

BIG BROTHER WATCH

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

March 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

CONTENTS

SUMMARY.....	4
INTRODUCTION.....	5
PART 1: DATA PROTECTION.....	8
Clause 1 – Information relating to an identifiable living individual.....	8
Clause 5 – Lawfulness of processing.....	9
Clause 6 – The purpose limitation.....	11
Clause 7 – Vexatious or excessive requests by data subjects.....	12
Clause 11- Automated decision making.....	14
Law enforcement and ADM.....	20
Intelligence services and ADM.....	23
Clause 14 – Senior Responsible Individual, Clause 16 – Logging of law enforcement processing & Clause 17 – Assessment of high risk processing.....	25
Clause 27 – The Information Commissioner & Clause 28 – Strategic Priorities... ..	26
PART 2: DIGITAL VERIFICATION SERVICES.....	27
Clause 54 – Power of public authority to disclose information to registered person.....	28
PART 4: OTHER PROVISION ABOUT DIGITAL INFORMATION.....	28
Clause 79 – Storing information in the terminal equipment of a subscriber or user.....	28
CONCLUSION.....	30

SUMMARY

- **The Data Protection and Digital Information (No. 2) Bill (DPDI2 Bill) is legislation that proposes to provide a new legal framework to govern data protection and digital identity verification services in the UK. It is part of the Government's mission to build its own regulatory regime for the processing of personal data following the UK's exit from the EU in 2020.**
- **The Government claim the Bill is aimed to "simplify the UK's data protection framework with a view to reducing burdens on organisations."¹ However, the Bill would be a significant burden on UK businesses, particularly small businesses, who will have to adapt to entirely new data protection obligations under the UK's third data protection framework in five years. Businesses operating in the EU will have to navigate both the DPDI2 Bill and GDPR frameworks, or choose to follow GDPR regulations only.**
- **The Bill tears up important UK GDPR safeguards that protect the public from the unfair, opaque and potentially discriminatory impact of automated decision making. Instead of protecting against the impact of algorithmic bias, the Government offers free reign to organisations using AI systems in high-risk areas of significant consequence (e.g. welfare, policing, exam grading).**
- **Provisions throughout this Bill provide the Secretary of State with a whole host of new and disproportionate powers that evade the usual processes of democratic scrutiny. These new abilities will allow the Secretary of State to exercise political influence over both the public's personal data processing and the UK's independent data protection regulator. Not only would the powers allow the executive to change the framework, they would allow executive exemptions to evade the framework, thus undermining its very purpose.**
- **We would like to draw your attention to several of the key issues of concern within the Bill in anticipation of the Second Reading of the DPDI2 Bill in the House of Commons on Monday 17th April. We call upon Members of Parliament to ensure that much of this Bill is either revoked or significantly revised in order to protect the British public's privacy and**

¹ Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, p.10, 8th March 2023: <https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf>

data protection rights, uphold equality and non-discrimination, and defend the rule of law.

- **We believe that the Bill should:**
 - **Ensure that personal data is protected to at least as high of a standard as it is under the existing data protection framework;**
 - **Uphold vital safeguards in the context of automated decision making;**
 - **Protect the independence of the data protection regulator, and avoid excessive Henry VIII powers to permit executive exemptions from the framework.**

INTRODUCTION

1. The Data Protection and Digital Information (No. 2) Bill (DPDI2 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. It builds upon the inherently flawed foundations of its predecessor, the Data Protection and Digital Information Bill (DPDI1 Bill), introduced in July 2022 by the Department for Digital, Culture, Media and Sport (DCMS). The result is a fundamentally ill-conceived piece of legislation that threatens to weaken crucial privacy and data protection rights across the UK, as well as exacerbate inequalities and threaten the rule of law.
2. 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”,² the DPDI2 Bill drastically veers away from the privacy protecting mandate of the current UK data protection framework.³ In addition to weakening these rights, the Bill permits the use of inherently biased algorithms in high-risk contexts.⁴ This will

² Michelle Donelan, ‘Our plan for growth in the digital, cultural, media and sport spheres.’ Transcript of speech delivered at Conservative Party Conference, (3 October 2022) <https://www.conservatives.com/news/2022/our-plan-for-digital-infrastructure--culture--media-and-sport>

³ 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).

