BIG BROTHER WATCH

Big Brother Watch Briefing on the Data (Use and Access) Bill for Second Reading in the House of Commons

February 2025

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.

Jasleen Chaggar

Legal and Policy Officer

Direct line: 07935 926492

Email: jasleen.chaggar@bigbrotherwatch.org.uk

Table of Contents

SUMMARY

- Big Brother Watch is concerned that the Data (Use and Access) (DUA) Bill threatens to weaken vital privacy and data protection rights in the UK, particularly in the context of automated decision-making where millions of individuals' rights are at stake. We urge the Government to amend the Bill to maintain strong protections in the context of automated decisions, to protect the British public's privacy rights of and uphold key rights to equality and non-discrimination.

- WEAKENING DATA RIGHTS: The DUA Bill will weaken protections around personal data processing, thereby reducing the scope of data protected by safeguards within data protection law. We are particularly concerned about the executive power to determine 'recognised legitimate interests', which will allow for more data to be processed with fewer safeguards than currently permitted.

- 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 public of the right not to be subject to solely automated decisions, which risks exacerbating the likely possibility of unfair, opaque and discriminatory outcomes from ADM systems; limiting individuals' rights to challenge ADM; permitting ADM use in law enforcement and intelligence with significant carveouts in relation to the existing safeguards ; 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, inclusive step to codify a right for members of the public to use non-digital ID where reasonably practicable. Such a right is vital to protect privacy and equality in the

digital age. The right to use a non-digital ID where practicable would protect accessibility, inclusion and people's choice in how they choose to verify their identities when accessing public and private services, legally protecting the millions of people who cannot or do not want to hand over personal identity data online where an alternative is reasonably practicable.

RECOMMENDATIONS:

1) We urge MPs to reject the new concept of 'recognised legitimate interests' and oppose Clause 70 of the Data (Use and Access) Bill.

2) We urge MPs to reject the dilution of Article 22 UK GDPR protections on solely automated decision-making, including in the context of law enforcement and intelligence agencies, and oppose Clause 80 of the Bill.

3) We urge MPs to introduce a legal right to use non-digital verification services.

INTRODUCTION

1. Big Brother Watch is concerned that the Data (Use and Access) Bill (DUA) contains grave threats to privacy and data protection rights in the UK. The Government must amend the Bill in order to protect the public from the series of harms caused by weakening fundamental data privacy rights.

2. The Bill was published on 23rd October 2024 by the Department for Science, Innovation and Technology as part of the Government's plan to "unlock the secure and effective use of data".[1] The DUA Bill borrows a significant number of provisions from the previous Conservative Government's Data Protection and Digital Information (DPDI) Bill. Many of these are broadly unchanged, and many have been reintroduced with minor changes or moved text that have little impact on said changes. Some examples of resurrected proposals include those on recognised legitimate interests, automated decision-making, and digital verification services, which are concerning given the considerable criticism many of these areas drew from experts, civil society[2] and MPs.[3]

3. The DUA Bill could have been an opportunity to build upon AI regulation and strengthen existing protections to support responsible innovation, benefiting both businesses and the public. However, instead of safeguarding the public's privacy and data rights against the risks inherent in an age of AI and increasing digitalisation, the Bill constitutes a missed opportunity replete with recycled plans that would further erode legal safeguards. While the Government has announced its ambitions to pursue AI-driven innovation, the DUA Bill simultaneously dilutes key legal rights that protect individuals when technology-fuelled processes go wrong.[4]

---

1 Department for Science, Innovation and Technology, "New data laws unveiled to improve public services and boost UK economy by £10 billion", 24 October 2024, https://www.gov.uk/government/news/new-data-laws-unveiled-to-improve-public-services-and-boost-uk-economy-by-10-billion

2 Civil society letter to Rt Hon Michelle Donelan, 7 March 2023, https://www.politico.eu/wp-content/uploads/2023/03/06/UK-civil-society-letter-DPDI.pdf; Joint letter to Rt Hon Michelle Donelan, 14 April 2023, https://defenddigitalme.org/wp-content/uploads/2024/04/DPDI-Bill-Ministers-Open-Letter-14042024.pdf

3 Public Bill Committee Stage of the Data Protection and Digital Information (No. 2) Bill, 10-23 May 2024, https://publications.parliament.uk/pa/bills/cbill/58-03/0265/PBC265_DataProtectionBill_1st-8th_Compilation_23_05_2023.pdf

4 Department for Science, Innovation and Technology, "Ensuring trust in AI to unlock £6.5 billion over next decade" 6 November 2024, https://www.gov.uk/government/news/ensuring-trust-in-ai-to-unlock-65-billion-over-next-decade

4. In anticipation of Second Reading in the House of Commons, we would like to draw your attention to several key areas where the Bill threatens to undermine critical rights, and propose areas where action is needed in order to better protect privacy rights in the UK.

5. The Retained Regulation (EU) 2016/679 (UK GDPR) provides clear regulatory responsibilities that protect privacy and data protection rights. However, with the stated aim to "harness" the power of data,[5] the DUA Bill follows in the footsteps of its predecessor, the DPDI Bill, in lowering the standard of privacy protections granted by the current UK data protection framework.[6] In addition to weakening these rights, the DUA Bill also permits the use of opaque algorithms in high-risk contexts, with fewer safeguards.[7] This would create barriers to redress, disproportionately impact marginalised individuals and groups, and empower future Secretaries of State to shape the processing of the British public's personal data on an unprecedented level.

6. The legislation engages data protection rights provided in the UK General Data Protection Regulation (UK GDPR)[8], equality rights provided in the Equality Act (2010), and privacy and equality rights enshrined in Articles 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.[9] The presumption must rest in favour of protecting these rights.

7. 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 amended in the course of its passage through parliament. 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

5 Department of Science, Innovation and Technology, 'New data laws unveiled to improve public services and boost UK economy by £10 billion' (24 October 2024): https://www.gov.uk/government/news/new-data-laws-unveiled-to-improve-public-services-and-boost-uk-economy-by-10-billion

6 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).

