BIG BROTHER WATCH

Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Lords Second Reading

December 2023

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

SUMMARY

- 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 serious threat to privacy rights in the UK. Additionally, new Government amendments would allow law enforcement agencies to retain pseudonymised biometric data indefinitely – essentially facilitating a large biometric database that can be traced back to individuals.

- **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 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. The framework currently lacks important safeguards and human rights principles that prevent the broad sharing of the public's identity data beyond its original purpose. Further, 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 a non-digital ID would protect people's choice in how they choose to verify their identities and ensure that no one feels forced to hand over personal identity data online.

- **FINANCIAL SURVEILLANCE:** Government amendments to 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.

- **RETENTION OF BIOMETRIC DATA:** Other Government amendments to the Bill would drastically change the way that UK law enforcement agencies can handle biometric personal data. These amendments would allow for data received from overseas law enforcement agencies to be stored in a pseudonymised (i.e. traceable) format indefinitely.

RECOMMENDATIONS

We believe that the Bill should:

- **Remove the new definition of personal data in 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;

- **Remove clause 14** to uphold vital safeguards in the context of automated decision-making;

- **Establish a digital identity verification framework that protects users and upholds important data protection, privacy, and equality rights.** This should include establishing **a right to use non-digital verification methods** in order to protect the public's ability to choose how they express and verify their digital identity.

Additionally, we would like to highlight the harmful potential of two of the Government's proposed amendments that propose to:

- **Create expansive and disproportionate 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. It is imperative that these new powers are removed during scrutiny of the Bill;

- **Enable law enforcement agencies to retain pseudonymised biometric data indefinitely**.

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 Second Reading in the House of Lords on Tuesday 19th December 2023, we would like to draw your attention to a number of concerning issues both within the Bill and the government's proposed amendments. 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.

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

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-andsport

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/

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 the 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 the new Clause introduced to 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, 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-

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.

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.

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. Data protection expert Dr Chris Pounder explains 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.[8] 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.

11. 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".[9] 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 access the public's genetic information as a matter of routine.[10] 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.

12. 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.

8 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
9 Ibid
10 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

Clause 5 – Lawfulness of processing

13. 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. This provides businesses and other organisations with a broader scope of justification for data processing.

14. 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 of data subjects"[11] (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.

15. 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.

11 DPDI Bill, clause 5.

16. Clause 5 could allow for companies to use people's data outside of the protective influence of data protection law. As Marcus Fysh MP said at the Bill's Third Reading:

> "Before companies share data or use data, they should have to think about what the balance is between a legitimate interest and the data rights, privacy rights and all the other rights that people may have in relation to their data. **We do not want to give them a loophole or a way out of having to think about that.**"[12]

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 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.[13]

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.

12 HC Deb 29 November 2023 vol 741 cc896-897: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill

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

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. The last time MPs did not approve a statutory instrument under the affirmative procedure was 1978.[14] 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 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.

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

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).[15]

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

25. 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

15 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

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

26. Article 22(B) would maintain a general prohibition on ADM only when decisions process special category personal data e.g. ethnicity or religion.[17] 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).

27. 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."[18]

16 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
17 DPDIB Article 22B.
18 Data Protection and Digital Information (No. 2) Bill (Fouth 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

28. 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 DPDI 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.[19] 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 race[20] when processed in an algorithm. Indeed, the Public Sector Equality Duty 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."[21]

29. Algorithm Watch explains that "automated decision-making is never neutral".[22] 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;[23] welfare systems to uphold economic disparities;[24] algorithmically generated A-level grades to entrench socio-economic inequalities;[25] and recruitment systems to discriminate against women, single mothers, and people with disabilities.[26] Many of these kinds of data-driven automated decisions

19 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)

20 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-anddata-protection/how-do-we-ensure-fainess-in-ai/what-about-fairness-bias-and-discrimination/#address>

21 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

22 Algorithm Watch, 'The ADM Manifesto' https://algorithmwatch.org/en/the-adm-manifesto/

23 Student Borrower Protection Center, 'Educational Redlining' (February 2020) https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf

24 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

25 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

26 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/

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".[27]

30. 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 this technology" which, by nature, implies a corollary increase in its negative effects.[28] 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".[29] 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."[30] 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

27 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)

28 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

29 Ibid

30 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

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.

31. 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 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.

32. 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

33. 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)).

34. 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 Service[31] 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.

35. 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

31 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)

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".

36. 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 (...)".[32]

37. 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).[33]

38. Overall, the new law enforcement ADM powers will lead to a vast expansion of purely automated decisions with significant adverse

32 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

33 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

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.

39. 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.

40. **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

41. 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)).