⁴ Data Protection and Digital Information (No. 2) Bill, DSIT <https://publications.parliament.uk/pa/bills/cbill/58-03/0265/220265v2.pdf> Clause 11

“unleash data discrimination”,⁵ 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.

3. The Government claims that the DPDI2 Bill would clear up confusion⁶ over data processing and protection. However, clarification is not a case where legislation is necessarily required. Connected by Data has highlighted that **most significant challenges with data sharing are often cultural and organisational, not legislative.**⁷ The government has an opportunity to develop guidance and support to build upon the current established system, rather than bulldozing existing regulations and replacing them with weaker protections. Further legislation may fail to benefit - and may even distract from - effective data sharing.
4. The Secretary of State for Science, Innovation and Technology, Michelle Donelan, has claimed the Bill was developed through a “detailed co-design process”.⁸ In reality, there has been little to no engagement with civil society or the public. Civil society has denounced the initial consultation under the previous Secretary of State Nadine Dorries as a “rigged” and potentially unlawful process.⁹ Open Rights Group has reported that if the Government had listened to the public, they would have found consistent evidence of public support for more and better regulation and the expectation for innovation to “be ethical, responsible and focused on public benefit”.¹⁰ **The Government’s cherry-picking approach to co-design has created a data protection proposal that fails to represent the people whose data is at stake or Britain’s long-term interests.**

5 Open Rights Group, Stop Data Discrimination (19 October 2022)

<https://www.openrightsgroup.org/campaign/stop-data-discrimination/>

6 Department for Digital, Culture, Media and Sport, Data Protection and Digital Information Bill: Impact Assessment Update, February 2023

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1140162/Data_Protection_and_Digital_Information_Bill_Impact_Assessment_-_June_2022.pdf 15

7 Gavin Freeguard and Paul Shepley, ‘Data-sharing during coronavirus: lessons for government’, Institute for Government (February 2023) https://www.instituteforgovernment.org.uk/sites/default/files/2023-02/Data%20sharing%20during%20coronavirus%20lessons%20for%20government_2.pdf 9.

8 Michelle Donelan, ‘Introduction of the Data Protection and Digital Information (No. 2) Bill’, Statement made in the House of Commons (8 March 2023) <https://questions-statements.parliament.uk/written-statements/detail/2023-03-08/hcws617>; Michelle Donelan, ‘Today, we announce data protection reforms. And seize a major Brexit opportunity.’ 8 March 2023 <https://conservativehome.com/2023/03/08/michelle-donelan-today-we-announce-data-protection-reforms-and-seize-a-major-brex-it-opportunity/>

9 Sophia Waterfield, ‘Data Reform Bill consultation was ‘rigged’ says civil rights groups,’ 13 June 2022 <https://techmonitor.ai/policy/privacy-and-data-protection/data-reform-bill-consultation-dcms-nadine-dorries>

10 ‘Open Rights Group Analysis: The UK Data Protection and Digital Information Bill’, Open Rights Group (19 October 2022) <https://www.openrightsgroup.org/app/uploads/2022/10/ORG-Analysis-DPDI2-2.pdf> 6.