7 Data (Use and Access) Bill, DSIT https://bills.parliament.uk/publications/56527/documents/5211 Clause 80.

8 See in particular UK GDPR Chapter 2 on principles and Chapter 3 on rights of data subject.

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

measures to establish the right to non-digital ID and ensure that future digital identity systems uphold important principles of choice and consent.

WEAKENING DATA RIGHTS

Clause 70 – Lawfulness of processing

8. Under the current law, it is only lawful to process personal data if it is performed for at least one lawful purpose (Article 6 of the UK GDPR). One such lawful purpose 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.

9. Clause 70(2) of the DUA Bill adds to the UK GDPR's Article 6 'legitimate interest' provisions by introducing the concept of "recognised legitimate interests" (RLI). This new category would allow data to be processed without a legitimate interests balancing test for any broad "interests" designated by the Secretary of State. Schedule 4, Annex 1 in the Bill initiates the list of interests that qualify as RLIs including national security, public security and defence, emergencies, and crime – however, this is non-exhaustive.

10. The RLI list in Schedule 4, Annex 1 is incredibly broad, vague and moreover, amendable.[10] Consider the stated RLI of "crime" (paragraph 5), where efforts to tackle it can be harmful to multiple rights and have always required careful balancing - for instance, as data protection lawyer Alex Lawrence-Archer pointed out by when discussing RLIs in the DPDI Bill, a person could rely on the broad scope provided by 'crime' to film their neighbours' homes, despite the impact upon others' privacy.[11] For state actors, this broad interpretation could facilitate sweeping access to data without a balancing test, allowing government departments to process personal data with minimal justification.

10 Data Protection and Digital Information Bill as amending in Grand Committee, 25 April 2024, https://bills.parliament.uk/publications/55222/documents/4745 Annex 1

11 HC Deb 10 May 2023 c79 https://hansard.parliament.uk/commons/2023-05-10/debates/a3e435be-d416-41dd-832e-dab28622b152/DataProtectionAndDigitalInformation(No2)Bill(SecondSitting)

11. The Secretary of State can also add a new processing "interest" to Annex 1 by statutory instrument (subject to the affirmative procedure) if it meets a broad objective listed in Article 23(1)(c) to (j) of UK GDPR – this includes public security, crime prevention, public health, taxation and safeguarding the economic and financial interests of the UK, among others. 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.[12]

12. RLIs would remove the important balancing test from many areas of data processing, where that test currently protects individuals' rights and freedoms. For example, a future Secretary of State could designate "workplace productivity" as a RLI (citing the economic interests of the UK as the Article 23 purpose) which, without a balancing test, would open the floodgates to intrusive workplace surveillance and unsustainable data-driven work intensification – issues the Labour Party promised to clamp down on when in government.

13. To add additional interests to the list of RLIs, the Secretary of State need only "have regard to, among other things, the interests and fundamental rights and freedoms of data subjects"[13] (emphasis added) (new Article 6(8)). The current 'legitimate interests' test is much stronger, as the data controller cannot lawfully rely on a legitimate interests basis to process an individual's data, if the data subjects' interests override those of the data controller. By contrast, this Henry VIII power under clause 70 of the DUA Bill makes the interests and fundamental rights and freedoms of the public merely a topic that the Secretary of State need only have "regard" to.

14. There is also a question as to why the introduction of RLIs is necessary. Data processing under the proposed list of RLIs at Schedule 4, Annex 1 of the DUA would very likely be permissible under the current Article 6(1)(e), i.e. "performance of a task carried out in the public interest", or indeed under Article 6(1)(f) i.e. "legitimate interests" albeit with the important balancing test accounting for the rights and freedoms of the data

12 HC Deb 24 July 1978 vol 954 cc1289-325: https://api.parliament.uk/historic-hansard/commons/1978/jul/24/dock-labour-scheme
13 DUA Bill, clause 70.

subjects.. However, as discussed, the current proposed list is not exhaustive and can be added to.

15. The lack of necessity for RLIs was also criticised during the DPDI Bill. Baroness Jones of Whitchurch, who is leading the DUA Bill for the Labour Government in the Lords, raised concerns around the "broad" nature of the objectives when they were proposed under the DPDI Bill.[14] She rightly said:

> "There is no strong reason for needing that extra power, so, to push back a little on the Minister, why, specifically, is it felt necessary? If it were a public safety interest, or one of the other examples he gave, it seems to me that that would come under the existing list of public interests."

However, the Labour Government has reintroduced the same "extra power" with no new articulation of any "strong reason" for needing it.

16. Many other members of the House of Lords echoed these worries, with Baroness Kidron noting the unnecessary nature of such powers:

> "'Legitimate interest' is a flexible concept [...] I am somewhat bewildered as to why the Government are seeking to create change where none is needed".[15]

Further, data protection and privacy lawyer Alex Lawrence-Archer labelled the change a "radical departure" from the existing data protection framework.[16]

17. The Conservative Government argued for RLIs on the basis that companies were concerned about the legal consequences of unfairly balancing their interests with the rights and freedoms of data subjects. Some companies had expressed this in the course of a consultation undertaken by the Conservative Government to seek so-called 'Brexit

14 HL Deb 25 March 2024 vol 837 c 101GC https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill

15 HL Deb 25 March 2024 vol 837 c 106GC https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill

16 HC Deb 10 May 2023 c79 https://hansard.parliament.uk/commons/2023-05-10/debates/a3e435be-d416-41dd-832e-dab28622b152/DataProtectionAndDigitalInformation(No2)Bill(SecondSitting)

dividends' in the context of data protection law. The (then) minister Viscount Camrose explained:

> "The clause was introduced as a result of stakeholders' concerns raised in response to the public consultation Data: A New Direction in 2021. Some informed us that they were worried about the legal consequences of getting the balancing test in Article 6(1)(f) wrong."[17]

