Public Law Project

Public Law Project briefing for the House of Lords Committee Stage of the Data Protection and Digital Information Bill

January 2024

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 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 Committee stage in the House of Lords 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 can both protect and access their data in future.**

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

PLP therefore recommends:

- **Clause 9 (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, when taken in conjunction with Clause 9, is likely to mean that data subjects are less likely to receive the information they requested about their own data. Assurances should be provided that Clause 12 (searches in response to data subjects' requests) will not reduce or lower the requirement to search for data subjects' information. If such assurances are not meaningfully provided, the clause should be removed.**

- **Clause 14 (automated decision-making) should be amended so that it does not weaken existing protections around automated decision-making.**

- **The adoption of a new Clause 15 which would put a legislative obligation on public bodies using algorithmic tools to publish reports under the Central Digital and Data Office (CDDO) and Centre for Data Ethics and Innovation (CDEI)'s Algorithmic Transparency Recording Standard.**

- **Clause 20 (assessment of high risk processing) should be removed from the Bill: it means impact assessments are only required for 'high risk processing'.**

- **Clause 128 and Schedule 11 (power to require information for social security purposes) should be removed from the Bill. The power is extremely and unprecedentedly wide, disapplying the previous restriction which limited the DWP to undertaking fraud checks on a claimants account only where there is already suspicion of fraud.**

- **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 150 (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 9: 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.[23] However, Clause 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 9:

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 ("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 9 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 9 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 in the House of Commons 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

[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/.

been'.[4] 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.[5] 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 9 be removed from the Bill (see Clause 9, Amendment 1 in the Appendix).

In the alternative, PLP recommends an amendment requiring the provision of reasons detailing why the request is considered vexatious or excessive (see Clause 9, Amendment 2 in the Appendix).

Subject Access Requests: a case study

Catt v. the United Kingdom[6]

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 right 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.

[4] 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.
[5] 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.
[6] Catt v United Kingdom (43514/15) (2019) 69 E.H.R.R. 7.

Clause 12: Searches in response to data subjects' requests

7. This new clause is said to confirm that, in responding to subject access requests, controllers are only required to undertake reasonable and proportionate searches for personal data and other information.

8. At report stage and third reading in the House of Commons, the clause was explained as being introduced to specifically "address the loss of the EU general principle of proportionality at the end of 2023 as a result of the Retained EU Law (Revocation and Reform) Act 2023",[7] and codify the principle currently set out in domestic case law.

9. Clause 12 does not provide a definition for 'reasonable and proportionate searches' but when introducing the amendment Sir John Whittingdale suggested that a search for information may become unreasonable or disproportionate when the information is of "low importance or of low relevance to the data subject".[8]

10. These considerations are a deviation from those provided in the Information Commissioner's Office (ICO) guidance on rights of access, which states that when determining whether searches may be unreasonable or disproportionate, the data controller must consider the circumstances of the request, any difficulties involved in finding the information, and the fundamental nature of the right of access.[9]

The problem with Clause 12:

Whilst apparently introduced to clarify the current position, some of the accompanying communications have indicated a potential intention on the part of Government to weaken the existing position making it less likely that data subjects will receive information requested about their own data. This would be particularly concerning when taken in conjunction with Clause 9 (which lowers the threshold for data controllers to be able to refuse subject access requests[10]).

First, the considerations suggested at report stage and third reading for determining when a search may be unreasonable or disproportionate departs from existing ICO guidance. This is exacerbated by the fact that the example provided of what is 'important or relevant' to the data subject is to be made by the data controller, who is not personally impacted by the disclosure or non-disclosure of the requested information.

[7] Sir John Whittingdale, HC Deb Wednesday 29 November, Data Protection and Digital Information Bill, volume 741, column 873, https://hansard.parliament.uk/Commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill#.

[8] Sir John Whittingdale, HC Deb Wednesday 29 November, Data Protection and Digital Information Bill, volume 741, column 873, https://hansard.parliament.uk/Commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill#.