5. Following the government's mandate to create a business-friendly system of data protection, MEPs denounced the DPDI1 Bill as **"all about growth and innovation and nothing about human rights"** and "giving in on privacy in exchange for business gain".¹¹ Human rights should not be diluted for the purpose of business interest. However, given the consensus from civil society that the DPDI2 Bill is "even worse" than its previous iteration,¹² it is clear that this is what the current proposals will do.
6. The DPDI2 Bill will amend the current data protection system rather than repeal it, which means that the UK GDPR, Data Protection Act (2018) and Privacy and Electronic Communications (EC Directive) Regulation 2003 will remain in place subject to the Bill's various amendments. As Lord Collins of Highbury has noted, this creates "a series of patchwork amendments" which "further complicates what is an overcomplex legislative area".¹³
7. 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 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 DPDI2 Bill fails even to deliver its business-first ethos, it begs the question: what's the point in it?**
8. The legislation engages data protection rights provided in the UK General Data Protection Regulation (UK GDPR)¹⁴, equality rights provided in the Equality Act (2010), and privacy and equality rights enshrined in Article 8 and 14 of the European Convention of Human Rights (ECHR). Any interference with these rights is only lawful when there is a legal basis and it is necessary and proportionate.¹⁵ The presumption must rest in favour of protecting these rights.

¹¹ Vincent Manancourt, "We were taken for fools": MEPs fume at UK data protection snub', 7 November 2022 <https://www.politico.eu/article/we-were-taken-for-fools-meps-fume-at-uk-data-protection-snub/>

¹² Sophia Waterfield, "Worse than the last version: Experts unimpressed with the new Data Protection and Digital Information Bill", 8 March 2023 <https://techmonitor.ai/policy/privacy-and-data-protection/privacy-experts-data-protection-and-digital-information-bill>

¹³ Lord Collins of Highbury speaking in the House of Lords (23 March 2023) <https://parliamentlive.tv/Event/Index/39ad3b3f-46c4-4408-882a-a6d1694496d8>

¹⁴ See in particular UK GDPR [Chapter 2](#) on principles and [Chapter 3](#) on rights of data subject.

¹⁵ The Human Rights Act, EHRC, <https://equalityhumanrights.com/en/human-rights/human-rights/-act>

9. We believe that the DPDI2 Bill is not fit for purpose. In order to protect the individual and collective privacy rights of the British public, safeguard the rule of law and uphold key rights to equality and non-discrimination, the Bill must be majorly revised in the course of its passage through parliament, or revoked.
10. This document is not a complete line-by-line analysis of the DBDIB2. However, this briefing seeks to draw parliamentarians' attention to the key threats to human rights that are raised throughout the Bill as the House of Commons prepares to scrutinise its text at Second Reading.

PART 1: DATA PROTECTION

Clause 1 – Information relating to an identifiable living individual

11. 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 is only 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.
12. 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. In practical terms, this means businesses can process more data than they are currently permitted to. This is determined by a wholly subjective test that is measured by a business's capacity and context “at the time of processing”, rather than by the nature of the data being processed. Dr Chris Pounder explains that this could mean that if a CCTV operator cannot find someone they are searching for, then searching CCTV does not qualify as processing any personal data (of this person or anyone else).¹⁶ 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

¹⁶ Chris Pounder, 'New Data Protection Bill defines "personal data" below DPA1984 threshold' (4 August 2022) <https://amberhawk.typepad.com/amberhawk/2022/08/new-data-protection-bill-defines-personal-data-below-dpa1984-threshold.html>

process the data in such a way that others can identify them. This means that more information about the public can be processed with fewer safeguards and without people's knowledge. This undermines the entire data protection framework.

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

Clause 5 – Lawfulness of processing

14. As it currently stands, the processing of personal data is only lawful if it is 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 DPDI2 Bill amends the UK GDPR's 'legitimate interest' provisions by introducing the concept of "recognised legitimate interests", 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.

15. Clause 5 would amend Article 6 of the UK GDPR to equip the Secretary of State with the power to determine these recognised legitimate interests (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"¹⁷ (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. The Bill also proposes a much more litigious data environment – whereas currently, an organisation's assessment of their lawful purposes for processing data can

¹⁷ DPDI2 Bill, Clause 5.

be challenged through correspondence or an ICO complaint, 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.

