when the legislation comes into force (see Clause 12, Amendment 3 in Appendix).

Clause 114

Clause 114 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

[15] Jack Maxwell and Joe Tomlinson, 'Model students: why Ofqual has a legal duty to disclose the details of its model for calculating GCSE and A level grades' (July 2022), https://ukconstitutionallaw.org/2020/07/28/jack-maxwell-and-joe-tomlinson-model-students-why-ofqual-has-a-legal-duty-to-disclose-the-details-of-its-model-for-calculating-gcse-and-a-level-grades/.

restricted by some type of objective test of 'necessity'.[16] In the Bill, what is 'consequential' is left to the subjective judgment of ministers.

We recommend that Clause 114 is narrowed to allow ministers to make provisions that are consequential on the Act only where necessary.

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

Contact

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

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

Joseph Summers
Research Assistant
j.summers@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/