

BIG BROTHER WATCH

Big Brother Watch Briefing on the Data Protection and Digital Information Bill for House of Lords Committee Stage

March 2024

About Big Brother Watch

Big Brother Watch is a civil liberties and privacy campaigning organisation, fighting for a free future. We're determined to reclaim our privacy and defend freedoms at this time of enormous technological change.

We're a fiercely independent, non-partisan and non-profit group who work to roll back the surveillance state and protect rights in parliament, the media or the courts if we have to. We publish unique investigations and pursue powerful public campaigns. We work relentlessly to inform, amplify and empower the public voice so we can collectively reclaim our privacy, defend our civil liberties and protect freedoms for the future.

Contact

Silkie Carlo

Director

Direct line: 020 8075 8478

Email: silkie.carlo@bigbrotherwatch.org.uk

Susannah Copson

Legal and Policy Officer

Direct line: 07935926492

Email: susannah.copson@bigbrotherwatch.org.uk

Table of Contents

RECOMMENDATIONS.....	5
SUMMARY.....	6
INTRODUCTION.....	7
WEAKENING DATA RIGHTS.....	9
Clause 1 – Information relating to an identifiable living individual.....	9
Clause 5 – Lawfulness of processing.....	11
AUTOMATED DECISION MAKING.....	14
Clause 14 – Automated decision-making.....	14
Law enforcement and ADM.....	19
Intelligence services and ADM.....	22
DIGITAL IDENTITY FRAMEWORK.....	24
Right to non-digital ID.....	24
FINANCIAL SURVEILLANCE.....	26
Clause 128 and Schedule 11 – Power to require information for social security purposes.....	26
Summary: 30 key issues with the financial spying powers.....	26
Existing powers.....	28
Mass surveillance.....	30
Article 8 - Privacy and data protection issues.....	33
Risks of automated decisions and 'Horizon-style' errors.....	36
Equality impact.....	39

Impact on housing crisis.....	41
Compliance challenges for affected third party organisations.....	42
An abuse of the parliamentary process.....	42
Code of practice.....	43
CONCLUSION.....	44

RECOMMENDATIONS

We believe that Peers should:

- **Support Lord Clement-Jones' amendment to remove clause 1, to ensure that personal data is protected** to at least as high of a standard as it is under the existing data protection framework;
- **Remove the new concept of 'recognised legitimate interests'** to prevent the Secretary of State from having the ability to pre-authorise data processing outside of the usual legally-defined route. This is important to avoid a two-tier data protection framework in which the Secretary of State can decide that certain processing is effectively above the law;
- **Support Lord Clement-Jones' amendment to remove clause 14 to uphold vital safeguards in the context of automated decision-making;**
- Establish a right to use non-digital verification methods in order to protect privacy and uphold the public's ability to choose how they express and verify their identity.
- **Support Baroness Kidron's amendments to remove clause 128/Schedule 11 to prevent the expansive and disproportionate powers to force banks to monitor all bank accounts** on the premise of targeting welfare recipients and people linked to those payments, potentially including landlords, and report anyone who triggers potential fraud indicators (such as frequent travel or savings over a certain amount) to the Department for Work and Pensions. It is imperative that these new powers are removed during scrutiny of the Bill.

SUMMARY

- **In order to protect crucial privacy and data protection rights, peers should support amendments to remove clauses 1, 14, 128 and Schedule 11.**
- Big Brother Watch believes that the Data Protection and Digital Information Bill (DPDI Bill) threatens to greatly weaken the existing data protection framework and is not fit for purpose. The Bill must be majorly revised in the course of its passage through parliament or revoked in order to protect the individual and collective privacy rights of the British public, safeguard the rule of law, and uphold key rights to equality and non-discrimination.
- **WEAKENING DATA RIGHTS:** The DPDI Bill will dilute protections around personal data processing, thereby reducing the scope of data protected by safeguards within data protection law. We are particularly concerned about the provisions that change the definition of personal data and the purposes for which it can be processed. More data will be processed with fewer safeguards than currently permitted as it will either no longer meet the threshold of personal data, or will be permitted for processing under the new 'recognised legitimate interests' provisions. Such a combination is a grave threat to privacy rights in the UK.
- **AUTOMATED DECISION-MAKING:** Where automated decision-making (ADM) is currently broadly prohibited with specific exceptions, the Bill would permit it in all but a limited set of circumstances. This will strip the right not to be subject to solely automated decisions, which risks exacerbating the likely possibility of discriminatory outcomes inherent in ADM systems; permitting ADM use in law enforcement and intelligence with few safeguards for special category data; as well as giving the Secretary of State executive control over the ADM regulatory framework through secondary legislation.
- **DIGITAL IDENTITY FRAMEWORK:** The Bill misses the opportunity to take a positive step and codify a right to use non-digital ID. Such a right is vital to protect privacy and equality in the digital age. The right to use a non-digital ID would protect people's choice in how they choose to verify their identities when accessing public and private services and ensure that no one feels forced to hand over personal identity data online.

- **FINANCIAL SURVEILLANCE:** The Bill would introduce new powers to force banks to monitor all bank accounts to find welfare recipients and people linked to those payments, potentially including landlords, and report anyone who triggers potential fraud indicators (such as frequent travel or savings over a certain amount) to the Department for Work and Pensions.

INTRODUCTION

1. Big Brother Watch believes that the Data Protection and Digital Information Bill (DPDI Bill) threatens to greatly weaken the existing data protection framework and is not fit for purpose.
2. The DPDI Bill was published on 8th March 2023 by the newly created Department for Science, Innovation and Technology (DSIT) as part of government efforts to establish a UK independent data protection framework. In anticipation of Committee stage in the House of Lords, we would like to draw your attention to a number of concerning issues within the Bill. We propose recommendations that are required in order to protect well-established privacy and data rights, maintain adequacy with EU law, and uphold the rule of law.
3. The Retained Regulation (EU) 2016/679 (UK GDPR) provides clear regulatory responsibilities that protect privacy and data protection rights. However, with the stated aim of sidestepping GDPR “red tape”¹, the Bill drastically veers away from the privacy protecting mandate of the current UK data protection framework.² In addition to weakening these rights, the Bill permits the use of inherently biased algorithms in high-risk contexts.³ This will “unleash data discrimination”,⁴ create barriers to redress, disproportionately impact marginalised individuals and groups, and empower the Secretary of State to shape the regulation and processing of the British public’s personal data on an unprecedented level.

¹ Michelle Donelan, ‘Our plan for growth in the digital, cultural, media and sport spheres.’ Transcript of speech delivered at Conservative Party Conference (3 October 2022):

<https://www.conservatives.com/news/2022/our-plan-for-digital-infrastructure--culture--media-and-sport>

² The UK privacy and data protection legislative framework is comprised of the following: the UK’s incorporation of the EU’s General Data Protection Regulation (GDPR) into domestic law (UK GDPR), the Data Protection Act 2018 (DPA) and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR).

³ Data Protection and Digital Information (No. 2) Bill, DSIT
<https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf> Clause 11.

⁴ Open Rights Group, Stop Data Discrimination (19 October 2022)
<https://www.openrightsgroup.org/campaign/stop-data-discrimination/>

4. The Bill will amend the current data protection system rather than repeal it, which means that UK GDPR, Data Protection Act (2018) and Privacy and Electronic Communications (EC Directive) Regulation 2003 will remain in place subject to the Bill's various amendments. As Lord Collins of Highbury has noted, this creates "a series of patchwork amendments" which "further complicates what is an overcomplex legislative area".⁵
5. In practice, many organisations operating between the UK and the EU will be hindered by difficulties in separating data that is processed to the weaker standards of UK data protection from other data held to the higher standards set by the GDPR. This will be a costly and burdensome challenge for businesses operating between the UK and the EU. Many organisations are likely to continue to operate under the existing data protection frameworks to avoid having to work to two different standards. Imposing this inconsistent framework undermines the stated purpose of supporting businesses that originally set out by DCMS/DSIT. **If the DPDI Bill fails even to deliver its business-first ethos, it begs the question: what is the point in it?**
6. The legislation engages data protection rights provided in the UK General Data Protection Regulation (UK GDPR)⁶, equality rights provided in the Equality Act (2010), and privacy and equality rights enshrined in Article 8 and 14 of the European Convention on Human Rights (ECHR). Any interference with these rights is only lawful when there is a legal basis and it is necessary and proportionate.⁷ The presumption must rest in favour of protecting these rights.
7. We are deeply concerned by Clause 128 and Schedule 11, introduced at Report stage in the House of Commons, which give the Secretary of State power to direct banks to monitor bank accounts and surveil welfare recipients and people linked to those payments, potentially including ex-partners, children, and landlords, and report anyone who matches for potential fraud or error precursors to the Department for Work and Pensions for further investigation. This disproportionate and intrusive financial surveillance, affecting every bank account holder in the country,

⁵ Lord Collins of Highbury speaking in the House of Lords (23 March 2023)

<https://parliamentlive.tv/Event/Index/39ad3b3f-46c4-4408-882a-a6d1694496d8>

⁶ See in particular UK GDPR [Chapter 2](#) on principles and [Chapter 3](#) on rights of data subject.

⁷ The Human Rights Act, EHRC: <https://www.legislation.gov.uk/ukpga/1998/42/schedule/1>.

has been ushered in at a late stage of the Bill with minimal opportunities for democratic scrutiny and debate.