However, the purpose of a requirement for a company or organisation to balance their own interests with the rights and freedoms of data subjects is precisely to cause the consideration and apprehension described by Viscount Camrose – for the general public, this is a vital feature, not a flaw, of a meaningful data protection framework. As Viscount Colville of Culross explained during Second Reading of the DUA Bill, whilst "this power will create less friction for companies when using data for their businesses...the test must not be dropped at the cost of the rights of people whose data is being used."[18]

18. The Bill 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 resurrection of this expansive power is particularly concerning given Labour's opposition to it during the course of scrutiny of the DPDI Bill – and indeed, attempt to remove the delegated power through amendments – and concern from the Lords European Affairs Committee over how this would impact EU-UK data adequacy agreements.[19] Baroness Jones of Whitchurch, now the minister leading the Bill for the Government in the

17 HL Deb 25 March 2024 col.105GC: https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill

18 Second Reading of the Data (Use and Access) Bill in the House of Lords, HL Deb, 19 November 2024, Vol 841, col 169

19 HL Deb 25 March 2024 vol 837 c103GC: https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill ; Amendment 12, Data Protection and Digital Information Bill, https://bills.parliament.uk/bills/3430/stages/18402/amendments/10012505; Lords European Affairs Committee Letter to the Rt Hon Peter Kyle MP re: UK-EU data adequacy, 22 October 2024, https://committees.parliament.uk/publications/45388/documents/225096/default/ 3.

House of Lords, cited the concerns of the Delegated Powers and Regulatory Reform Committee during Committee Stage of the Bill regarding such measures:

> "The grounds for lawful processing of personal data go to the heart of data protection legislation and therefore in our view should not be capable of being changed by subordinate legislation."[20]

Indeed, when it reported on the Conservative Government's DPDI Bill, the Delegated Powers and Regulatory Reform Committee recommended that the equivalent power should be removed from the Bill.[21] It said it was "inappropriate" for subordinate legislation to be used to make changes to grounds that "go to the heart of data protection legislation"; further, the Committee was "not convinced that the Department (DSIT) has provided strong reasons for needing the power". Both points remain the case under the new Bill.

We have included Baroness Jones' previous comments on this matter in Annex 1 to this briefing.

20. Big Brother Watch shares these concerns, and believes that this Henry VIII power is unjustified and undermines the very purpose of data protection legislation to protect the privacy of individuals in a democratic data environment, as it vests undue power over personal data rights in the executive.

21. Clause 70 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 (clause 70(4); proposed Article 6(11)). Including direct marketing allows businesses to use the public's personal data for profit without necessarily obtaining

20 L Deb 25 March 2024 vol 837 c103GC: https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill

21 House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 2. The relevant power in the Conservatives' Bill was in clause 6: https://committees.parliament.uk/publications/43322/documents/215723/default/

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 a serious problem in terms of invasive online tracking from a profit perspective. It also fails to account for the psychological harm that targeted advertising can cause, such as the emotional toll taken upon people who have suffered a miscarriage but are hounded by adverts for baby products.[22]

22. Weakening the purposes for which personal data can be processed is an unjustified reduction of privacy rights in the UK. In its efforts to increase possibilities for data processing without balancing the interests and rights of data subjects, the DUA Bill risks leaving the public at risk of exploitation of their data.

Clause 71 – The purpose limitation

23. The principle of purpose limitation, set out in Article 5 of UK GDPR, means that data lawfully processed for one specified purpose cannot be processed for another unrelated purpose. However, Article 5 can currently be restricted by law to safeguard prevention/detection of crime, other important objectives of general public interest including the economic interests of the UK, and the protection of the data subject or the rights and freedoms of others, among other purposes. However, this exemption to purpose limitation may only apply "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society" (Article 23)(emphases added).

24. Clause 71 introduces new Article 8A to the UK GDPR, which allows the Secretary of State to pre-emptively exempt data uses from the principle of purpose limitation if the processing meets a condition as set out under a new annex to the UK GDPR (Annex 2).

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

25. The Secretary of State would be able to amend or add to the Annex 2 conditions by secondary legislation (proposed new Article 8A(5)) subject to the affirmative procedure (new Article 8A(8)) – but a condition may only be added if the Secretary of State "considers that the processing in that case is necessary to safeguard an objective listed in Article 23(1)(c) to (j)" (Article 8A(6)). It is unclear whether the reformulation of the A23 exemption leaves out safeguards contained by the current A23 exemption test – namely, that any exemption from purpose limitation "respects the essence of the fundamental rights and freedoms" and is a "proportionate measure in a democratic society". The ambiguity arising from this drafting requires clarification, as such an omission would be a worrying departure from current protections.

26. The purposes currently set out in Annex 2 are broad and include archiving in the public interest, public security, crime, safeguarding vulnerable individuals and taxation. Moreover, they are amendable. As per the proposed changes to Article 6 explored in the previous section, if a future government were to add "workplace productivity" as an Annex 2 condition (i.e. exempt from the restrictions on repurposing data), citing economic interests as the A23 objective, data collected by bosses for one purpose could be repurposed for another end. For example, data collection for the purpose of fighting retail crime could be repurposed to monitor staff productivity, (e.g. productivity algorithms or emotion recognition applied to constantly assess staff on a retailer's CCTV) opening the floodgates to intrusive workplace surveillance.

27. The Select Committee on the Constitution noted the broad scope of the Secretary of State's proposed powers in this regard during scrutiny of the DPDI Bill, recommending that Parliament consider whether such changes to the regulation of personal data should be the subject of primary rather than secondary legislation.[23] Further, the Delegated Powers and Regulatory Reform Committee recommended that the equivalent power in the Conservative Government's DPDI Bill should be removed from the Bill.[24] It said it was "inappropriate" for subordinate legislation to be used to

23 HL Select Committee on the Constitution, "Data Protection and Digital Information Bill", 25 January 2024, para. 6, p.3: https://committees.parliament.uk/publications/43076/documents/214262/default/

24 House of Lords Delegated Powers and Regulatory Reform Committee, 'Data Protection and Digital Information Bill, Pedicabs (London) Bill [HL]', 14 February 2024, HL Paper 60 of session 2023–24, p 3. The

make changes to a "fundamental principle" of the UK GDPR. Big Brother Watch agrees.