42. 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.

43. 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.

44. 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."[34]

45. **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, 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.**

DIGITAL IDENTITY FRAMEWORK

Right to non-digital ID

46. 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.

47. 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.

48. 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

34 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))

cannot participate digitally, or can be vulnerable to hackers. 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 — this is where the issue is directly relevant to this Bill — 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."[35]

49. It is imperative that services are never contingent on a digital identity check, as this could prevent people from participating in key activities. **There should always be an offline alternative for those electing to use the online services of an organisation for which there is an offline alternative do not wish to share their information digitally, so that participation is not coercive. David Davis MP tabled a new clause that would introduce a right to use non-digital verification services and, in doing so, protect people's right to choose. As he said during debate on the amendment:**

> **"[...] 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."[36]**

50. This amendment garnered a wealth of cross-party support, with signatories including John McDonnell MP, Alistair Carmichael MP, Marcus Fysh MP, Chris Green MP, Sir Graham Brady MP, and Sir Charles Walker MP., indicating that this is an issue of shared concern.

51. 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

35 HC Deb 29 November 2023 vol 741 cc889-890: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill

36 Ibid

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.

52. 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.

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

Embedding privacy into the DVS Trust Framework

54. 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. Clause 53 (1)-(3) requires the Secretary of State publish a digital verification services (DVS) trust framework. This framework would allow authorities to disclose personal information to "trusted" digital verification services for the purpose of identity verification.

55. The Government's digital identity and verification plans, including the DVS provisions in this Bill, have the potential to give rise to excessive data sharing, privacy intrusion, and a digital identity environment that could be invasive, exclusionary and have discriminatory impacts. It is important that the Government gets the DVS framework right. Digital

verification services must be designed around users needs and reflect important data protection principles and human rights. The framework must be trusted by the public in order for it to work, which is why it is important to build it upon established principles.

56. The Identity Assurance Principles were developed by the independent Privacy and Consumer Advisory Group, which "advises the government on how to provide a simple, trust and secure means of accessing public services".[37] They build upon these concerns through a series of identity principles, offering a framework designed to cultivate trust in the Identity Assurance Service by giving "real meaning to 'individual privacy' and 'individual control'".[38]

57. The Bill gives the Secretary of State a series of new Henry VIII powers throughout its text, allowing much of the regulatory framework to be changed subject to the Secretary of State's discretion. **It is therefore vital that the Secretary of State is obligated to uphold user-centred concerns in the development of a DVS trust framework, as articulated in the 9 Identity Assurance Principles, to ensure that such services protect the people who use them.** This will help to install limitations around the purposes and substance of data sharing, which is vital in any discussion around the development of a digital verification trust framework.

FINANCIAL SURVEILLANCE

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

58. Everyone wants fraudulent uses of public money to be dealt with and the government already has powers to review the bank statements of welfare fraud suspects. 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. There are already multiple powers for this purpose: HMRC shares banking data with the DWP on an annual basis; the Proceeds of Crime Act 2002 requires banks and building societies to

37 Privacy and Consumer Advisory Group – UK Government: https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group
38 Identity Assurance Principles, 2015: https://www.gov.uk/government/publications/govuk-verifyidentity-assurance-principles/identity-assurance-principles

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.[39]

59.However, this new power would amend the Social Security Administration Act 1992 to allow the DWP to access the personal data of welfare recipients by requiring the third party served with a notice – such as a bank or building society - to conduct mass monitoring without suspicion of fraudulent activity. Schedule 11 of the DPDI Bill would add New Schedule 3B to the Social Security Administration Act; sub-paragraph 2(3)(a) states that a "matching account" that can be flagged to the government includes anyone "linked" to the receipt of a benefit - which, as per our understanding, could include ex-partners, co-habitants, children, or even landlords. Sub-paragraph 2(6) seems to say that 'linked' means the same person, but this is badly worded and unclear. This is not only is bad lawmaking, but dangerous in such a high-risk context.

60. Once issued, an account information notice requires the receiver to give the Secretary of State 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 for benefits recipients. Further, sub-paragraph 2(1)(b) and 2(1)(c) state that an account information notice requires "other specified information relating to the holders of those accounts" and other connected information "as may be specified". This vague definition would allow for an incredibly broad scope of information to be requested – something the DWP itself has acknowledged itself - and stands in contrast to the DWP's claim that they will adhere to the GDPR principle of data minimisation.[40] As Patrick Grady MP noted:

> "[...]**why is the power needed at all,** given that the Government already have the power to investigate where there is suspicion of

39 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 10.