8. Big Brother Watch believes that the DPDI Bill is not fit for purpose. In order to protect the individual and collective privacy rights of the British public, safeguard the rule of law and uphold key rights to equality and non-discrimination, the Bill must be majorly revised in the course of its passage through parliament, or revoked. This briefing seeks to draw attention to key threats to privacy and data protection, equality, and other human rights raised throughout the Bill. It also highlights opportunities to take positive measures to establish the right to non-digital ID to ensure that future digital identity systems uphold important principles of choice and consent. **In order to protect crucial privacy and data protection rights, peers should support amendments in the name of Lord Clement Jones and Baroness Kidron to remove clauses 1, 14, 128 and Schedule 11.**

WEAKENING DATA RIGHTS

Clause 1 – Information relating to an identifiable living individual

9. Clause 1 narrows the definition of personal data provided by the UK Data Protection Act 2018 (DPA). The DPA defines personal data as "any information relating to an identified or identifiable living individual" (s.3(2)) where a person is identifiable either "directly or indirectly" (s.3(3)). Clause 1(2) raises this threshold by introducing a test that means data only qualifies as personal data if it relates to an individual who is identifiable by a data controller/processor by "reasonable means at the time of the processing", or if the data controller/processor ought to "reasonably know" that another person will be able to obtain the information as a result of the processing and identify the individual "by reasonable means" at the time of processing.
10. Changing the definition of personal data in this way allows more data to be processed with lower levels of protection, narrowing the scope of information safeguarded by data protection law and placing disproportionate power in the hands of the data controller. 'Reasonable means' is a non-exhaustive list that includes the time, effort and costs in identifying the individual by that means and the technology and other

resources available to that person. By this definition, an organisation with minimal resources could assess that it does not have the reasonable means available to it, and can therefore process information as if it were not personal data and without the relevant protections. In practical terms, businesses will be able to process more data than currently permitted. This is determined by a wholly subjective test defined by a business's capacity and context "at the time of processing", rather than by the nature of the data being processed. As Lord Bishop of St Albans said:

"data protection legislation should define what is or is not personal data by the type of data it is, not by how easy or feasible it may be for an organisation or third party to use that data to identify an individual at every given point."⁸

11. Data protection expert Dr Chris Pounder has explained how this could increase data processing with minimal safeguards in the context of facial recognition CCTV, as the threshold for personal data would only be met if the data subject is on a watch-list and therefore identified.⁹ If an individual is not on a watchlist and the camera images are deleted instantly after checking the watchlist, then the data may not be considered personal and therefore would not qualify for data protection obligations. This would put the UK completely out of step with the rest of Europe, which is legislating against facial recognition; not to permit less safe use of it.

12. This new clause would permit the widespread operation of facial recognition CCTV systems across the UK – systems that can be legally operated outside of data protection purview and used "more or less in secret".¹⁰ The new definition could also mean that personal photos scraped from the internet and stored to train an algorithm may no longer be seen as personal data, so long as the controller does not recognise the individual; is not trying to identify them; and will not process the data in such a way that others can identify them. Additionally, as GeneWatch have highlighted, the police and security services will no longer have to go to court if they want access to genetic databases – they will be able to

⁸ HL Deb 19 December 2023 vol 834 cc2174:

<https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

⁹ Chris Pounder, 'Facial recognition CCTV excluded from new data protection law by definition of "personal data"' (25 April 2023) <https://amberhawk.typepad.com/amberhawk/2023/04/facial-recognition-cctvexcluded-from-new-data-protection-law-by-definition-of-personal-data.html>

¹⁰ Ibid

access the public's genetic information as a matter of routine.¹¹ The Bill will allow for more information about the public to be processed than ever before, with fewer safeguards and without people's knowledge. This undermines the entire data protection framework.

13. In effect, clause 1 means that personal data will not be defined by the nature of the data itself nor its relationship to the individual, but by the organisation's processing capacity at that moment in time. The replacement of a stable, objective definition that gives rights to the individual in favour of an unstable, subjective definition that determines the rights an individual has over their data according to the capabilities of the processor is not only illogical, complex, and bad law-making – it is contrary to the premise of data protection law, which is about personal data rights.

We urge peers to join Lord Clement-Jones in giving notice of their intention to oppose the Question that clause 1 stand part of the Bill.

Clause 5 – Lawfulness of processing

14. Processing personal data is currently only lawful if it is performed for at least one lawful purpose, one of which is that the processing is for legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights of the data subject. As such, if a data controller relies on their 'legitimate interests' as a legal basis for processing data, they must conduct a balancing test of their interests and those of the data subjects. Clause 5 of the DPDI Bill amends the UK GDPR's 'legitimate interest' provisions by introducing the concept of "recognised legitimate interests" (RLI), which allows data to be processed without a legitimate interests balancing test.
15. Clause 5 would amend Article 6 of the UK GDPR to equip the Secretary of State with the power to determine these RLIs (new Article 6(1)(ea)). Under the proposed amendment, the Secretary of State must only "have regard to, **among other things**, the interests and fundamental rights and freedoms

¹¹ GeneWatch, "The Data Protection and Digital Information Bill: A dangerous loss of personal control over genetic information" (December 2023): http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/gw-briefing-dataprot_1.pdf

of data subjects”¹² (emphases added). The usual ‘legitimate interests’ test is much stronger, whereby rather than merely a topic to have “regard” to, a legitimate interests basis cannot lawfully apply if the data subjects’ interests override those of the data controller.

16. Annex 1 of the Bill provides a list of exemptions that is overly broad and vague, including national security, public security and defence, emergencies, and crime as recognised legitimate interests for data processing without an assessment. Consider the example of crime. Attempts by individuals or companies to tackle crime can be damaging to privacy. For example, a company using facial recognition CCTV to film shoppers could rely on the recognised legitimate interest for their processing, despite the severe impact on the public’s privacy. Alternatively, a person could also rely on the broad scope of ‘crime’ as a RLI to film neighbouring houses, despite the impact upon others’ privacy that this would have. As such, Big Brother Watch agrees with the legal opinion of Stephen Cragg KC that :

“A list of ‘legitimate interests’ (mostly concerning law and order, safeguarding and national security) has been elevated to a position where the **fundamental rights of data subjects (including children) can effectively be ignored** where the processing of personal data is concerned”.¹³

17. The amendment in clause 5 also provides examples of processing that “may be” considered legitimate interests under the existing legitimate interests purpose (i.e. under Article 6(1)(f), rather than under the new “recognised legitimate interests” purpose). These include direct marketing, intra-group transmission of personal data for internal administrative purposes, and processing necessary to ensure the security of a network (subsection 9). Including direct marketing allows businesses to use the public’s personal data for profit without necessarily obtaining consent. This appears to be a significant watering down of current standards and is a retrograde step, undoing the significant benefits the public has enjoyed with regards to reducing unwanted junk mails/calls since the introduction of GDPR. Instituting direct marketing is not only a

¹² DPDI Bill, clause 5.

¹³ Stephen Cragg KC, 'In the matter of the Data Protection and Digital Information Bill' (22 November 2023): <https://defenddigitalme.org/wp-content/uploads/2023/11/KC-opinion-DPDI-Bill-27112023-Stephen-Cragg.pdf>

problem in terms of invasive online tracking from a profit perspective. It fails to account for the psychological harm that targeted advertising can cause, such as the emotional toll that people who have suffered a miscarriage experience as they are relentlessly pursued by adverts for baby products.¹⁴

18. The Bill also proposes a much more litigious data environment. Currently, an organisation's assessment of their lawful purposes for processing data can be challenged through correspondence or an ICO complaint, whereas under the proposed system an individual may be forced to legally challenge a statutory instrument in order to contest the basis on which their data is processed.

19. The Bill would give the Secretary of State the power to determine "recognised legitimate interests" through secondary legislation, which is subject to minimal levels of parliamentary scrutiny. Although the affirmative procedure is required, this does not entail usual scrutiny procedures or a Commons debate in every case. The last time MPs did not approve a statutory instrument under the affirmative procedure was 1978.¹⁵ In practice, interests could be added to this list at any time and for any reason, facilitating the flow and use of personal data for limitless potential purposes. Businesses could be obligated to share the public's personal data with government or law enforcement agencies beyond what they are currently required to do, all based upon the Secretary of State's inclination. Big Brother Watch is concerned that this Henry VIII power is unjustified and undermines the very purpose of data protection legislation, which is to protect the privacy of individuals in a democratic data environment, as it vests undue power over personal data rights in the executive.

20. Weakening both the definition of personal data and the purposes for which personal data can be processed is a double attack on the foundations of data protection in the UK, a major departure from existing UK and European data protection standards, and a serious and unjustified reduction of privacy rights in the UK. In its efforts to increase possibilities for data processing without consent, the Bill risks leaving the public at risk

¹⁴ Evidence on the Data Protection and Digital Information (No. 2) Bill and proposed amendments to the House of Commons Public Bill Committee (16 Mar 2023): <https://publications.parliament.uk/pa/cm5803/cmpublic/DataProtectionDigitalInformation/memo/DPDIB24.html>

¹⁵ HC Deb 24 July 1978 vol 954 cc1289-325: <https://api.parliament.uk/historic-hansard/commons/1978/jul/24/dock-labour-scheme>

and with lower trust in the digital economy and data processing, whether by the government or institutions.

AUTOMATED DECISION MAKING

Clause 14 – Automated decision-making

21. Automated decision-making (ADM) is the process by which decisions are made without meaningful human involvement, often using AI or algorithms. ADM is increasingly being used in important contexts such as welfare, immigration, and the criminal justice system. It provokes a range of concerns including encoded bias and discriminatory outcomes, data rights and privacy issues, transparency, accountability and redress, amongst other issues.
22. Under Article 22 of the UK GDPR, data subjects have the right not to be subject to a decision with legal effect (e.g. denying a social benefit granted by law) or similarly significant effect (e.g. access to education, employment or health services) based solely on automated processing or profiling, unless there is a legal basis to do so (e.g. explicit prior consent, a contract between the data subject and the controller, or where such activity is required or authorised by law).¹⁶
23. Clause 14 of the DPDI Bill replaces Article 22 with Article 22A-D, which redefines automated decisions and would enable solely automated decision-making in far wider circumstances. Big Brother Watch welcomes the clarification in Article 22A(1)(a), which we have long called for, defining a decision based on solely automated processing as one that involves “no meaningful human involvement”. This is an important clarification that prevents merely administrative approval of an automated decision being considered adequate to qualify a decision as a human one and thus exempt from the legal safeguards that should apply.
24. However, we have grave concerns about the broader reversal of the Article 22 right not to be subjected to solely automated decisions. Indeed, the proposed Articles 22A-D invert the current Article 22 protections: where

¹⁶ WP29 (2018). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, 17/EN/WP/251 rev. 01 https://ec.europa.eu/newsroom/article29/items/612053_21-22; Jim Killock, Ana Stepanova, Han-Wei Low and Mariano delli Santi, 'UK data protection reform and the future of the European data protection framework' (26 October 2022) <https://eu.boell.org/en/ukdata-protection-reform>

ADM is currently broadly prohibited with specific exceptions, the Bill would broadly permit ADM and only restrict it in very limited circumstances.