[9] Information Commissioner's Office, UK GDPR guidance and resources, 'How do we find and retrieve the relevant information?', https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/how-do-we-find-and-retrieve-the-relevant-information/.

[10] See PLP's briefing on Clause 9, vexatious or excessive requests by data subjects.

Second, we continue to be concerned about the incongruity between the impact assessment for the Bill and Government's claims that the new provisions in relation to subject access requests are for 'clarification' only. The impact assessment indicates that a significant proportion of the savings predicted would come from lighter burdens on organisations in dealing with subject access requests.[11] This suggests that while the Government claims that Clauses 9 and 12 are a 'clarification' of the existing position, they are in fact intended to weaken obligations on controllers to respond to and search for the information requested under subject access requests, and correspondingly weaken the rights of data subjects.

Government must make meaningful assurances that Clause 12 (searches in response to data subjects' requests) will not reduce or lower the requirement to search for data subjects' information.

If such assurances are not provided, or do not provide sufficient confidence, the clause should be removed.

Clause 14: Reduced protections against solely automated decision-making

11. 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.[12] 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 decision.[13]

12. The Government data consultation response acknowledges that, for respondents, 'the right to human review of an automated decision was a key safeguard'.[14] Despite the government acknowledging the importance of human review in an automated decision, if implemented,

[11] 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.

[12] 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.

[13] 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.

[14] 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.

Clause 14 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 14:

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 14, 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[15] - 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.[16]

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.[17] 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.

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 14 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 14, Amendment 1 in the Appendix).

[15] 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.

[16] 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/.

[17] 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.

PLP has also drafted an amendment 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 (see Clause 14, Amendment 2 in the Appendix).

A new Clause 15: Transparency in public use of algorithmic tools

13. The Central Digital and Data Office (CDDO) and Centre for Data Ethics and Innovation (CDEI) launched the Algorithmic Transparency Recording Standard (ATRS) in November 2021. The idea for the ATRS arose from a recommendation by the CDEI that "the UK Government should place a mandatory transparency obligation on public sector organisations using algorithms to support significant decisions affecting individuals".[18] It is intended to help public sector organisations provide clear information about the algorithmic tools they use, how they operate and why they're using them.

14. The ATRS is a promising initiative that could go some way to addressing the current transparency deficit around the use of algorithmic and AI tools by public authorities. Organisations are encouraged to submit reports about each algorithmic tool that they are using that falls within the scope of the Standard.[19] However, engagement has not been made mandatory and only seven transparency reports have been submitted. Many of the key government departments using tools that fall within the scope of the ATRS, such as the Home Office and Department for Work and Pensions,[20] have never submitted a report.[21]

15. PLP is concerned that the lack of engagement with the ATRS from public authorities reduces its ability to fulfil its aim of becoming a 'cross-government standard for algorithmic transparency' as set out in the Government's National Data Strategy, [22] and as reiterated in the National AI Strategy.[23]

16. In March 2022, the House of Lords Justice and Home Affairs Committee recommended that "full participation in the Algorithmic Transparency [Recording] Standard collection should become mandatory, and its scope extended to become inclusive of all advanced algorithms used in the

[18] Cabinet Office, UK government publishes pioneering standard for algorithmic transparency: (29 November 2021): https://www.gov.uk/government/news/uk-government-publishes-pioneering-standard-for-algorithmic-transparency.
[19] Central Digital and Data Office and Centre for Data Ethics and Innovation, Guidance for organisations using the Algorithmic Transparency Recording Standard (5 January 2023), https://www.gov.uk/government/publications/guidance-for-organisations-using-the-algorithmic-transparency-recording-standard.
[20] See Public Law Project's Tracking Automated Government (TAG) Register for further information on the use of automation, algorithms and AI by public authorities. Public Law Project, Tracking Automated Government 'TAG' Register (9 February 2023) http://trackautomatedgovernment.org.uk/.
[21] Central Digital and Data Office and Centre for Data Ethics and Innovation, Algorithmic Transparency Reports (13 January 2023), https://www.gov.uk/government/collections/algorithmic-transparency-reports.
[22] Department for Digital, Culture, Media and Sport, UK National Data Strategy (9 September 2020), https://www.gov.uk/government/publications/uk-national-data-strategy.
[23] Department for Science, Innovation and Technology, Office for Artificial Intelligence, Department for Digital, Culture, Media & Sport, and Department for Business, Energy & Industrial Strategy, National AI Strategy (22 September 2021), https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version.