AUTOMATED DECISION-MAKING

Clause 80 - Automated decision-making

28. 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, health, education, 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.

29. 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).[25]

30. Clause 80 of the DUA Bill mimics the changes in the Conservatives' DPDI Bill to replace Article 22 with Article 22A-D, which redefines automated decisions and would enable solely automated decision-making in far wider circumstances. Proposed new Article 22A defines automated decisions; Article 22B significantly narrows the existing prohibition on automated decisions, so that it only applies to decisions based on special category (i.e. highly sensitive) personal data ; Article 22C sets out watered-down safeguards that would apply to all the newly permitted automated decisions; and Article 22D introduces Henry VIII powers for the executive to determine how the definition of automated decisions is interpreted via regulations.

relevant power in the Conservatives' Bill was in clause 6: https://committees.parliament.uk/publications/43322/documents/215723/default/

25 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

31. The Government describes the objective of the Article 22 replacement as "authorising ADM for all purposes"[26] for economic reasons, considering any interferences with the protected ECHR rights to privacy and freedom from discrimination as "justifiable (...) given the legitimate aim of ensuring the economic wellbeing of the country".[27] We are incredibly concerned about the broad reversal of the Article 22 right not to be subjected to solely automated decisions. The proposed Articles 22A-D invert the current Article 22 protections: where ADM is currently generally prohibited with specific exceptions, the Bill would broadly permit ADM and only restrict it in very limited circumstances. This would mean that ADM would likely become the norm in the UK with very few protections for the people affected.

32. The Government notes that there will be "an increase in the number of decisions made using this (ADM) technology"[28] as a result of the Article 22 reversal and that this increase "could potentially lead to discrimination under Article 14"[29] - however, also notes that "this will be from predominantly private organisations" which "will generally not raise ECHR concerns, because Article 8 ECHR will not be engaged because the controller is not an emanation of the State".[30] That is, the Government acknowledges that the Article 22 reversal risks increasing discrimination and interferences with protected rights in practice, but views the legal risks as tolerable as citizens have fewer rights protections in the context of harms caused by private companies anyway. This is a dangerously negligent approach to take to the public's rights in the context of high-risk new technologies.

Definition of meaningful human involvement

33. 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 mere administrative approval, or

26 Data (Use and Access Bill): European Convention on Human Rights Memorandum, 24 October 2024: https://bills.parliament.uk/publications/56595/documents/5246 para. 71, p.23
27 Data (Use and Access Bill): European Convention on Human Rights Memorandum, 24 October 2024: https://bills.parliament.uk/publications/56595/documents/5246 p.6
28 Ibid, para. 75, p. 23
29 Ibid. para 80, p.25
30 Ibid. para. 77, p.24

"rubber-stamping" 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.

34. However, Article 22D(1) and 22D(2) confer regulation-making powers that would allow the Secretary of State determination over when meaningful involvement has taken place, and when a decision has a "significant effect" on an individual. In effect, Article 22(D) gives total executive control over the operation of the ADM regulatory framework by way of secondary legislation. The Bill's explanatory notes claim these powers "enable the Government to provide legal clarity on the circumstances in which safeguards must apply", accounting for emerging technologies and societal expectations of what constitutes a significant decision.[31] However, Governments provide "legal clarity" by making laws, not interpreting them or controlling their application. It is wholly inappropriate to grant adjudicative, interpretative Henry VIII powers to the executive over the meaning and application of legislation passed by parliament – particularly in the case of statutory rights providing essential protections to the public at a time of expanding technological threats.

35. Whilst this Government claims that such an extraordinary executive power will "ensure individuals are protected", that is manifestly not the case – these are interpretative powers that allow the executive to declare that "there is, or is not, to be taken to be meaningful human involvement in the taking of a decision" and that a decision "is, or is not, to be taken to have a similarly significant effect for the data subject" (proposed new Article 22D (1-2)) – i.e. the executive can use this adjudicative power to waive fundamental protections. Inappropriately broad executive powers controlling the interpretation of laws designed to protect individuals' rights are not future-proof – quite the opposite. It violates the doctrine of the separation of powers and makes individuals' rights, and the very meaning of the law in question, vulnerable to changing political tides. The impartial interpretation of the law should be appropriately vested in independent courts, not politicians. The exceptional scope for political arbitration of the regulatory framework undermines its very purpose.

31 Data (Use and Access) Bill [HL] Explanatory Notes, 23 October 2024,paras. 611-612 https://bills.parliament.uk/publications/56554/documents/5227 pp.80-81.

Narrowed prohibitions on ADM

36. Automated decisions based on non-special category data will no longer be prohibited under the DUA Bill. Article 22(B) would maintain a highly narrowed prohibition on ADM, only applying when decisions involve the processing of special category personal data e.g. ethnicity or religion.[32] However, as noted by the Ada Lovelace Institute, this would still permit the automated processing of many types of data in invasive, unfair or otherwise sensitive ways without additional safeguards. For example, decisions about people could be made based on their socioeconomic status, regional or postcode data, inferred emotions, or even regional accents.[33] This greatly expands the possibilities for bias, discrimination, and a lack of transparency in a wealth of settings such as the use of emotional analysis of candidates in AI-powered hiring, despite so called "emotion recognition" technology being flagged by the ICO for being at high risk of discrimination and widely dismissed as inaccurate.[34]

37. Further, under Article 22(B), automated decisions based on special category data could still be permitted if 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 'recognised legitimate interests' for data processing, . This carveout tacitly acknowledges that these executive-made RLIs involve higher risk data processing.