25. The DPDI Bill could have been an opportunity to build upon the discourse around AI regulation. It could have strengthened existing protections to support responsible innovation to benefit both businesses and the public. Instead, as Baroness Young of Old Scone said during Third Reading in the House of Lords, the Bill signifies a **"missed opportunity"** that "erodes further the already inadequate legal safeguards that should protect individuals from discrimination or disadvantage by AI systems".¹⁷

26. Article 22C permits solely automated decisions based on personal data and waters down the safeguards that currently apply to permitted automated decisions. Whereas the law currently prescribes a number of safeguards with regards to automated decisions authorised by law – namely, that the controller must notify the data subject and that the data subject has the right to request a new decision (including one that is not automated) – Article 22C only requires that the controller ensures safeguards are in place (A22C(1)) and that they include measures which "provide the data subject with information" about the automated decision and enable them to make representations, contest and obtain human intervention with regard to the decision. The proposed requirement to "provide information" would seem to be a departure from the current legal requirement to "notify" an individual that they have been subjected to an automated decision – for example, this could be interpreted as a reactive responsibility if information is requested, rather than a proactive duty. It could even be interpreted as a general responsibility that could be addressed with generic references to ADM in privacy policies. The explanatory notes to the Bill clarify that newly permitted automated decisions will not require the existing legal safeguard of notification, stating that only **"where appropriate, this may include notifying data subjects after such a decision has been taken"**¹⁸ (emphases added). This is an unacceptable dilution of a critical safeguard that will not only create uncertainty for organisations seeking to comply, but could lead to vastly expanded ADM operating with unprecedented opacity. If ADM takes place

¹⁷ HL Deb 19 December 2023 vol 834 cc 2180-2181:
<https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

¹⁸ Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, p.35, para.177, 8th March 2023:
<https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf>

effectively in secret, data subjects may not even know they are being subjected to ADM and cannot exercise their legal rights in practice.

27. Article 22(B) would maintain a general prohibition on ADM only when decisions process special category personal data e.g. ethnicity or religion.¹⁹ It would exempt decisions authorised by law if the data subject consents to the processing, or if the processing is required for a contract or authorised by law and the processing is "necessary for reasons of substantial public interest" as per Article 9(2)(g) (i.e. one of the legal bases upon which special category personal data can be lawfully processed). However, automated decisions processing special category data are prohibited in any circumstances where an Article 6(1)(ea) basis is relied on partly or entirely for the processing, (i.e. a basis on the Secretary of State's new proposed list of legitimate purposes for data processing, made by Henry VIII powers).
28. The same watered-down "safeguards" apply as per Article 22(C) – meaning that even where ADM involving sensitive personal data is concerned, an affected data subject may not be notified. As Stephanie Peacock MP has noted, this will exacerbate power imbalances by "hiding an individual's own rights from them."²⁰
29. While Article 22(B) would appear to acknowledge the heightened risk of ADM for marginalised individuals or groups, the emaciation of Article 22 rights proposed by the DPD Bill in fact puts them at risk. There is a real risk that such changes in the context of automated-decision making could impact rights protected by the Equality Act, as raised during Committee stage of the Bill.²¹ There are many contexts in which personal data that is not special category acts as a proxy for protected characteristics when used in ADM. For example, data about a person's name or occupation can act as a proxy for their sex, or postcodes may act as a proxy for race²² when processed in an algorithm. Indeed, the Public Sector Equality Duty

¹⁹ DPD Bill Article 22B.

²⁰ Data Protection and Digital Information (No. 2) Bill (Fourth sitting) Debate, 16th May 2023, 129-130: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf

²¹ Data Protection and Digital Information (No. 2) Bill (First sitting) Debate, 10th May 2023, 33-34: [https://hansard.parliament.uk/commons/2023-05-10/debates/8fafb6ee-f2dc-45ba-b2be-d092330ea8c7/DataProtectionAndDigitalInformation\(No2\)Bill\(FirstSitting\)](https://hansard.parliament.uk/commons/2023-05-10/debates/8fafb6ee-f2dc-45ba-b2be-d092330ea8c7/DataProtectionAndDigitalInformation(No2)Bill(FirstSitting))

²² ICO, 'What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?' (2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/#address>

assessment of the Bill acknowledges this issue in its recounting of the automated A-Level grading scandal:

“Though precautions were taken to prevent bias based on protected characteristics, the profiles of those attending different schools inevitably led to outcomes being different based on their protected characteristics, including race and sex.”²³

30. Algorithm Watch explains that “automated decision-making is never neutral”.²⁴ ADM outputs are defined by the quality of the data they are trained on. Where data is unfair or biased, machine learning will propagate and enhance these differences. For example, credit-scoring systems have been found to operate on racial and ethnic bias;²⁵ welfare systems to uphold economic disparities;²⁶ algorithmically generated A-level grades to entrench socio-economic inequalities;²⁷ and recruitment systems to discriminate against women, single mothers, and people with disabilities.²⁸ Many of these kinds of data-driven automated decisions have a serious impact on people’s lives and require serious safeguards – yet this Bill would significantly deregulate ADM and remove vital safeguards for individuals’ rights, transparency, scrutiny, and accountability. Big Brother Watch shares the view of The Ada Lovelace Institute given during Committee Stage that safeguards are vital in the context of automated decision-making, and the permissive approach that this Bill takes will “lead to greater harms”.²⁹

31. Automated decision-making can engage the Equality Act 2010 and the ECHR respectively, due to its capacity to negatively impact equality and human rights, particularly the right to privacy. In its impact assessment on the DPDI Bill, DSIT acknowledges that the Article 22 replacements will likely “increase the number of decisions made using

²³ Public Sector Equality Duty assessment for Data Protection and Digital Information (No.2) Bill - DSIT, 8th March 2023: <https://www.gov.uk/government/publications/data-protection-and-digital-informationbill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digitalinformation-no2-bill>

²⁴ Algorithm Watch, ‘The ADM Manifesto’ <https://algorithmwatch.org/en/the-adm-manifesto/>

²⁵ Student Borrower Protection Center, ‘Educational Redlining’ (February 2020) <https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf>

²⁶ 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>

²⁷ Adam Santario, ‘British Grading Debacle Shows Pitfalls of Automating Government’ (20 August 2020) <https://www.nytimes.com/2020/08/20/world/europe/uk-england-grading-algorithm.html>

²⁸ Algorithm Watch, ‘Austria’s employment agency AMS rolls out discriminatory algorithm, sees no problem’ (6 October 2019) <https://algorithmwatch.org/en/austrias-employment-agency-ams-rolls-outdiscriminatory-algorithm/>

²⁹ Data Protection and Digital Information (No. 2) Bill (First sitting) Debate, 10th May 2023, 30-31: [https://hansard.parliament.uk/commons/2023-05-10/debates/8fafb6ee-f2dc-45ba-b2be-d092330ea8c7/DataProtectionAndDigitalInformation\(No2\)Bill\(FirstSitting\)](https://hansard.parliament.uk/commons/2023-05-10/debates/8fafb6ee-f2dc-45ba-b2be-d092330ea8c7/DataProtectionAndDigitalInformation(No2)Bill(FirstSitting))

this technology” which, by nature, implies a corollary increase in its negative effects.³⁰ The impact assessment also acknowledges that the Bill “will make it more feasible for public authorities processing for law enforcement purpose to make automated decisions” but stated that the framework has “strong safeguards”.³¹ Our analysis would clearly contest that assertion – the Bill proposes to significantly weaken existing safeguards. The Public Sector Equality Duty assessment of the Bill acknowledges that “without further mitigation, [increased ADM under the Bill] could perpetuate inequalities by increasing the number of decisions made about people based on their protected characteristics”, but states that the proposal “is mitigated by the approach to bias mitigation as set out in the national policy position on AI governance that will be detailed in the White Paper later this year and in the other AI reforms proposed to enable organisations to test AI-driven automated decision-making for potential biases and to ensure appropriate steps are taken to mitigate risks associated with bias.”³² It is unacceptable, irresponsible, and a failure of the state to uphold its rights and equality responsibilities to legislate in a way that invokes serious risks of perpetuating discrimination based on the future publication of pre-legislative plans and vague expectations associated with experimental AI testing. It is, frankly, magical thinking. In sum, we conclude that the Government has, on its own account, introduced serious risks of proliferated discrimination its proposal to significantly expand ADM but has not been able to propose appropriate safeguards.

32.By providing new adjudicative powers to the Secretary of State, clause 14 provokes serious concerns for the rule of law and democratic accountability. New Article 22D allows the Secretary of State to determine by way of regulations whether meaningful human intervention is required in the cases described in the regulations (Article 22(D)(1)); whether or not an automated decision of a certain description is to be considered of “significant effect” for a data subject (Article 22(D)(2)), thereby triggering safeguards; what safeguards are or are not required

³⁰ DSIT, ‘Impact assessment: Data Protection and Digital Information (No. 2) Bill: European Convention of Human Rights Memorandum’, para. 20 (updated 8 March 2023), <https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impactassessments/data-protection-and-digital-information-no-2-bill-european-convention-on-humanrights-memorandum>

³¹ Ibid

³² Public Sector Equality Duty assessment for Data Protection and Digital Information (No.2) Bill - DSIT, 8th March 2023: <https://www.gov.uk/government/publications/data-protection-and-digital-informationbill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digitalinformation-no2-bill>

to satisfy the weakened ADM safeguards in Article 22(C), and to vary the safeguards required under Article 22(C) (Article 22(D)(4)). In effect, Article 22(D) gives total executive control over the operation of the ADM regulatory framework by way of secondary legislation.