40 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

fraud? And how can only "a minimum amount" of data be accessed when the Government say in the same breath that they want to be able to carry out those checks proactively and at scale?"[41]

61. There is no explanation provided as to how these new surveillance powers will be able to differentiate between cases of intentional fraud and accidental error. The scale of surveillance suggested by these powers is so vast that scanning for such 'indicators' is likely to be automated - therefore resulting in huge numbers of false positives. Such mistakes will have serious ramifications. Innocent people could lose their benefits for no good reason, resulting in the inability to pay heating bills, purchase medical supplies, or afford basic necessities such as food. If the DWP choose to make these decisions through human intervention, the scale of the operation will require a team so large that it will be an incredibly expensive endeavour – defeating the money-saving mandate underpinning this proposed new power.

62. Big Brother Watch finds it wholly inappropriate for the UK Government to order private banks, building societies and other financial services to conduct mass, algorithmic, suspicionless surveillance and reporting of their account holders on behalf of the state in pursuit of its policy aims. The government should not intrude on the privacy of anyone's bank account in this country without very good reason, 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. Such proposals do away with the long-standing democratic principle in Britain that state surveillance should follow suspicion rather than vice versa. It would be dangerous for everyone if the government reverses this presumption of innocence. This level of financial intrusion and monitoring affecting millions of people is highly likely to result in serious mistakes and sets an incredibly dangerous precedent.

63. The DWP's impact assessment notes that **"the power is not limited to a specific type of data"**.[42] This lack of limitation would allow for extensive information about a person to be collected. An individual's

41 HC Deb 29 November 2023 vol 741 cc891-892: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill

42 Ibid

outgoings can reveal highly sensitive information about them - what someone buys and where they spend is personal enough, but can reveal other intimate details by proxy; such as sexuality. This is incredibly intrusive, and extraordinarily so with no cap on the type of data that the DWP will be able to access.

64. The amendment allows for third parties who do not comply with account notice requests to be levied with financial penalties. The power 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 that 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.

65. This level of auditing and insight into people's private lives is a frightening level of government overreach – more so, for some of the most marginalised in society. Big Brother Watch agrees with Sir Stephen Timms MP that these powers are "extremely wide"[43] - powers that would introduce disproportionate and expansive surveillance, and sets a worrying precedent for how the government oversee, access, and use people's personal data to make hugely impactful decisions about their lives. **Such a decision will allow disproportionate and intrusive surveillance of people in the welfare system** - that means that people including some of the poorest in our society, people with disabilities (including illnesses such as cancer), carers, or even elderly people depending on pensions will be subject to their spending essentially being pre-emptively examined, rather than on suspicion. It would put some of the most marginalised and vulnerable people on trial through intrusive bank surveillance. Questions must be asked about how banks will use this data and whether this will impact people's access to financial services.

66. In addition to the serious surveillance concerns, it is unlikely to be an effective measure. The requirement upon banks to monitor and report upon the accounts of benefits claimants is reminiscent of a bank's role in combating money laundering etc, through producing

43 HC Deb 29 November 2023 vol 741 cc898-899: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBi

"Suspicious Activity Reports" (SARs). SARs have been found to be a broadly pointless measure that produce an overwhelming amount of false positives.[44] 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.[45] Ultimately, this means that 90-95% of the individuals that banks report on were likely innocent. The important difference between the NCA investigating financial crime, and the DWP investigating suspected benefits fraud *and error*, is that the former are working to a criminal level of proof of crime that the DWP are not. Without that higher level, it is even more likely that this power will see an aggressive approach, resulting in a vast number of accounts being incorrectly flagged – despite people being completely innocent.

67. In its impact statement, the DWP says that it will ensure data will be "transferred, received and stored safely".[46] Such a claim stands in stark contrast to the Department's track record of data security – particularly, 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.[47] With no limitations set around the type of data the DWP can access, the impact could be even more severe.

68. Big Brother Watch has previously expressed serious concern over impact of automated decision-making, particularly in relation to how the Data Protection and Digital Information Bill will exacerbate such effects.[48] Regarding how people's data will be assessed, the DWP has stated that "we are clear [...] that no automatic decisions will be made based on data alone".[49] However, this statement has not been reflected in any form of legally binding decision. Big Brother Watch condemns the

44 UN High Level Panel on International Financial Accountability Transparency and Integrity (FATFI), Concept Note (24 September 2020): https://uploads-ssl.webflow.com/5e0bd9edab846816e263d633/5f528f0d340d93cd49ddc726_Concept%20Note_FACTI%20interim%20report%20launch%20-%20DRAFT%204%20SEP%2020%20-%20for%20public.pdf