38. The emaciation of Article 22 rights proposed by the DUA Bill puts marginalised groups at risk of opaque, unfair and harmful automated decisions. There is a real risk that such changes in the context of

32 DUA Bill Article 22B.
33 The Ada Lovelace Institute, Policy briefing – Data Use and Access Bill, 15th November 2024, https://www.openrightsgroup.org/app/uploads/2024/11/2024-11-BRIEFING-data-bill-second-reading-ORG.pdf 4.
34 ICO, 'Immature Biometric Technologies Could Be Discriminating Against People' Says ICO in Warning to Organisations', 26th October 2022, https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations

automated ~~decision~~making could impact rights protected by the Equality Act. In the Impact Assessment for the DUA Bill:

> "The Government acknowledges that those with protected characteristics such as race, gender, and age are more likely to face discrimination from ADM due to historical biases in datasets. To mitigate this potential impact, the bill maintains the existing limits on the lawful bases when special category data can be processed for solely ADM."[35] (emphasis added)

39. However, 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[36] when processed in an algorithm. Indeed, the Public Sector Equality Duty assessment of the DPDI Bill acknowledged 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."[37]

40. 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;[38] welfare systems to uphold economic disparities;[39] and hiring systems to discriminate candidates on the basis of personal characteristics.[40] Further,

35 Data (Use and Access Bill), Impact Assessment from DSIT, 23 October 2024: https://bills.parliament.uk/publications/56548/documents/5221 para. 531, p.163

36 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>

37 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

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

39 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

40 Information Commissioner's Office, 'ICO intervention into AI recruitment tools leads to better data protection for job seekers' 6 November https://ico.org.uk/about-the-ico/media-centre/news-and-

automated decisions are prone to serious error. Recent reports found that a DWP algorithm incorrectly flagged 200,000 people for investigation for housing benefit fraud and error.[41] Many of these kinds of data-driven automated decisions have a serious impact on people's lives and require serious safeguards, particularly as the use of technology in decision-making increases – yet this Bill would significantly deregulate ADM and remove vital safeguards for individuals' rights, transparency, scrutiny, and accountability.

41. The law currently prescribes a number of safeguards with regards to automated decisions authorised by law – namely, that the data subject has the right to request a new decision, including one that is not automated (Article 22(3)). Article 22C outlines safeguards that would apply to permitted automated decisions but, as also noted by Open Rights Group, these do not offer any additional protections or clarity when compared to those under existing Article 22.[42] This lack of enhancement is troubling in light of the fact that new Article 22 proposals significantly broaden the scope of contexts in which ADM can be employed, thereby increasing the potential for misuse or harmful errors. Lord Knight of Weymouth emphasised this point during the second reading of the DUA Bill in the House of Lords in the context of hiring, firing and management automated decisions:

"I fear that, under the Bill as drafted, those people may get a general explanation of how the automated decision-making algorithms are working, when in those circumstances they need a much more personalised explanation of why they have been impacted in this way. What is it about you, your socioeconomic status and the profile that has caused the decision to go the way it has?"[43]

Lord Davies reiterated the point during the second reading of the DUA Bill, stating, "people will struggle to get meaningful explanations about

blogs/2024/11/ico-intervention-into-ai-recruitment-tools-leads-to-better-data-protection-for-job-seekers/

41 Robert Booth, "DWP algorithm wrongly flags 200,000 people for possible fraud and error" (23 June 2024) https://www.theguardian.com/society/article/2024/jun/23/dwp-algorithm-wrongly-flags-200000-people-possible-fraud-error

42 Open Rights Group, 'Data Use and Access Bill: Briefing to the House of Lords Second reading' 14 November 2024, https://www.openrightsgroup.org/app/uploads/2024/11/2024-11-BRIEFING-data-bill-second-reading-ORG.pdf pp 6-7.

43 Hansard, Second Reading of the Data (Use and Access) Bill in the House of Lords, HL Deb, 19 November 2024, Vol 841, col 156

decisions that will deeply affect their lives and will have difficulty exercising their right to appeal against automated decisions when the basis on which the decisions have been made is kept from them."

42. As the same limited "safeguards" apply to special category and non-special category data, an affected data subject may not be notified – even where a decision has been made using their most sensitive personal data. As the (then) Labour Shadow minister Stephanie Peacock MP noted during Committee Stage of the DPDI Bill, this will exacerbate power imbalances and obstruct redress by "hiding an individual's own rights from them."[44]

Law enforcement and ADM

43. 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 80(2) and (3) would amend the Data Protection Act 2018 to reverse the current general prohibition on ADM by law enforcement. Under the DUA,only ADM that involves the processing of special category personal data by law enforcement will be prohibited (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)). For the purposes of law enforcement ADM, a decision qualifying as ADM is one that either "produces an adverse legal effect" (emphasis added) or "similarly significant adverse effect for the data subject" (s.50A(1)(b)).

44. 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, due to a vacuum of specific laws applying to new technologies. This is for case for over seven police forces, including most notably South Wales Police and the Metropolitan Police Service,[45] with regards to their use of live facial

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

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

recognition (which is currently subject to a legal challenge).[46] As such, police will be able to conduct ADM without limitation, and to conduct ADM involving sensitive data with very few limitations.

45. Unlike the proposed general prohibition on ADM involving special category personal data at proposed 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 'recognised legitimate interests' enabling data processing, made by Henry VIII powers). As such, ADM involving sensitive personal data could be used in UK policing following a political decree. Further diluted safeguards apply under proposed s.50C(3) whereby, rather than explicitly requiring the data controller to "notify" an affected individual (as is currently the case under s.50(2)(a) of the Data Protection Act 2018), they must merely create measures to provide information about the ADM and enable the subject to contest the decision.