application of the law that have direct or indirect implications for individuals".[24]

17. At House of Commons Public Bill Committee stage Stephanie Peacock, Labour MP and then opposition spokesperson for the Bill, tabled a new Clause 9 entitled 'transparency in use of algorithmic tools'. The clause aimed to put a legislative obligation on Government departments, public authorities and Government contractors using algorithmic tools to process personal data to use the ATRS.[25]

18. PLP supported Stephanie Peacock MP's clause and endorses the recommendation of the House of Lords Justice and Home Affairs Committee. We propose an equivalent Clause 15 updated to reflect the current terminology for the standard. This puts a legislative obligation on public bodies using algorithmic tools that have a significant influence on a decision-making process with direct or indirect public effect, or directly interact with the general public, to publish reports under the ATRS (see New Clause 15, Alternative 1 in the Appendix).

19. Sir John Whittingdale, Minister for Data and Digital Infrastructure and spokesperson for the Bill in the Commons, rejected the clause proposed by Stephanie Peacock MP on the basis that the "algorithmic transparency recording standard is still a maturing standard that is being progressively promoted and adopted". Stating that its evolving nature means that "enshrining the standard into law at this point of maturity could hinder the ability to ensure that it remains relevant in a rapidly developing technology field".

20. Should PLP's new Clause 15 (Alternative 1) be rejected, we are recommending an alternative amendment (Alternative 2) to reflect the Government's concerns. We propose a new Clause 15 which reflects both these concerns and the Government's commitment to algorithmic transparency. PLP's new Clause 15 would require the Secretary of State to introduce a compulsory transparency reporting requirement (such as the ATRS) but only when she considers it appropriate to do so. In support of transparency, the new Clause 15 would also, for as long as the Secretary of State considers making the ATRS compulsory inappropriate, require the Secretary of State to regularly explain why and to keep her decision under continual review (see New Clause 15, Alternative 2 in the Appendix).

PLP recommends that the Algorithmic Transparency Recording Standard (or equivalent) be made compulsory (see New Clause 15, Alternative 1 in the Appendix).

In the alternative, PLP recommends that the Secretary of State be required to regularly provide reasons for not making such a standard compulsory and to keep that decision under continual review (see New Clause 15, Alternative 2).

Clause 20: Watered-down impact assessments

21. Data Protection Impact Assessments (DPIAs) are currently required under Article 35 of the UK

[24] House of Lords, Justice and Home Affairs Committee, 'Technology rules? The advent of new technologies in the justice system' (30 March 2022), HL Paper 180, page 46.
[25] House of Commons, Public Bill Committee (Bill 265), Data Protection and Digital Information (No. 2) Bill (23 May 2023), New Clause 9, 284, https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf.

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.[26] However, under Clause 20, the requirement to perform an impact assessment would be seriously diluted.

The problem with Clause 20:

Under Clause 20, 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 20 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 encompass both necessity and proportionality (in line with existing standards and case law).

Retaining the requirement around assessing proportionality is important to avoid a reduction in the standards of impact assessments. We therefore recommend 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.

In the absence of this change, we urge members 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 20.

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 20, Amendment 1 in the 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 20, Amendment 2 in the Appendix).

[26] 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.

Data Protection Impact Assessments: a case-study

The *Bridges* case[27]

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).