16. 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 1978.¹⁸ 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. Michael Veale, associate professor in digital rights and regulation at UCL, has highlighted the undemocratic nature of this power. He notes that the government will be able to “amend anything they feel [...] about the text of the UK GDPR through regulations, circumventing parliamentary debate”.¹⁹ 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.
17. Annex 1 of the Bill provides national security, public security and defence, emergencies, and crime as recognised legitimate interests for data processing without an assessment.
18. 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 (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

¹⁸ HC Deb 24 July 1978 vol 954 cc1289-325: <https://api.parliament.uk/historic-hansard/commons/1978/jul/24/dock-labour-scheme>

¹⁹ Michael Veale, @mikaerv, 18 July 2022 <https://twitter.com/mikaerv/status/1549094207649972224>

the public has enjoyed with regards to reducing unwanted junk mails/calls since the introduction of GDPR. This commodifies the public, rather than recognising people's rights and controls over their data.

19. Clauses 5 and 6 aim to fulfil the government's intention to "provide organisations with greater confidence about when they can process personal data without consent".²⁰ Yet this is likely to reduce individual protections. This could disproportionately impact marginalised groups and individuals who already suffer from disproportionate data collection and processing practices, such as people in the welfare system²¹, BAME people in the criminal justice systems²², or elderly people accessing their pensions. Removing processing protections will only exacerbate this burden.
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.
21. In its efforts to increase possibilities for data processing without consent, the Bill risks leaving the public at risk and with lower trust in data processing whether by the government or institutions, and the digital economy.

Clause 6 – The purpose limitation

22. 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 be restricted by law "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) to safeguard national security, defence, public security, prevention/detection of crime, other important objectives of general public interest and the protection of the data subject or the rights and freedoms of others, among other purposes.

²⁰ DSIT, 'British Businesses to Save Billions Under New UK Version of GDPR' (8 March 2023) <https://www.gov.uk/government/news/british-businesses-to-save-billions-under-new-uk-version-of-gdpr>

²¹ 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>

²² Ethnicity and the criminal justice system: What does recent data say on over-representation? (2 October 2020) <https://commonslibrary.parliament.uk/ethnicity-and-the-criminal-justice-system-what-does-recent-data-say/>

23. Clause 6 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). The Secretary of State would be able to amend or add to those conditions by secondary legislation (section 5) using the affirmative procedure (section 8) – but a condition may only be added to Annex 2 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)” (section 6). This reformulation of the A23 exemption leaves out elements of 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”. **These tests, reflecting essential tests required for a lawful interference with an individual’s privacy rights, must be added explicitly to the DPDI2 Bill.**
24. The creation of a pre-emptive list of restrictions on the Article 5 safeguard of purpose limitation, particularly absent the explicit requirement of essential proportionality tests, marks the codification and normalisation of function creep, expanding the legal basis for the public’s personal data to be used in contexts that people have not consented to.
25. A particularly alarming example of possible applications of this power is DNA testing companies. Such companies are used for ancestral tracing or to uncover potential health issues. However, this Bill will allow for sensitive genetic information to be shared outside its original purpose for a far broader range of justifications than currently possible. Repurposing data like this would be a serious invasion of privacy, but permitted by the DPDI2 Bill nonetheless. This gravely undermines privacy and data protection rights, as well as provoking serious concerns around general population surveillance.

Clause 7 – Vexatious or excessive requests by data subjects

26. Subject access requests (SARs) are an invaluable tool for promoting accountability, challenging decisions of discriminatory or harmful effect, and empowering individuals to exercise control over their data. Arguably, if an individual does not have the right to access and view their data, they cannot in practice fully exercise their data rights.