Weakened safeguards in the law enforcement context

46. We are also concerned that s.50C(3)-(4) would exempt controllers from the need to apply even these minimal transparency and redress 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)). 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).[47] 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,

46 Landmark legal challenges launched against facial recognition after police and retailer misidentifications - Big Brother Watch, 24 May 2024: https://bigbrotherwatch.org.uk/press-releases/landmark-legal-challenges-launched-against-facial-recognition-after-police-and-retailer-misidentifications/

47 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/Poverty-Panopticon.pdf

so long as a human review of the decision takes place at some time after the fact.

47. 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" (emphases added). As Lord Holmes of Richmond remarked during the Second Reading debate on the DUA Bill in the House of Lords, "How can somebody effectively assert their right if they do not even know that AI and automated decision-making were in the mix at the time?"

48. The Government's intention is to permit secret police automated decision-making with significant adverse effects. This is made clear in the ECHR memo on the DUA Bill, which states:

> "Currently controllers processing for law enforcement purposes under Part 3 of the DPA 2018 rarely make use of automated decision-making. The requirement to inform an individual whenever automated decision-making takes places could tip off people that they are subject to investigation. As part of the changes to automated decision-making we are introducing an exemption to the safeguards which will enable the controller to review such a decision after it has been taken, instead of informing the individual at the time (...) As a result of the reforms detailed above, it is anticipated that there may be an increase in the number of decisions made using this technology."[48]

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.

49. Safeguards for law enforcement automated decision are further weakened by the new power in proposed s.50D that would allow the SoS to determine what "meaningful human input" and a "similarly significant

48 Data (Use and Access) Bill: European Convention on Human Rights Memorandum – 24 October 2024, para.74-5: https://www.gov.uk/government/publications/data-use-and-access-bill-supporting-documents/data-use-and-access-bill-european-convention-on-human-rights-echr-memorandum

adverse effect" means – i.e. what will be included or indeed exempt under the definition of a solely automated decision for law enforcement purposes. This interpretative executive power is wholly inappropriate.

50. Overall, the new law enforcement ADM powers will lead to a vast expansion of secret, 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.

51. 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 will invoke extraordinary dangers of executive-led discrimination.

52. 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 80(3) would introduce a new era of discriminatory, techno-authoritarianism in British policing.

Intelligence services and ADM

53. Clause 80(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 DUA 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)).

54. Further, clause 80(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. It is very poor law-making and illogical to define "significant effects" arising from automated decisions in multiple ways in the same Bill.

55. 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. 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. For example, an automated intelligence services

vetting system could process masses of sensitive personal data and flag individuals as suspicious, with consequential adverse employment impacts, without an opportunity for human review even being considered and in total secrecy, with no route to address. The proposed new definition of ADM is so weak as to render the proposed safeguards almost meaningless.

56. 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."[49]

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.

LAW ENFORCEMENT & NATIONAL SECURITY

Clause 81 – Logging of law enforcement processing

57. The Bill also erodes important accountability mechanisms for law enforcement. Clause 81 removes paragraphs 62(2)(a) and 62(3)(a) from the DPA, abolishing the requirement for law enforcement agencies to record the justification for searches or disclosures of personal data via

49 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))

their systems. Diluting accountability processes is the opposite of what the Bill should do, particularly given recent reports of officers using police databases to stalk members of the public.[50] The explanatory notes to the Bill justify this on the basis that an individual under investigation for inappropriately accessing personal data would not be a reliable source of information, and that systems cannot easily automatically record a justification without manual input.[51] This completely misses the point of justification and accountability processes. People should not be able to access personal data logs without a proper reason. Having a justification requirement is not a watertight defence against abuse of database system, but it acts as a procedural gateway to discourage the casual checking of these systems. It helps to encourage people to be mindful of when and why they need to access personal data, as well as engendering trust in the police's ability to engage in responsible data use.

DIGITAL IDENTITY FRAMEWORK

Right to non-digital ID

58. 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.

59. 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.

60. Digital inclusion is not only about providing training and creating routes for people who are offline to come online – it is also about accommodating for people who are not online, whether due to age, disability, financial circumstances or choice, in an increasingly digital world. Overall, 7% of UK households do not have internet access; this rises to 18% for low income

50 George Torr and Nigel Slater, 'Derbyshire officer 'used police database to find woman on Instagram' (23 March 2023) https://www.bbc.co.uk/news/uk-england-derbyshire-65031368
51 Data (Use and Access Bill) - Explanatory Notes, 23 October 2024, https://bills.parliament.uk/publications/56554/documents/5227 82.

households and 18% of people aged 65+ years respectively.[52] More than 1 in 3 over 65s (4.7 million) lack the basic skills to use the internet successfully and 1 in 6 (2.3 million) do not use it at all.[53] As Age UK set out in a recent expert report, Offline and Overlooked, "it will never be possible to get everyone online and trying to force the issue poses a real risk to older people's health, finances and ability to participate in society".[54] Ahead of the General Election, Age UK called on all parties to make sure that all public services offer and promote an affordable, easy to access, offline way of reaching and using them, and that essential private sector-run services – many of which require identity verification, including banks - should ensure that their customers can continue to meet their day-to-day needs offline.[55] Too often, organisations and companies tell customers they must complete onerous tasks online despite having physical offices and branches where an offline alternative should be quick and simple. This is all the more important where identity documents are concerned, as exchanging such sensitive data electronically can cause panic, anxiety and fraud risks for people who lack digital and basic information security skills. In practice, digital inclusion means including offline alternatives as far as is reasonably practicable. If the government is to engender trust in a digital identity framework, it must also protect non-digital identity processes.

61. Digital identity systems can 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 digitally excluded people, or be vulnerable to hackers. As David Davis MP said of the proposed digital identity framework during Report Stage of the DPDI Bill:

> "[…] 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

52 Ofcom Technology Tracker 2023: https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/data/statistics/2023/technology-tracker/technology-tracker-2023-data-tables?v=329770#page=217
53 More than 1 in 3 over 65s (4.7 million) lack the basic skills to use the internet successfully – Age UK, 2 April 2024: https://www.ageuk.org.uk/latest-press/articles/2024/more-than-1-in-3-over-65s-4.7-million-lack-the-basic-skills-to-use-the-internet-successfully/
54 Ibid.
55 Ibid.