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 20 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 128 and Schedule 11: Power to require information for Social Security Purposes

22. Schedule 11 gives the Secretary of State for Work and Pensions far reaching and intrusive powers of surveillance in relation to the accounts of anyone in receipt of a wide range of benefits (including the State Pension, Universal Credit, Pension Credit, Personal Independence Payments and Bereavement Support Payments).

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

23. Government has indicated that the intent behind this proposal is to allow fraud checks to be carried out at scale,[28] proactively and regularly,[29] on the speculative basis that claimants may have committed fraud.

24. PLP has existing concerns about the Department for Work and Pension's (DWP) approach to investigating fraud which includes numerous reports of people whose benefits, often their only source of income, have been indefinitely suspended pending investigation. People report having not been provided with any explanation of what they need to prove or disprove for the benefit to be reinstated, nor of how they might seek redress for any incorrect suspension and for the hardship it has caused. [30]

25. We are concerned that DWP is rapidly rolling out new systems for detecting fraud while there is a lack of effective independent assessment of the potential harm, reliability, efficiency and lawfulness of those systems.[31]

26. We also have ongoing concerns about a lack of transparency on the part of DWP, in particular in relation to the equalities implications of relevant measures.[32] DWP has also acknowledged that its ability to test for and take steps to avoid unfair impacts across protected characteristics, and hence ensure that it is not acting discriminatorily, is currently limited due to deficiencies in its data collection.[33]

27. DWP's response to a recent parliamentary question asking for publication of an Equality Impact Assessment (EIA) of Schedule 11, referred to a set of documents that includes an Impact Assessment of the economic impacts of the measures but no EIA.[34] DWP's response to recent PLP Freedom of Information Act request have stated that an EIA has not yet been undertaken in relation to the 'test and learn' exercise DWP has stated it wishes to undertake under Schedule 11 should it be adopted.[35] DWP has stated that it has already undertaken two 'proof of concepts'

---

[28] DWP's Policy Paper: Fighting Fraud in the Welfare System (May 2022), para 40: https://www.gov.uk/government/publications/fighting-fraud-in-the-welfare-system/fighting-fraud-in-the-welfare-system--2

[29] Press release, Changes to data protection laws to unlock post-Brexit opportunity (November 2023) Changes to data protection laws to unlock post-Brexit opportunity - GOV.UK (www.gov.uk)

[30] PLP Written Evidence (DWP0008) to the Public Accounts Committee Inquiry into DWP's Annual Report & Accounts 2022-23, paras 30(i) & 70-76: committees.parliament.uk/writtenevidence/123479/pdf/

[31] PLP Written Evidence (DWP0008) to the Public Accounts Committee Inquiry into DWP's Annual Report & Accounts 2022-23, paras 30 (ii) & (iii), 80-85 & 90-91 : committees.parliament.uk/writtenevidence/123479/pdf/

[32] PLP Written Evidence (DWP0008) to the Public Accounts Committee Inquiry into DWP's Annual Report & Accounts 2022-23, paras 6-8. 11 - 14, 30(ii), 56 - 69 and 80 - 89: committees.parliament.uk/writtenevidence/123479/pdf/ PLP Press Release, DWP need to assess bias is its automated systems says committee, 13 December 2023, https://publiclawproject.org.uk/latest/dwp-needs-to-assess-bias-in-its-automated-systems-says-committee/

[33] National Audit Office, Report on Accounts – Department for Work and Pensions, July 2023 para 5.12: https://www.nao.org.uk/wp-content/uploads/2023/07/dwp-report-on-accounts-2022-23.pdf

[34] Response to Question from Chris Brynt MP (UIN 6994): https://questions-statements.parliament.uk/written-questions/detail/2023-12-14/6994

[35] DWP response to PLP Freedom of Information Act Request, 15 January 2024, https://questions-statements.parliament.uk/written-questions/detail/2023-12-14/6994

relating to its proposed use of the new power.[36] DWP's response to a PLP FOIA request has confirmed that they hold information relating to PLP's request, but that they need more time to consider whether they will disclose it.[37]

We are concerned that Government is proposing the adoption of Schedule 11 before decision makers have had the opportunity to scrutinise and understand the potential equality impacts of these sweeping new powers.