33. These are some of the most extraordinary Henry VIII powers that Big Brother Watch has ever seen. Not only would they give executive control to amend primary legislation setting a regulatory framework for important data and privacy rights, but they effectively give the Secretary of State the power to bypass the regulatory framework by making adjudicatory decrees. This exceptional scope for political arbitration of the regulatory framework undermines its very purpose.

Law enforcement and ADM

34. In the context of law enforcement processing, the potential for people's rights and liberties to be infringed upon by automated processing is extremely serious. Clauses 14(2) and (3) would amend the Data Protection Act 2018 to replace the current general prohibition on ADM by law enforcement with a general prohibition only on ADM processing special category personal data by law enforcement (proposed s.50B), with exceptions for cases where the data subject has consented to the processing or where "the decision is required or authorised by law" (s.50B(3)). A decision qualifying as ADM is one that either "produces an adverse legal effect" or "similarly significant adverse effect for the data subject" (s.50A(1)(b)).

35. We expect that police in England and Wales may rely on a very broad interpretation of ADM "authorised by law" based on common law and a patchwork of laws pre-dating the technological revolution, as South Wales Police and the Metropolitan Police Service³³ have with regards to the use of live facial recognition, due to a vacuum of specific laws applying to new technologies. As such, police will be able to conduct ADM without limitation, and to conduct ADM involving sensitive data with very few limitations.

³³ Live Facial Recognition: Legal Mandate 3.0 – Metropolitan Police Service: <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/new/lfrlegal-mandate-v.3.0-web.pdf> (accessed 8 April 2023)

36. Unlike the proposed general prohibition on ADM involving special category personal data at Article 22(B), the law enforcement provision does not require an Article 9(2) basis (i.e. that the processing is “necessary for reasons of substantial public interest”) nor does it preclude ADM being undertaken where Article 6(1) (ea) is relied on for the processing (i.e. the Secretary of State’s new proposed list of legitimate purposes for data processing made by Henry VIII powers). As such, ADM involving sensitive personal data could be used in UK policing following a political decree. Similarly diluted safeguards apply under proposed s.50C(3) whereby, rather explicitly requiring the data controller to notify an affected individual, they must merely create measures to provide information about the ADM and enable the subject to contest the decision. However, s.50C(3)-(4) exempt controllers from the need to have any safeguards on ADM for a broad range of reasons, such as “to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties” so long as the controller reconsiders the decision, with meaningful human intervention, as soon as reasonably practicable (s.50C(3)). This means that law enforcement ADM with significant adverse effects can take place in secret with no safeguards and using special category data that may even pertain to protected characteristics, so long as a human review of the decision takes place at some time after the fact. There are no provisions for any course of action after such secret ADM decisions are made – not even if, for example, the human review finds that an automated decision was wrong. It is worth restating that ADM, according to the proposed definition, “produces an adverse legal effect” or “similarly significant adverse effect for the data subject”.

37. The Government’s intention is to permit secret police automated decision-making with significant adverse effects. This is clear in the Bill’s ECHR Memo, which states:

“Currently controllers processing for law enforcement purposes under Part 3 of the DPA rarely make use of automated processing. However, one of the reforms being made will make it more possible for the police and others to use this technology. Currently the requirement to inform an individual whenever automated decision-making takes places limits operational usefulness, as it could tip off

people that they are subject to investigation. These reforms will enable the controller to review such a decision after it has been taken, instead of informing the individual at the time (...).³⁴

38. It is important to remember that in order to qualify as ADM, the decision must have significant legal adverse effects or similarly significant adverse effects for the data subject. It is extremely concerning that any ADM can take place about a person without their right to know, but to be conducted by police in secret and in a way that detrimentally impacts their life is an affront to justice and is likely to interfere with any number of individuals' rights. Further, the safeguard of providing the data subject with information about the ADM at an undefined time after the fact would be subject to sweeping exemptions such as to avoid prejudicing the prevention of crime and to protect public security (proposed s.50C(4)(b)-(c)). Our research shows that such broad exemptions in other laws are frequently relied on to maintain excessive, unjustified secrecy over data processing and ADM (e.g. in the welfare system).³⁵

39. Overall, the new law enforcement ADM powers will lead to a vast expansion of purely automated decisions with significant adverse impacts on people where personal data is used that, in many cases, will act as a proxy for protected characteristics, particularly race and sex. In any context, this expansion of ADM along with reduced safeguards would be dangerous. However, in a context where UK policing is suffering from well-documented issues with chronic, institutionalised racism and sexism, it is recklessly so.

40. Further, the ability of law enforcement to use ADM with explicit special category personal data, such as race and sex variables, if the decision-making is authorised by law – even if the lawful basis is one provided by a Ministerial pen that circumvents the general regulatory framework – creates technological policing powers that create extraordinary dangers of executive-led discrimination.

³⁴ Data Protection and Digital Information (No. 2) Bill: European Convention on Human Rights Memorandum – 8th March 2023, para.19, p.9:

<https://publications.parliament.uk/pa/bills/cbill/58-03/0265/echrmemo.pdf>

³⁵ For example, see Poverty Panopticon: the hidden algorithms shaping Britain's welfare state – Big Brother Watch, July 2021: <https://bigbrotherwatch.org.uk/wp-content/uploads/2021/07/PovertyPanopticon.pdf>

41. Big Brother Watch has successfully scrutinised and challenged a number of ADM and big data uses by police in the UK – such as the AI recidivism tool HART, which predicted reoffending risks partly based on an individual’s postcode in order to inform charging decisions; PredPol, which was used to allocate policing resources based on postcodes; facial recognition, which has well-documented demographic bias issues disproportionately impacting people of colour; and the Gangs Matrix, which harvests “intelligence” disproportionately impacting innocent young black men. Under the proposed changes, the legal presumption could easily be in favour of using such discriminatory tools on a larger and more intrusive scale, with fewer safeguards and potentially even in secrecy. Indeed, this appears to be the aim of the proposals. This means affected individuals or groups will have no or highly limited routes to redress and could either be affected by ADM with adverse legal effects in total secrecy, or if they do discover ADM has impacted them, will have to attempt to prove discriminatory impacts or a failure to uphold the Public Sector Equality Duty in order to challenge decisions. Big Brother Watch is concerned that clause 14(3) would introduce a new era of discriminatory, techno-authoritarianism in British policing.

Intelligence services and ADM

42. Clause 14(4) would amend s.96 and s.97 of the Data Protection Act (DPA) 2018 to change the definition of ADM in the context of intelligence services processing. Whereas the current law maintains the same definition of ADM across various provisions and data controllers, the DPDI Bill proposes that an entirely different definition of ADM applies to the intelligence services in order to create an incredibly enabling framework, whereby a decision is only made by ADM “if the decision-making process does not include an opportunity for a human being to accept, reject or influence the decision” (proposed s.96(4)).

43. Further, clause 14(5)(c) proposes to remove s.96(6) of the DPA 2018, which clarifies that “a decision that has legal effects” is to be regarded as significantly affecting the individual and thus qualifies as ADM. If decisions by the intelligence services that have legal effects on an individual do not qualify as significant, it is unclear what does and as such, unclear how ADM should be defined for the intelligence services.

Whilst it may be convenient law-making, it is very poor law-making and illogical to define “significant effects” arising from automated decisions in multiple ways in the same Bill.

44. Under the new framework proposed for the intelligence services, a decision will not be subjected to ADM legal safeguards even if the “opportunity” for a human being to accept, reject or influence the decision is not used or not even considered; and even where the human involvement is non-meaningful and purely administrative. The proposed changes weaken safeguards so significantly that the system proposed for the intelligence services could be compared to merely requiring a cookie banner style of approval process that could approve a suite of automated decisions that have significant legal effects on individuals (DPA 2018 s.96(1)). However, unlike a cookie banner, one need not even click to accept/reject the ADM. As long as the opportunity to accept/reject a decision exists, regardless of whether it is considered or used, the decision does not incur the minimal ADM legal safeguards. The proposed new definition of ADM is so weak as to render the proposed safeguards almost meaningless.

45. During Report Stage (HL) on the DPA, Home Office Minister Baroness Williams gave an example of how the intelligence services use ADM:

“The intelligence services may use automated processing in their investigations, perhaps in a manner akin to a triage process to narrow down a field of inquiry. The decision arising from such a process may be to conduct a further search of their systems; arguably, that decision significantly affects a data subject and engages that individual’s human rights.”³⁶

46. **The Minister claimed that the intelligence services may subject an individual to further surveillance as a result of automated decision-making. However, this is precisely the kind of decision that requires meaningful human input. Individual warrants are not necessarily required for intelligence agencies to process individuals’ personal data, but an assessment of necessity and proportionality is required. The proposed new system makes human assessments even more likely,**

³⁶ Data Protection Bill, Report stage, 2nd day, 13 December 2017 ([https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill\(HL\)](https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL)))

opening the door to automated surveillance systems that significantly engage Article 8 rights with no meaningful safeguards. The proposed changes to intelligence services' ADM must be rejected.

We urge peers to join Lord Clement-Jones in giving notice of their intention to oppose the Question that clause 14 stand part of the Bill.

DIGITAL IDENTITY FRAMEWORK

Right to non-digital ID

47. Part 2 of the Bill introduces a new regime for digital verification services. It sets out a series of rules governing the future use and oversight of digital identities as part of the government's roadmap towards digital identity verification.