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."[56]

62. Further, digital identity requirements risk greatly exacerbating the risks for digitally excluded groups. For instance, a 2020 National Audit Office review found that only around 20 per cent of Universal Credit applicants were able to verify their identity online, and highlighted concerns that people with low digital skills might find it particularly difficult to provide this information to submit claim applications.[57] This highlights the importance of preserving offline alternatives for people who are not able – or do not want – to prove their identity online. As stated in a report the Communications and Digital Lords Select Committee on digital exclusion, "not everyone wants to be online, or online all the time [...] accessible services and offline alternatives are essential to ensuring people are not left behind in an increasingly connected world."[58] Lord Vaux reiterated this point during the Second Reading debate of the DUA Bill, emphasising that "the "not willing" part of it is important" and explaining that people may be wary of putting detailed identity information online given the inherent security risks."[59] It is imperative that critical services are never contingent on a digital identity check, as this could prevent people from participating in key activities.

63. Indeed, Baroness Jones of Whitchurch highlighted the importance of a right to use non-digital ID during Committee Stage of the DPDI Bill:

" [...] there appear to be no assurances that people can opt out of digital verification and use offline methods of identification instead. This is particularly important for vulnerable and marginalised groups

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

57 National Audit Office, Universal Credit: getting to first payment (Session 2019-2021, HC 376) https://www.nao.org.uk/wp-content/uploads/2020/07/Universal-Credit-getting-to-first-payment.pdf 12.

58 Communications and Digital Lords Select Committee, Digital Exclusion, 29 June 2023, https://committees.parliament.uk/publications/40662/documents/198365/default/ 6.

59 HL Deb, 19 November 2024, vol 841, col 165.

who might be excluded from the technology. We need to ensure that this new system does not become compulsory by default."[60]

This sentiment was shared by cross-party peers, including Lord-Clement Jones, Lord Sikka, and Lord Vaux, who signed an amendment tabled by Lord Kamall to create the right for data subjects to use non-digital identity verification as an alternative to digital verification services, thereby preventing digital verification from becoming mandatory in certain settings.

64. 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 – a stated objective in the government's digital strategy[61] - which must exist to empower people with real choices rather than to coerce people with digital demands. As Lord Kamall said during the DPDI Bill debate,

> "a number of people will not be digitally literate or will not have this digital ID available. It is important that we offer them enough alternatives."[62]

65. A move towards digitalisation is not a justification for compelling individuals to use systems that could compromise their privacy or rights more broadly. 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.

60 HL Deb 17 April 2024 vol 837 c 339GC: https://hansard.parliament.uk/Lords/2024-04-17/debates/D7D6616F-4588-4AF9-A699-18D0582CB981/DataProtectionAndDigitalInformationBill

61 Department for Science, Innovation and Technology (DSIT), "Public dialogue on trust in digital identity services: a findings report", 28 February 2024, https://www.gov.uk/government/publications/public-dialogue-on-trust-in-digital-identity-services/public-dialogue-on-trust-in-digital-identity-services-a-findings-report

62 HL Deb 17 April 2024 vol 837 c 340GC: https://hansard.parliament.uk/Lords/2024-04-17/debates/D7D6616F-4588-4AF9-A699-18D0582CB981/DataProtectionAndDigitalInformationBill

66. 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

67. Part 2 of the Bill introduces a new regime for digital verification services. Broadly similar to the drafting of the DPDI Bill, 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 28 (1)-(3) requires the Secretary of State to 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.

68. 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. As Baroness Jones of Whitchurch said during Committee stage of the DPDI Bill, "it is vital [...] that this new system has the absolute trust of those using it".[63] Lord Clement-Jones reiterated these concerns during the Second Reading debate of the DUA Bill: "For high levels of trust in digital ID services, we need high-quality governance."[64] 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.

63 HL Deb 17 April 2024 vol 837 c 339GC: https://hansard.parliament.uk/Lords/2024-04-17/debates/D7D6616F-4588-4AF9-A699-18D0582CB981/DataProtectionAndDigitalInformationBill

64 HL Deb 19 November 2024, vol 841, col 189

69. The Identity Assurance Principles were developed by the independent Privacy and Consumer Advisory Group (now the One Login Inclusion and Privacy Advisory Group (OLIPAG)), which "advises the government on how to provide a simple, trust and secure means of accessing public services".[65] 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'".[66] As a Shadow minister, Stephanie Peacock MP spoke to the importance of these principles during Second Reading of the DPDI Bill, questioning their absence as they "would give people the reassurance to trust that the framework is in keeping with their needs and rights, as well as those of industry".[67]

70. Part 2 of the Bill gives the Secretary of State a series of new Henry VIII powers, allowing much of the DVS framework to be changed subject to the Secretary of State's discretion. The government has failed to justify why the 9 Identity Assurance Principles have not been included in the DVS trust framework as a protective measure for people using such services, given their recognised ability 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.