The problem with Clause 128 and Schedule 11:

Under current legislation, the DWP has the power to require banks (and others) to share account information provided DWP has reasonable grounds to believe that an identified person has committed, or intends to commit, a benefit offence. This means that the DWP can only undertake fraud checks on a claimant's account where there is already a suspicion of fraud rooted in objective fact.

Schedule 11 disapplies this restriction and instead gives the Secretary of State the power to access information relating to claimants' accounts regardless of whether there is any suspicion of fraud or error, to identify cases that merit further consideration. This power is extremely (and unusually) wide. It could allow, for example, Government to access information about the accounts of all Universal Credit claimants in receipt of the childcare element because a few people in receipt of this element have committed fraud or information relating to the spending habits of Pension Credit claimants to look for indicators of whether their partner might have moved in without being declared.

The Impact Assessment for Schedule 11 indicates that Government's intention is to initially use the power in relation to Universal Credit, Pension Credit and Employment Support Allowance.[38] However, the draft legislation applies to a much wider range of benefits, including non means tested benefits such as Personal Independence Payments and Bereavement Support Payments.

While Government's stated intent is to use the power in relation to bank accounts in the first instance, the provision drafting is not limited to these organisations, instead allowing the extension of the power to non-financial institutions by way of secondary legislation.[39]

Government has stated that only a minimum amount of data will be accessed and only in instances

[36] DWP Impact Assessment: Third Party Data Gathering (September 2023), para 33: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

[37] DWP response to PLP FOIA request, 22 January 2024, https://www.whatdotheyknow.com/request/banking_data_proof_of_concepts#incoming-2528269

[38] DWP Impact Assessment: Third Party Data Gathering (September 2023), para 41: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

[39] Schedule 3B, para 1(1); DWP Impact Assessment: Third Party Data Gathering (September 2023), para 58: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

which show a potential risk of fraud and error.[40] However, these safeguards are not contained in the proposed new provisions, which instead give the Secretary of State the power to request any information relating to accounts and account holders, regardless of whether there is any suspicion of fraud or error. The Government's own Impact Assessment states that it is a "broad data sharing power",[41] intended to enable the accessing of data "at scale".[42]

PLP is recommending that Clause 128 and Schedule 11 should be removed.

Clauses 5, 6, 14 and 150: increased delegated powers mean less Parliamentary scrutiny

28. 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,[43] 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, 14 and 150:

Clause 5

The UK GDPR contains a finite set of lawful bases on which personal data can be processed. The protections provided currently by the UK GDPR 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

[40] Press Release, Changes to data protection laws to unlock post-Brexit opportunity (November 2023), https://www.gov.uk/government/news/changes-to-data-protection-laws-to-unlock-post-brexit-opportunity
[41] DWP Impact Assessment: Third Party Data Gathering (September 2023), pages 1, 9 & 12: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf
[42] DWP Impact Assessment: Third Party Data Gathering (September 2023), para 4, https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pd
[43] 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.

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

Clause 6

Clause 6(5) of the Bill inserts Article 8A in the UK GPDR 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 14

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 14(1) of the Bill inserts Article 22D(1) to the UK GDPR 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 UK Constitutional Law Association.[44] 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 Government 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 14, Amendment 3 in the Appendix).

Clause 150

Clause 150 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

[44] 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/.

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'.[45] In the Bill, what is 'consequential' is left to the subjective judgment of ministers.

We recommend that Clause 150 is narrowed to allow ministers to make provisions that are consequential on the Act only where necessary.

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

Contact

Caroline Selman
Senior Research Fellow
c.selman@publiclawproject.org.uk

Mia Leslie
Research Fellow
m.leslie@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/