48. Having different ways to prove identity online can be useful. However, although the ability to verify identity online can be helpful for some people, it is equally a difficulty for those who cannot – or do not want – to use digital methods.

49. Digital identity systems pose serious risks to rights, security, and equality. In the worst case scenario, they can be misused for mass surveillance, to track marginalised groups, to construct population-wide databases of personal data, exacerbate inequalities for people who cannot participate digitally, or can be vulnerable to hackers. During the Bill's passage through the House of Commons, Sir David Davis MP highlighted the risks that such a system would pose to the entire population:

“[...] as time passes and the rise of artificial intelligence takes hold, the ability to make use of central databases is becoming formidable. It is beyond imagination, so people are properly cautious about what data they share and how they share it. For some people [...] that caution will mean avoiding the use of digital identity verification, and for others that digital verification is simply inaccessible. The Bill therefore creates two serious problems by its underlying assumptions.”³⁷

³⁷ HC Deb 29 November 2023 vol 741 cc889-890:
<https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA->

50. It is imperative that services are never contingent on a digital identity check, as this could prevent people from participating in key activities. It is also important that people do not have a different level of service because they are digitally excluded. During Report stage (HC) Sir David Davis MP tabled a new clause to introduce a right to non-digital verification services and, in doing so, protect people's right to choose. As he said during the debate:

"[...] what matters is that people have a choice and are not coerced into providing the data through digital means, whether their reason is concern about their privacy or something else."³⁸

51. This amendment secured strong cross-party support in the Commons, with signatories including John McDonnell MP, Alistair Carmichael MP, Marcus Fysh MP, Chris Green MP, Sir Graham Brady MP, and Sir Charles Walker MP, demonstrating that this is an issue of cross-party concern.

52. A legal right for an individual to choose whether to use digital or non-digital means of verifying their identity is important not only for the liberty and equality of individuals but also to cultivate trust in growing digital identity systems, which must exist to empower people with real choices rather than to coerce people with digital demands. A move towards digitalisation is not a justification for compelling individuals to use systems that could compromise their privacy or rights more broadly. Even in this age of technological change, it is vital that core legal protections exist to protect our rights and liberties, even if this means promoting "offline" alternatives or the choice to opt-out.

53. People should always have a choice in how they choose to prove their identity and share personal data. Creating the legal right to choose enshrines the ability to opt out and use offline methods of identification verification where needed and, in doing so, mitigates the risk of funnelling people into handing over data online, or leaving people out from accessing services.

54. The growing presence of digital identity systems and services should not mean that offline government services that require identity

38 [6A3683EB8B87/DataProtectionAndDigitalInformationBill](#)
Ibid

verification are made any less accessible, affordable or usable for people who cannot or do not want to use them. While there is no immediate plan for the introduction of a UK-wide mandatory digital ID, the Government is both creating a digital identity system to allow access to state services in the form of OneLogin and cultivating a new digital identity market in the private sector through the DVS Trust Framework, which is why it is crucial to get important safeguards in place. **It is for these reasons that we believe peers should seek to emulate the amendment laid by Sir David Davis during House of Commons report stage, which would create a legal right to non-digital verification services.**

FINANCIAL SURVEILLANCE

Clause 128 and Schedule 11 – Power to require information for social security purposes

Summary: 30 key issues with the financial spying powers

- 1. The Government has existing powers to investigate the accounts of fraud suspects.**
- 2. This extraordinary power is ineffective and entirely disproportionate to the revenue the Government expects to raise via its use.**
- 3. It must also be recognised that DWP is currently responsible for record underpayments.**
- 4. This power would force third party organisations to trawl *all* customers' accounts in search of "matching accounts".**
- 5. This is a mass data trawling power targeted at recipients of all benefits, including of the state pension – approximately 40% of the population – as well as people linked to claims, including landlords.**
- 6. This would be a precedent-setting power that enables intrusive generalised financial surveillance across the population - *not* restricted to serious crime, or even crime - but in relation to general administration.**
- 7. Even in the context of crime, this suspicionless surveillance power would be an assault on the presumption of innocence.**

8. The Information Commissioner does not currently view these powers as proportionate – in which case, they may be unlawful and a breach of individuals' right to privacy protected by the Human Rights Act.
9. The proposed power contains no data minimisation requirement and no oversight of the secret search criteria or algorithms involved.
10. The power would create data protection conflicts for banks and other affected third parties, requiring them to breach their duty of confidence to customers.
11. The power is particularly intrusive, as the information monitored includes special category data that invokes extra protections.
12. The proposals could impact EU adequacy.
13. The power would create data security risks.
14. Thousands of decisions regarding the collection and reviewing of private financial information of people receiving benefits will be automated.
15. There are no provisions for algorithmic transparency and accountability.
16. With the constant scanning of tens of millions of accounts in relation to often complex claims, false positive matches for fraud or error are highly likely.
17. Financial institutions' 'Suspicious Activity Reports' already have a very high false hit rate.
18. A related trial indicated that this extraordinary power is unlikely to be an effective measure.
19. Errors resulting from the proposed surveillance power are likely to have particularly serious negative consequences for welfare recipients.
20. The Government must learn lessons from the Horizon scandal.
21. The Public Accounts Committee raised concerns about DWP's lack of algorithmic transparency.
22. The privacy intrusion and risks of other consequential harms will have the greatest impact on those in receipt of benefits, many of whom are in receipt of benefits due to a protected characteristic such as disability or age.

23. In addition to landlords, some banks and other third party organisations may choose not to accept individuals in receipt of benefits, or treat them less favourably.
24. DWP has not done enough to assess the risks of the proposed policy discriminating against protected groups.
25. This power could decimate the private rental market for recipients of benefits.
26. Third parties face fines for failures to comply.
27. The proposed power will create a significant resource burden for affected third parties.
28. Smaller third party organisations may face significant compliance challenges.
29. This rushed power has had inadequate scrutiny as it was introduced at Report Stage in the House of Commons – almost 9 months after the DPDI Bill was introduced.
30. The Government cannot offer Parliament or the public reassurance by deferring vital legal protections in favour of guidance in a possible future code of practice.

Existing powers

55. **The Government has existing powers to investigate the accounts of fraud suspects.** It is right that fraudulent uses of public money are robustly be dealt with and the government already has significant powers to review the bank statements of welfare fraud suspects – for example, under the Social Security Fraud Act 2001. Under current rules, the Department for Work and Pensions (DWP) is able to request bank account holders' bank transaction details on a case-by-case basis if there is reasonable grounds to suspect fraud. On DWP's admission:

“DWP currently has the power to compel prescribed information holders to share data on individuals if fraudulent activity is suspected but does not have the power to compel Third Parties to share data that is signalling potential signs of fraud and error on ‘persons unknown’ at scale.”³⁹

³⁹ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023), p.10: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf 10.

We would argue that such a vague and intrusive surveillance project has not been enabled thus far for very good reason.

There are already multiple powers and processes by which DWP exchanges data with third parties. For example, HMRC shares banking data with DWP on an annual basis; the Proceeds of Crime Act 2002 requires banks and building societies to notify law enforcement of suspicious activity; open banking enables consumers to give third parties access to their financial accounts; private companies that administer the UK's banking infrastructure can see transactional data; and Credit Reference Agencies can view credit histories.⁴⁰ The Government must reduce benefit fraud and error – but there are more effective and proportionate means, including the proper use of existing powers, of doing so.

56. **This extraordinary power is ineffective and entirely disproportionate to the revenue the Government expects to raise via its use.** The Government's own analysis shows that, if it works as hoped, this unprecedented bank intrusion is expected to generate approx. £250m net annual revenue – this would be mean recovering less than 1/34th or less than 3% of the estimated annual loss to fraud and error (the 'best estimate' is still only £320m)⁴¹.

57. **It must also be recognised that DWP is currently responsible for record underpayments.** In comparison, benefits underpaid by the Government were a record £3.3bn in 2022-3, leading to criticism from the National Audit Office.⁴² The Public Accounts Committee recently raised particular concern about

“yet another historic underpayment of State Pension, which [DWP] estimates may have left some 210,000 pensioners out of pocket by a total of £1.3 billion.(...) This is in addition to the previous underpayment of £1.2 billion affecting 165,000 pensioners due to historical errors by DWP.”⁴³

40 Ibid.

41 Ibid.

42 Benefits claimants in UK were underpaid by record £3.3bn last year – Rupert Jones, the Guardian, 6 July 2023: <https://www.theguardian.com/society/2023/jul/06/benefits-claimants-in-uk-were-underpaid-by-record-33bn-last-year>

43 House of Commons Committee of Public Accounts, The Department for Work and Pensions Annual Report and Accounts 2022-2023 (6 December 2023), p.3: <https://committees.parliament.uk/publications/42434/documents/210942/default/>

The State Pension is one of the benefits the government plans to target with this surveillance power. However, DWP is only seeking to use the proposed power to “recover monies owed to DWP”⁴⁴ – not to pay the billions of pounds underpaid and owed to citizens. Whilst both are important, fraud costs the public purse whereas underpayment errors can cost lives. However, neither of these complex issues justifies or can be appropriately addressed by mass financial surveillance.