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

46 Ibid

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

48 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

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

proposed amendment in its entirety but would like to highlight that, given the catalogue of risks raised by automated decision-making in key areas, it is completely inappropriate to make this kind of promise in non-binding methods that are subject to change, e.g. policy or Code of Practice. The lack of legal assurance is particularly concerning given the DWP history of conducting algorithmic surveillance on people in the welfare system.[50]

69. Given the severe impact of such expansive surveillance powers on fundamental rights and freedoms, it is entirely inappropriate that this amendment was tabled at this stage of the Bill alongside 239 others on the last available day,as it has not allowed for either proper democratic scrutiny or parliamentary debate. As Sir Chris Bryant MP noted during Report Stage of the Bill, some of these amendments give new powers to ministers and "introduce completely **new topics that have never been previously mooted, debated, or scrutinised by Parliament** in relation to this Bill."[51] Sir Stephen Timms MP also raised concerns about the late stage at which such dramatic powers have been introduced:

> "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 s**ubstantial expansion of the state's powers to intrude"**[52]

70. Being a part of the benefits system is a last resort – a necessity for survival. These new powers would mean that for people who are otherwise unable to support themselves, for whatever reason, they will have to depend on a system where they are subject to intrusive surveillance and broadly without their knowledge). **Scanning data without suspicion will effectively put welfare recipients – including the poor, parents and carers and disabled people - under constant financial**

50 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
51 HC Deb 29 November 2023 vol 741 cc848-849: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill
52 HC Deb 29 November 2023 vol 741 cc899-900: https://hansard.parliament.uk/commons/2023-11-29/debates/46EF0AA6-C729-4751-A3DA-6A3683EB8B87/DataProtectionAndDigitalInformationBill

surveillance. Such measures would be a wholly unnecessary and disproportionate violation of the public's privacy and will be incredibly damaging for the most disadvantaged in our society.

71. **It is vital that these powers are removed to prevent expansive surveillance of millions of members of the public, with disproportionate detrimental impact upon people in the welfare system and individuals linked to them.**

RETENTION OF BIOMETRIC DATA

Clause 130 – "Retention of biometric data and recordable offences", Clause 131 - "Retention of pseudonymised biometric data", and new Clause 132 - "Retention of biometric data from INTERPOL"

72. Clause 130 – "Retention of biometric data and recordable offences", Clause 131 - "Retention of pseudonymised biometric data", and Clause 132 "Retention of biometric data from INTERPOL", would allow UK law enforcement agencies to hold biometric data received from overseas law enforcement agencies in a pseudonymised format. In cases where the authority ceases to hold the material pseudonymously, and the individual has no previous convictions or only one exempt conviction, the data may be retained in a non-pseudonymous format for up to 3 years. Therefore, the general rule is indefinite retention with continuous pseudonymisation, except for a specific circumstance where non-pseudonymised retention is permitted for a fixed period.

73. This is a major change in the way that personal data can be handled – permitting storage of pseudonymised or non-pseudonymised data will facilitate a vast biometric database that can be traced back to individuals. While this does not apply to data linked to offences committed in the UK, it sets a concerning precedent for reshaping how law enforcement agencies hold data, i.e. in a traceable and identifiable way. It seems that there is nothing to stop a law enforcement agency from pseudonymising data just to reattach the identifying information, which they would be permitted to hold for 3 years.

74. The clauses do not explicitly define the steps that must be taken to achieve pseudonymisation. This leaves a broad scope for interpretation

and variation in practice. The only requirement is that the data is pseudonymised "as soon as reasonably practicable", which is a totally subjective threshold.

75. The collective impact of these clauses, which were a late addition to the Bill at Report Stage in the Commons, is deeply concerning. Individuals with either no or minimal previous convictions could have their data stored pseudonymously (i.e. still traceable back to them) indefinitely, which completely contrasts the key privacy principles of necessity and proportionality. Instituting these kinds of intrusive measures is yet another example of expansive powers being ushered through under counterterror reasoning – and a slippery slope for how members of the public's data may be treated in the future, particularly with Chris Philp, Minister for Policing, calling to make the passport database more readily available to law enforcement agencies.[53]

76. **We believe these powers must be withdrawn to prevent a dangerous precedent being set for police retention of vast amounts of traceable biometric data.**

CONCLUSION

77. 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.

78. It is vital that parliamentarians 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. It is vital that the legislation is substantially altered in order to mitigate the most

53 The Guardian, 'UK Passport images database could be used to catch shoplifters' (2 October 2023): https://www.theguardian.com/uk-news/2023/oct/02/uk-passport-images-database-could-be-used-to-catch-shoplifters

damaging elements for the public's human rights and fundamental freedoms.