WEAKENING ACCOUNTABILITY

Clause 45 - Power of public authority to disclose information to registered person

71. Clause 45 authorises personal data sharing from government for digital identification verification. The DPDI's Bill's impact assessment described what this means in practice, which is relevant to the DUA Bill given that clause 45 is modelled on the DPDI's clause 74:

> "the individual will create an online account with that organisation through which they will request the organisation verifies their identity

65 Privacy and Consumer Advisory Group – UK Government: https://www.gov.uk/government/groups/privacy-and-consumer-advisory-group
66 Identity Assurance Principles, 2015: https://www.gov.uk/government/publications/govuk-verifyidentity-assurance-principles/identity-assurance-principles
67 HC Deb 18 May 2023 col 201 https://hansard.parliament.uk/Commons/2023-05-18/debates/b305ad5e-ca7b-4761-b981-96694ebe0d1d/DataProtectionAndDigitalInformation(No2)Bill(FifthSitting)#contribution-9B612F59-7DE5-4CCD-B897-D4F3CE4A9B2A

or certain attributes about them against information held by a public authority which can be passed on to the relying party."[68]

72. Given that the drafting of clause 45 is identical to clause 74 in the DPDI bill, this suggests that public authorities will have a giant database of population-level ID information that can be repurposed under the broad mandate of identity verification. Under clause 51, the Secretary of State will be able to access information that they "reasonably require" to carry out their functions. However, it is unclear whether this refers to obtaining mass identity data from DVS providers or auditing the DVS providers themselves. If enabling the former, this would raise significant privacy concerns - Big Brother Watch has previously warned[69] against the slippery slope of pervasive surveillance brought about by such databases and strongly opposes mass centralised libraries of digital IDs, as well as any broad data-sharing systems that facilitate the unconsented spread of personal identity information beyond the purpose for which it is originally provided. Alternatively, if it focuses on auditing DVS providers, the scope and safeguards for such oversight need further clarity to ensure this power does not result in excessive intrusion or access to sensitive identity information.

WEAKENING THE ICO

73. Although the DUA Bill has not retained some of the most harmful provisions of the DPDI Bill concerning the role of the ICO, such as the power of the SoS to influence its 'strategic priorities', we are concerned about the Bill's potential to give the SoS undue influence over the Commission's decision-making processes in such a way that threatens to jeopardise the ICO's status as an impartial regulator. Clause 91 introduces new section 120B to the Data Protection Act, which requires the ICO to carry out its functions with regard to "the desirability of promoting "innovation" and "competition". This characterises the public's data as a

68 Department for Science, Innovation and Technology, 'Impact Assessment: Data Protection and Digital Information (No. 2) Bill: European Human Rights Memorandum', updated 18 July 2024, https://www.gov.uk/government/publications/data-protection-and-digital-information-bill-impact-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum#:~:text=In%20practice%20this%20means%20the,on%20to%20the%20relying%20party.

69 Big Brother Watch, 'Submission to the Cabinet Office's consultation on draft legislation to support identity verification' (February 2023) https://bigbrotherwatch.org.uk/wp-content/uploads/2023/02/BBW-Response_Digital-Legislation-Consultation_Final.pdf

resource ripe for exploitation, rather than private information that warrants protection. Imposing business interests upon the functions of the ICO undermines its core purpose of regulating data protection in the UK. As the ICO is also responsible for monitoring government data activities, it further jeopardises its role as an independent regulator.

74. Part 6 of the Bill proposes abolishing the office of the Information Commissioner and establishing a new body corporate, the Information Commission, under the increased authority of the Secretary of State. Schedule 14 introduces new Schedule 12A, which grants the SoS new powers to appoint members of the Commission – marking a significant shift from the current ICO, which operates with a more independent governance structure suited to an impartial regulator. This risks inappropriately politicising the UK's data protection watchdog, placing it under direct government influence and potentially compromising its ability to act independently. Such a move could erode public confidence in the Commission's role as an unbiased protector of data rights, undermining trust in the regulatory oversight essential to safeguarding personal information.

CONCLUSION

75. It is essential that MPs carefully consider the Bill's impact on the right to privacy during the course of legislative scrutiny. As the Government pushes on with its ambition of AI-driven innovation, it is vital that these objectives are underpinned by crucial rights to protect the public from the corollary risks to privacy, data protection, and equality. The Bill's most concerning issues include the executive control over data rights and the expanded use of automated decision-making. Significant amendments to the legislation are needed to protect the public's rights and mitigate these potentially harmful provisions.

ANNEX 1:

Baroness Jones of Whitchurch: comments on the Conservative Government's proposed creation of "recognised legitimate interests" during Committee Stage (HL) of the Data Protection and Digital Information Bill, March 2024

HL Deb 25 March 2024 vol. 837 col. 103GC: https://hansard.parliament.uk/lords/2024-03-25/debates/7C715124-A951-4D37-B410-C6F7BE24E78E/DataProtectionAndDigitalInformationBill

"My Lords, I thank noble Lords who have spoken to this group. As ever, I am grateful to the Delegated Powers and Regulatory Reform Committee for the care it has taken in scrutinising the Bill. In its 10th report it made a number of recommendations addressing the Henry VIII powers in the Bill, which are reflected in a number of amendments that we have tabled.

In this group, we have Amendment 12 to Clause 5, which addresses the committee's concerns about the new powers for the Secretary of State to amend new Annexe 1 of Article 6. This sets out the grounds for treating data processing as a recognised legitimate interest. This issue was raised by the noble Lord, Lord Clement-Jones, in his introduction. The Government argue that they are starting with a limited number of grounds and that the list might need to be changed swiftly, hence the need for the Secretary of State's power to make changes by affirmative regulations.

However, the Delegated Powers and Regulatory Reform Committee argues:

"The grounds for lawful processing of personal data go to the heart of the data protection legislation, and therefore in our view should not be capable of being changed by subordinate legislation".

It also argues that the Government have not provided strong reasons for needing this power. It recommends that the delegated power in Clause 5(4) should be removed from the Bill, which is what our Amendment 12 seeks to do.

These concerns were echoed by the Constitution Committee, which went one stage further by arguing:

"Data protection is a matter of great importance in maintaining a relationship of trust between the state and the individual".

It is important to maintain these fundamental individual rights. On that basis, the Constitution Committee asks us to consider whether the breadth of the Secretary of State's powers in Clauses 5 and 6 is such that those powers should be subject to primary rather than secondary legislation.

I make this point about the seriousness of these issues as they underline the points made by other noble Lords in their amendments in this group. In particular, the noble Lord, Lord Clement-Jones, asked whether any regulations made by the Secretary of State should be the subject of the super-affirmative procedure. We will be interested to hear the Minister's response, given the concerns raised by the Constitution Committee."