Mass surveillance

58. This power would force third party organisations to trawl all customers’ accounts in search of “matching accounts”. This new power would amend the Social Security Administration Act 1992 (‘SSA’) to allow DWP to access the personal data of welfare recipients by requiring the third party served with an account information notice (AIN) – such as a bank, building society or online marketplace – to conduct mass monitoring without suspicion of fraudulent activity. Once issued, an AIN requires the receiver to give the Secretary of State, or any staff member who has appropriate responsibility to exercise the power, the names of the holders of accounts (sub-paragraph 2(1)(a)). In order to do this, the bank will have to process the data of all bank account holders and run automated surveillance scanning according to secret search criteria supplied by DWP. Lord Vaux warned that the proposal “constitutes a worrying level of creep towards a surveillance society”.⁴⁵

59. This is a mass data trawling power targeted at recipients of all benefits, including of the state pension – approximately 40% of the population – as well as people linked to claims, including landlords. Schedule 11 of the DPDI Bill would add new Schedule 3B to the SSA; sub-paragraph 2(3)(a) states that a “matching account” that can be flagged to the government includes any account into which any benefit is paid, and the other accounts of that account holder. Approximately 22.6 million people are in receipt of a benefit – around 40% of the population.⁴⁶ Further, because in some circumstances benefits can be paid into a third party’s bank account,

⁴⁴ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023, p.1): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

⁴⁵ HL Deb 19 December 2023 vol. 834, col.2185: <https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

⁴⁶ Department for Work and Pensions, DWP benefits statistics: August 2023 (15 August 2023): <https://www.gov.uk/government/statistics/dwp-benefits-statistics-august-2023/dwp-benefits-statistics-august-2023>

such as a parent, partner, appointed person, joint account, or landlord (where claimants opt for landlords to receive their housing benefit directly), according to paragraph 2(5) all of these people's accounts can also be "matching accounts" eligible for surveillance, despite the fact they are not benefits claimants. Lord Sikka highlighted the alarming reach of the proposals during Second Reading (HL):

"Now comes snooping and 24/7 surveillance of the bank, building society and other accounts of the sick, disabled, poor, elderly and unfortunate, all without a court order [...] Can the Minister explain why people not receiving any social security benefits are to be snooped upon?"⁴⁷

60. **This would be a precedent-setting power that enables intrusive generalised financial surveillance across the population - not restricted to serious crime, or even crime - but in relation to general administration.** Paragraph 1(2) of proposed new Schedule 3B of the SSA imposes only one purpose limitation: that the Secretary of State's power to issue an AIN "may be exercised only for the purpose of assisting the Secretary of State in identifying cases which merit further consideration to establish whether relevant benefits are being paid or have been paid in accordance with the enactments and rules of law relating to those benefits." This is unlike any other surveillance legislation – there is no crime threshold to merit the financial privacy intrusion at all. The Government has been explicit that the power is designed to "proactively target **potential** fraud" (our emphasis) as well as "error", which accounts for almost a quarter of the cost of overpayments, and encapsulates DWP's own error. It would be wholly inappropriate, and set a disturbing precedent, to use mass financial surveillance powers to administrate a government department's errors. The Constitution Committee reported that it is "concerned by the breadth of these provisions, which empower the Government to demand access to individual bank accounts without grounds for suspicion."⁴⁸

⁴⁷ HL Deb 19 December 2023 vol. 834, col.2193:
<https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

⁴⁸ Data Protection and Digital Information Bill – Select Committee on the Constitution, 2nd Report of Session 2023-4, 25 January 2024, para. 18:
<https://committees.parliament.uk/publications/43076/documents/214262/default/>

61. DWP references Section 40A of the Immigration Act 2014 as a comparative legal basis for these proposals.⁴⁹ Section 40A requires banks and building societies to check accounts to identify any that may be held by disqualified persons named by the Home Office (people who are in the UK without leave to remain and whom the Home Secretary considers should not be permitted to open a current account). DWP's impact assessment suggests that these powers are similar in that they require banks and financial institutions to check consumer records, match against key criteria and report relevant data back to investigation and enforcement agencies.⁵⁰ This comparison is a complete misnomer. Checking the names of account holders who are not legally allowed to be in the country or to have a bank account is different to searching the accounts of the entire population, without suspicion, against secret criteria.

62. **Even in the context of crime, this suspicionless surveillance power would be an assault on the presumption of innocence.** Big Brother Watch finds it wholly inappropriate for the UK Government to order private banks, building societies and other third party organisation services to conduct mass, algorithmic, suspicionless surveillance. These unprecedented powers were accurately described by Lord Vaux as “draconian”⁵¹ and by Baroness Young as a “Big Brother mechanism”.⁵² The government should not intrude on the privacy of anyone’s bank account in this country without very good reason and a strong legal justification, whether a person is receiving benefits or not. People who are disabled, sick, carers, looking for work, or indeed linked to any of those people should not be treated like criminals by default. These proposals do away with the long-standing democratic principle in Britain that intrusive state surveillance should follow suspicion rather than vice versa – as such, the power undermines the presumption of innocence.

49 Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

50 DSIT, 'Impact assessment: Data Protection and Digital Information Bill: European Convention of Human Rights Memorandum', para.68: https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

51 HL Deb 19 December 2023 vol. 834, col. 2184-2185: <https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

52 HL Deb 19 December 2023 vol. 834, col. 2179-2180: <https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

Article 8 - Privacy and data protection issues

63. **The Information Commissioner does not currently view these powers as proportionate – in which case, they may be unlawful and a breach of individuals’ right to privacy protected by the Human Rights Act.** The Information Commissioner, who has responsibility for enforcing data protection legislation including the UK GDPR, has said that he has “not yet seen sufficient evidence that the measure is proportionate” and acknowledged that empowering DWP to obtain such financial details would engage Article 8 of the ECHR, as financial information pertains to individuals’ private lives.⁵³ In Big Brother Watch’s view, the powers are disproportionate and in fact privacy-altering. Indeed, the Information Commissioner further stated that he is “unable, at this point, to provide my assurance to Parliament that this is a proportionate approach.”⁵⁴

64. **The proposed power contains no data minimisation requirement and no oversight of the secret search criteria or algorithms involved.** While the explanatory notes offer search criteria examples of capital holdings or the legal limit for abroad stays, DWP’s impact assessment notes that “the power is not limited to a specific type of data”.⁵⁵ Whilst DWP may claim the search criteria will be limited to eligibility criteria, this is not stipulated on the face of the Bill. The Bill in fact permits very broad search criteria, given that the broad purpose of the regime is “identifying cases which merit further consideration” in relation to “potential” fraud and error. Further, in proposed new Schedule 3B to the SSA, sub-paragraphs 2(1)(b) and 2(1)(c) state that an AIN requires “other specified information relating to the holders of those accounts” and other connected information “as may be specified”. This would allow for an incredibly broad scope of information to be requested and stands in contrast to the GDPR principle of data minimisation.⁵⁶ The lack of legislative limitations would allow for extensive information about a person to be collected and means that the scope of scanning criteria

⁵³ Information Commissioner’s Further Response to the Data Protection and Digital Information (No. 2) Bill: (18 December 2023): <https://ico.org.uk/media/about-the-ico/consultation-responses/4027809/dpdi-commissioner-further-response-231218.pdf>

⁵⁴ Ibid.

⁵⁵ Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, p.134-135, para.1142, 7th December 2023: <https://bills.parliament.uk/publications/53323/documents/4144>; Department for Work and Pensions, DWP benefits statistics: August 2023 (15 August 2023): <https://www.gov.uk/government/statistics/dwp-benefits-statistics-august-2023/dwp-benefits-statistics-august-2023>

⁵⁶ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

could change at any time. Further, there is no oversight of the secret criteria that will be searched for using mass algorithmic surveillance.

65. **The power would create data protection conflicts for banks and other affected third parties, requiring them to breach their duty of confidence to customers.** Although paragraph 4 of proposed Schedule 3B to the SSA exonerates banks from breaches of confidence that arise from complying with an AIN, it is framed in a circular way. Paragraph 4 expressly states that the power to issue an AIN does not authorise the “processing of personal data that would contravene the data protection legislation” – but also stipulates that “in determining whether processing of personal data would do so, that power is to be taken into account” (para. 4(2)(a)). David Naylor and Malcolm Dowden of law firm Squire Patton Boggs assessed the legal uncertainty under UK GDPR arising from this as follows:

“While that provision appears to mean that a bank could not rely on Article 6(1)(c) (“processing is necessary for compliance with a legal obligation to which the controller is subject”), it would potentially be able to rely on Article 6(1)(f) (“legitimate interests”) as its lawful basis for disclosure. That position would be somewhat uncomfortable for the bank as it would be open to individuals to object to the bank’s reliance on legitimate interests, requiring a potentially costly and time-consuming balancing exercise in response to each objection received.”⁵⁷

A “legitimate interest” requires a purpose, necessity and balancing test – we believe the plan would fail to meet these tests. A reliance on “legitimate interests” to justify this extraordinary surveillance power is another way in which it is likely to be vulnerable to legal challenges.

66. **The power is particularly intrusive, as the information monitored includes special category data that invokes extra protections.** Information monitored and exchanged under AINs would give a detailed and potentially highly invasive picture of the private lives of those affected – especially for people who do not receive benefits but share an account with someone who does. Some financial data will be special category data under UK GDPR, revealing political opinions, religious and philosophical beliefs, trade

⁵⁷ David Naylor and Michael Dowden, ‘Government access to personal data in bank accounts: a compliance challenge for banks, and a threat to EU adequacy?’ (17 January 2024): <https://www.lexology.com/library/detail.aspx?g=3a4671d4-a37e-4785-80cc-36f8d3a13e75>

union memberships, health data and sexual orientation. The Information Commissioner drew attention to the likelihood of health data being processed under this power in particular.⁵⁸ In addition to an Article 6 legitimate interest, a special category condition under Article 9 must apply for the data to be lawfully processed. It is unclear which, if any, Article 9 interest could apply – given that the power does not in and of itself authorise breaches, it is unlikely to be Article 9(2)(b) (carrying out obligations under the law). The Information Commissioner advised that “government will need to consider how the relevant additional processing conditions required for such information in the UK GDPR will be met”.⁵⁹

67. The proposals could impact EU adequacy. Enacting a disproportionate and intrusive mass surveillance law would move the UK significantly away from existing data protection legislation, which is based upon EU regulations. As Lord Allan observed in relation to the EU adequacy decision:

“Bulk digital surveillance has been a point of particular concern from an EU-perspective – and bulk surveillance on a “suspicionless” basis is likely to raise significant questions.”⁶⁰

68. The power would create data security risks. Frequent searches and exchanges of masses of sensitive personal financial data within numerous third party organisations, and subsequent frequent transfers to the government, would incur security risks such as leaks, loss, theft and hacking. DWP's impact assessment says that it will ensure that data will be “transferred, received and stored safely”.⁶¹ Such a claim is dubious in light of the Department's track record of data security, considering that it was recently reprimanded by the ICO for data leaks so serious that they were reported to risk the lives of survivors of domestic abuse.⁶² With no limitations set around the type of data DWP can access, the impact could be even more severe.

⁵⁸ Information Commissioner's Further Response to the Data Protection and Digital Information (No. 2) Bill: (18 December 2023, p.5): <https://ico.org.uk/media/about-the-ico/consultation-responses/4027809/dpdi-commissioner-further-response-231218.pdf>

⁵⁹ Ibid.

⁶⁰ David Naylor and Michael Dowden, 'Government access to personal data in bank accounts: a compliance challenge for banks, and a threat to EU adequacy?' (17 January 2024):

<https://www.lexology.com/library/detail.aspx?g=3a4671d4-a37e-4785-80cc-36f8d3a13e75>

⁶¹ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf 8.

⁶² Information Commissioner's Office, Letter to the DWP (31 October 2022): <https://ico.org.uk/media/action-weve-taken/reprimands/4023126/dwp-reprimand.pdf>

Risks of automated decisions and 'Horizon-style' errors

69. **Thousands of decisions regarding the collection and reviewing of private financial information of people receiving benefits will be automated.** This is a high-risk way to make decisions, particularly in sensitive cases. The Information Commissioner has warned that the power is highly likely to involve automated decision-making:

"(...) given the volume of data involved and plans to expand how the power is used in the future, there is the potential that processing as a result of an information notice constitutes automated decision making within the definition of Article 22 of the UK GDPR. Parliamentary scrutiny will be important to determine whether this is the case (...)".⁶³

Big Brother Watch has previously expressed serious concern over disrespect for individuals' legal rights regarding automated decision-making – particularly in relation to how the Data Protection and Digital Information Bill stands to further weaken people's rights in this respect.⁶⁴ Regarding how people's data will be assessed, DWP has stated that "we are clear [...] that no automatic decisions will be made based on data alone".⁶⁵ Whilst that may be technically the case for decisions to suspend benefits, it is highly likely to be at least de facto the case in parts of the process that engage rights, such as decisions to intrude on financial privacy.

70. **There are no provisions for algorithmic transparency and accountability.** There is no information specifying who is responsible for supplying the algorithms required for this mass surveillance power. There are two options: either DWP will provide third party organisations with existing methods, or third parties will be responsible for developing and deploying their own. If the latter, third party organisations would be responsible for the expense associated with developing such systems. This could incur a

⁶³ Information Commissioner's Further Response to the Data Protection and Digital Information (No. 2) Bill: (18 December 2023): <https://ico.org.uk/media/about-the-ico/consultation-responses/4027809/dpdi-commissioner-further-response-231218.pdf>

⁶⁴ Big Brother Watch, Big Brother Watch Briefing on the Data Protection and Digital Information (No. 2) Bill for House of Commons Committee Stage (May 2023): <https://bigbrotherwatch.org.uk/wp-content/uploads/2023/05/Big-Brother-Watch-Briefing-on-theData-Protection-and-Digital-Information-2.0-Bill-for-House-of-Commons-Committee-Stage.pdf>

⁶⁵ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf

financial and operational burden on banks and other affected third party organisations. In both cases, there are serious questions around algorithmic transparency and accountability.

71. With the constant scanning of tens of millions of accounts in relation to often complex claims, false positive matches for fraud or error are highly likely. The scale of surveillance suggested by these powers is so vast that scanning for such 'indicators' will be automated. As a result, significant numbers of 'false positives' will lead to account-holders' personal details being wrongly flagged for further investigation to the government, which may incur further privacy intrusion and in some cases have more serious ramifications. When scanning 20+ million accounts, even a remarkably low error rate of 1% would lead to 200,000 people's accounts being wrongly flagged to DWP.

72. Financial institutions' 'Suspicious Activity Reports' already have a very high false hit rate. The requirement upon banks and other third parties to monitor and report on the accounts of benefits claimants is somewhat reminiscent of a bank's use of "Suspicious Activity Reports" (SARs) to combat money laundering, etc. In 2017, a study found that a sample of the largest banks reviewed approximately 16 million alerts, filed over 640,000 SARs, and showed that only 4% of those SARs resulted in law enforcement involvement.⁶⁶ Ultimately, this means that at least 90-95% of the individuals that banks reported on were innocent. The important difference between the NCA investigating financial crime, and DWP investigating suspected benefits fraud and error, is that the former are working to a criminal level of suspicion whereas DWP is not. Without that standard threshold, it is even more likely that this power will see an aggressive approach, resulting in a vast number of accounts being incorrectly flagged.

73. A related trial indicated that this extraordinary power is unlikely to be an effective measure. DWP has trialled similar measures through Proof of Concept (PoC) trials.⁶⁷ The government ran a small-scale PoC in 2017, in which a bank identified 549 accounts that received benefits payments and matched certain risk criteria (i.e., capital above benefits threshold),

⁶⁶ Bank Policy Institute, "The Truth About Suspicious Activity Reports" (22 September 2020): <https://bpi.com/the-truth-about-suspicious-activity-reports/>

⁶⁷ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf 13.

for review. The sample of cases were not randomly selected – instead, they were derived from suspicious activity reports (SARs). This means that the 'success' rate is significantly higher than what would be expected under these proposals.⁶⁸ Of this biased sample, half were deemed suitable for investigation, and subsequent action was needed to remedy either fraud or error in 62% of cases that were investigated. The government reported this as a success, but this means that fewer than 1 in 3 of the 549 SAR-flagged accounts were actionable.⁶⁹ This is a high rate of false positives, particularly in a context where being incorrectly flagged could have a serious impact on someone and even disrupt a person's ability to receive essential payments. Such a high inaccuracy rate would also undermine the argument that the powers are a proportionate interference with individuals' Article 8 right to privacy.

74. Errors resulting from the proposed surveillance power are likely to have particularly serious negative consequences for welfare recipients.

Wrongful benefits investigations can lead to burdensome documentation demands which, if not complied with accurately and in time, can lead to the suspension of benefits. In such cases, innocent and often vulnerable people may be unable to afford basic necessities such as food, medicine, or heating bills. Further, there are numerous documented cases, such as those identified in a BBC investigation, of vulnerable people dying following alleged negative actions by DWP including the wrongful suspension of benefits.⁷⁰ In a recent example, DWP falsely accused a single mother of owing £12,000 when, in actual fact, DWP owed her money.⁷¹

75. The Government must learn lessons from the Horizon scandal. Using algorithms in this high-risk context is uncomfortably reminiscent of the Horizon scandal, where hundreds of people were wrongfully prosecuted using data from faulty software – resulting in wrongful imprisonment,

⁶⁸ Department for Work and Pensions, Third Party Data Gathering Impact Assessment (IA) (September 2023): https://assets.publishing.service.gov.uk/media/6564bab01524e6000da10168/DWP_third_party_data_impact_assessment_november_2023.pdf 69.

⁶⁹ Department for Work and Pensions, Fighting Fraud in the Welfare System (26 May 2022): <https://www.gov.uk/government/publications/fighting-fraud-in-the-welfare-system/fighting-fraud-in-the-welfare-system--2#fn:1>

⁷⁰ Deaths of people on benefits prompt inquiry call – Alex Homer, BBC News, 10 May 2021: <https://www.bbc.co.uk/news/uk-56819727>

⁷¹ Isabella McRae, 'DWP falsely accuses single mum of owing £12,000 – when they actually owe her money' (16 January 2024): <https://www.bigissue.com/news/social-justice/dwp-benefits-universal-credit-money-owed-penny-davis/>

financial ruin, and suicide.⁷² Indeed, the same legal standards that saw people wrongfully convicted in relation to Horizon still apply. Courts are currently required to presume that systems operate correctly, placing the onus upon defendants to provide evidence that the system they are implicated by is flawed.⁷³ However, unlike the Horizon scandal, the individuals affected worst by this bank spying will not be small business owners but people already suffering on the poverty line, people who are vulnerable, sick or disabled or who care for vulnerable, sick or disabled people, people with mental health problems, and elderly people among others. The risks are incredibly high.

- 76. The Public Accounts Committee raised concerns about DWP's lack of algorithmic transparency.** In December 2023, the Public Accounts Committee noted that the DWP has not been clear as to what proportion of benefit claims have been subject to this algorithmic surveillance, nor has it published any assessment of the impact on customers.⁷⁴ Big Brother Watch shares the Committee's concerns about the lack of transparency surrounding these tools and the lack of consideration of claimants who may be vulnerable or from protected groups. DWP has not sufficiently addressed these problems.

Equality impact

- 77. The privacy intrusion and risks of other consequential harms will have the greatest impact on those in receipt of benefits, many of whom are in receipt of benefits due to a protected characteristic such as disability or age.** It means that some of the poorest in our society, people with disabilities or long term illnesses, carers, or even elderly people relying on pensions will be subject to their private financial data being pre-emptively intruded on by banks and other private companies they engage with, potentially examined by the government without their knowledge, and at risk of consequential harms as a result of that characteristic.

⁷² Kevin Peachey, Michael Race, and Vishala Sri-Pathma, 'Post Office scandal explained: What the Horizon saga is all about' (10 January 2023): <https://www.bbc.co.uk/news/business-56718036>

⁷³ David Allen Green, '"Computer says guilty" - an introduction to the evidential presumption that computers are operating correctly' (30 September 2023): <https://davidallengreen.com/2023/09/computer-says-guilty-anintroduction-to-the-evidential-presumption-that-computers-are-operating-correctly/>

⁷⁴ House of Commons Committee of Public Accounts, The Department for Work and Pensions Annual Report and Accounts 2022-2023 (6 December 2023): <https://committees.parliament.uk/publications/42434/documents/210942/default/>.

78. **In addition to landlords, some banks and other third party organisations may choose not to accept individuals in receipt of benefits, or treat them less favourably.** It is possible that third parties could make the decision not to accept customers on benefits, or to treat customers in receipt of benefits differently, to mitigate the potential costs and liabilities associated with processing their data for DWP or the financial penalty alternative.

79. **DWP has not done enough to assess the risks of the proposed policy discriminating against protected groups.** At the time of writing, the Government has yet to publish an Equality Impact Assessment addressing the potential impact of this unprecedented financial surveillance on people with protected characteristics, who may be disproportionately affected due to disability, age, sex and pregnancy/maternity. The National Audit Office (NAO) acknowledged that:

“When using machine learning to prioritise reviews there is an inherent risk that the algorithms are biased towards selecting claims for review from certain vulnerable people or groups with protected characteristics. This may be due to unforeseen bias in the input data or the design of the model itself.”⁷⁵

80. The NAO also stated that DWP “should be able to provide assurance that it is not unfairly treating any group of customers”. In response to the Public Accounts Committee’s report on benefits fraud and error in 2022, DWP committed to report annually to Parliament on the impact of data analytics on protected groups – however, ex post facto equality impact analysis may not satisfy the public sector equality duty, which must be fulfilled before and at the time when a policy is being considered.

81. Relatedly, the NAO reports that DWP performed a pre-launch ‘fairness’ analysis of its existing data analytics products currently in use to test for disproportionate impacts on people with the protected characteristics of age, gender and pregnancy. Reportedly, the results were largely “inconclusive” but did identify age bias towards older claimants. According to the Public Accounts Committee, DWP’s position is

⁷⁵ DWP Annual Report and Accounts 2022-3, 6 July 2023, para. 5.10, p.309: <https://assets.publishing.service.gov.uk/media/64a576d47a4c230013bba1e7/annual-report-accounts-2022-23-web-ready.pdf>

reportedly that “some level of algorithmic bias is to be expected because of how benefit payments work”.⁷⁶ This position does not necessarily conform with DWP’s legal obligations under the Equality Act, Human Rights Act and Data Protection Act. The NAO also acknowledged that DWP is unable to test conclusively for potential discrimination due to limited demographic data about claimants.⁷⁷ The Public Accounts Committee concluded that “DWP has not done enough to understand the impact of machine learning on customers to provide them with confidence that it will not result in unfair treatment”.⁷⁸

Impact on housing crisis

82. This power could decimate the private rental market for recipients of benefits. Already, there are well-documented issues with recipients of benefits being accepted as tenants by private landlords and benefits recipients are at risk of unlawful discrimination in the rental market.⁷⁹ A recent government survey found that 1 in 10 private renters – around 109,000 households – said they had been refused a tenancy in the past 12 months alone because they received benefits.⁸⁰ This is a precarious situation: due to the housing crisis, many people in receipt of benefits must rent from private landlords in order to secure housing. The unintended consequence of the rushed financial surveillance powers in this Bill will add a major new deterrent to landlords receiving rent via tenants’ housing benefit, as they will be subjected to financial surveillance across not only that bank account but all their personal financial accounts, as per the Bill. Such landlords will also be at heightened risk of DWP errors and wrongful investigations arising from the surveillance. Such an intrusive regime could decimate the private rental market for recipients of benefits by making them less desirable tenants and significantly exacerbate the housing crisis for Britain’s most vulnerable people.

⁷⁶ Committee of Public Accounts, The Department for Work and Pensions Annual Report and Accounts 2022–2023 (6 December 2023), p.18:

<https://committees.parliament.uk/publications/42434/documents/210942/default/>

⁷⁷ DWP Annual Report and Accounts 2022–3, 6 July 2023, para. 5.12, p.309:

<https://assets.publishing.service.gov.uk/media/64a576d47a4c230013bba1e7/annual-report-accounts-2022-23-web-ready.pdf>

⁷⁸ Committee of Public Accounts, The Department for Work and Pensions Annual Report and Accounts 2022–2023 (6 December 2023):

<https://committees.parliament.uk/publications/42434/documents/210942/default/> 7.

⁷⁹ Can private landlords refuse to let to benefit claimants and people with children? – House of Commons Library, October 2023: <https://researchbriefings.files.parliament.uk/documents/SN07008/SN07008.pdf>

⁸⁰ English Housing Survey 2021 to 2022: private rented sector – DLUHC, July 2023:

<https://www.gov.uk/government/statistics/english-housing-survey-2021-to-2022-private-rented-sector/english-housing-survey-2021-to-2022-private-rented-sector>

Compliance challenges for affected third party organisations

83. **Third parties face fines for failures to comply.** The proposals allow for third parties who do not comply with account notice requests to be levied with financial penalties if the Secretary of State considers that the person who has been given an AIN has failed to comply with it.
84. **The proposed power will create a significant resource burden for affected third parties.** To perform the required mass surveillance and prevent inadvertent disclosure of personal data from customers with similar names or frequently changing addresses, banks must conduct thorough data matching exercises and checks. Banks, financial service providers and other affected third parties will therefore face heightened financial and resource demands due to these requirements.⁸¹
85. **Smaller third party organisations may face significant compliance challenges.** The power to issue an AIN is not limited to a specific institution, which means banks are not the only third party that can receive such a notice. Small businesses, such as a small online platform that facilitates peer-to-peer transactions and may have minimal capacity to respond to such requests, could be levied with heavy fines of a £1,000 fixed penalty and £40 daily penalties, which can rise to £1,000 daily rate after review. Incurring penalties would be a public matter and would risk reputational damage.⁸²

An abuse of the parliamentary process

86. **This rushed power has had inadequate scrutiny as it was introduced at Report Stage in the House of Commons – almost 9 months after the DPDI Bill was introduced.** Many parliamentarians, and recently the Constitution Committee, have raised concerns about the late addition and limited debate time for these “far-reaching” powers.⁸³ Given the serious impact of such expansive surveillance powers on fundamental rights and freedoms,

81 David Naylor and Michael Dowden, 'Government access to personal data in bank accounts: a compliance challenge for banks, and a threat to EU adequacy?' (17 January 2024): <https://www.lexology.com/library/detail.aspx?g=3a4671d4-a37e-4785-80cc-36f8d3a13e75>

82 David Naylor and Michael Dowden, 'Government access to personal data in bank accounts: a compliance challenge for banks, and a threat to EU adequacy?' (17 January 2024): <https://www.lexology.com/library/detail.aspx?g=3a4671d4-a37e-4785-80cc-36f8d3a13e75>

83 Data Protection and Digital Information Bill – Select Committee on the Constitution, 2nd Report of Session 2023-4, 25 January 2024, paras 15-17: <https://committees.parliament.uk/publications/43076/documents/214262/default/>

it is entirely inappropriate that this amendment was tabled at such a late stage of the Bill alongside 239 others, as it did not allow for adequate democratic scrutiny or parliamentary debate – as Lord Bassam of Brighton said during Second Reading (HL), it is an “affront to our parliamentary system”.⁸⁴ Sir Stephen Timms MP also raised concerns about the late stage at which such significant powers were introduced during Report Stage (HC):

“It is surprising that the Conservative Party is bringing forward such a major expansion of state powers to pry into the affairs of private citizens, and particularly doing so in such a way that we are not able to scrutinise what it is planning [...] The proposal in the Bill is for surveillance where there is absolutely no suspicion at all, which is a substantial expansion the state’s power to intrude.”⁸⁵

Code of practice

87. The Government cannot offer Parliament or the public reassurance by deferring vital legal protections in favour of guidance in a possible future code of practice. Schedule 11, Part 2 states that the Secretary of State ‘may’ issue a code of practice – it is not a requirement. Nevertheless, we understand that DWP views many of the legislative gaps and serious challenges associated with this power as issues that can be addressed by a code of practice to be drafted after the enactment of the Bill. Whilst useful for providing guidelines to those using and affected by the powers, a code of practice is not enforceable and a failure to act in accordance with any future code does not make an individual liable to legal proceedings (paragraph 8).

We urge peers to oppose the Question that clause 128 and Schedule 11 stand part of the Bill.

It is vital that peers support amendments in the name of Baroness Kidron to remove Clause 128 and Schedule 11 in order to prevent expansive surveillance of millions of members of the public with disproportionate detrimental impact upon

⁸⁴ HL Deb 19 December 2023 vol. 834, col. 2210:
<https://hansard.parliament.uk/lords/2023-12-19/debates/2960AC9B-D86E-4EA1-8E4E-F3198BEE702F/DataProtectionAndDigitalInformationBill>

⁸⁵ HC Deb 29 November 2023 vol. 741 cc899-900:
<https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill>

the 40%+ of the population in receipt of or linked to benefits payments. The extraordinary power would set a deeply concerning precedent for generalised, intrusive financial surveillance in this country.

CONCLUSION

88. If passed unchanged, the Bill threatens to purge many key rights put in place to protect the British public. It is therefore not fit for purpose. We have set out some of the key ways in which this legislation poses to fundamental rights in the UK in this briefing.

89. It is vital that peers consider the impact of this Bill on the right to privacy in the course of their scrutiny. Whilst we believe that the Bill is fundamentally flawed in its approach, it suffers particularly from its weakening of data rights, expansion of ADM use, and insufficient incorporation of privacy principles into digital identity verification frameworks. Additionally, the new powers to spy on members of the public's bank accounts and for police to retain biometric data indefinitely are deeply concerning and must be removed. The legislation must be substantially altered in order to mitigate the most damaging elements for the public's human rights and fundamental freedoms.

In order to protect crucial privacy and data protection rights, peers should support amendments in the name of Baroness Kidron and Lord Clement-Jones which would remove clauses 1, 14, 128 and Schedule 11.