27. Where Article 12(5) of the UK GDPR allows data controllers to refuse to comply with data subject rights requests when they are “manifestly unfounded” or “excessive”, clause 7 lowers the threshold to “vexatious” or “excessive”. This mirrors the language used in refusal grounds in the Freedom of Information Act 2000 – however, this applies to individuals’ requests to access data that does not belong to them, whereas a subject access request (SAR) relates to requests to access data belonging to the individual, over which the individual has legal rights.
28. No definition of “vexatious” is provided in the Bill. The term requires the organisation in question to make an inference about why an individual wishes to exercise their data rights, which is plainly an inappropriate condition for any individual to exercise their legal rights. A non-exhaustive list of examples of vexatious requests given in the Bill, including those which intend to cause distress, are not made in good faith, or are an abuse of the process. The organisation receiving the SAR decides whether a request qualifies as vexatious, rendering it a subjective request. The proposed new Article 12A(4) requires that an organisation determines whether a request is vexatious or excessive whilst “having regard to the circumstances of the request”, which includes “the resources available to the controller” (paragraph c). This is a wholly inappropriate basis upon which to declare an individual’s request for their own personal data as vexatious or excessive and thus to refuse it. It risks creating a perverse incentive for organisations to under-resource information management, as new Article 12A may create the perception that unless they create the resources to respond to information rights requests, they do not have to.
29. Overall, new Article 12A allows companies to refuse or incur a fee for SARs much more easily, as the Bill both lowers the threshold for SAR refusals and institutes them as threshold arbiters. Indeed, this is the aim of clause 7 – the Bill’s explanatory notes state that it “allows requests made without the intention of accessing personal information to be **more easily refused or charged for than the existing threshold**”²³ (emphasis added). However, the wording in the Bill is not that requests “without the intention of accessing personal information” (which is actually the existing position in law²⁴) can be rejected but, more vaguely, that requests deemed “vexatious” can be refused. In doing so, it creates an imbalanced power dynamic that

²³ Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, p.11, para. 15, 8th March 2023: <https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf>

²⁴ What to expect after making a subject access request – ICO, <https://ico.org.uk/for-the-public/your-right-to-get-copies-of-your-data/what-to-expect-after-making-a-subject-access-request/#f> (accessed 5th April 2023)

disadvantages anyone seeking to exercise their data rights, understand how their data is being used and therefore to exercise their legal data rights.

30. Where an organisation processes data in a particularly opaque way, SARs can be a last resort for individuals to gain information about their data processing and open up data processing to vital scrutiny. For example, Big Brother Watch's 2023 report, "Ministry of Truth: the secretive government units spying on your speech", revealed that MPs, journalists, leading academics and human rights campaigners had their statements criticising government policies monitored and recorded by highly secretive government units. Those units had maintained their opacity in response to Freedom of Information requests, written parliamentary questions, and ISC calls for scrutiny – it was only SARs that allowed affected individuals, and thus the general public, to understand the nature of a major new "counter-misinformation" function of government.
31. SARs can also be a vital tool for people to exercise their data rights in highly vulnerable situations where there is already an unbalanced power relationship between data subject and controller – for example, when making welfare or immigration claims. The introduction of a subjective assessment permitting refusals into such an important area of personal data rights is unjustified, inappropriate and endangers individuals' privacy rights.

Clause 11- Automated decision making

32. 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, among other issues.
33. 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

34. Clause 11 of the DPDI2 Bill replaces Article 22 with Article 22A-D, which redefine 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.
35. 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.
36. Article 22C permits solely automated decisions based on personal data and waters down the safeguards that currently apply to permitted automated decisions. Whereas the law currently prescribes a number of safeguards with regards to automated decisions authorised by law – namely, that the controller must notify the data subject and that the data subject has the right to request a new decision (including one that is not automated) – Article 22C only requires that the controller ensures safeguards are in place (A22C(1)) and that they include measures which “provide the data subject with information” about the automated decision and enable them to make representations, contest and obtain human intervention with regard to the decision. The proposed requirement to “provide information” would seem to be a departure from the current legal requirement to “notify” an individual that they have been subjected to an automated decision – for example, this could be interpreted as a reactive responsibility if information is requested, rather than a proactive duty. It could even be interpreted as a general responsibility that could be addressed with generic references to ADM in privacy policies. The explanatory notes to the Bill clarify that newly permitted automated decisions will not require the existing legal safeguard of

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/uk-data-protection-reform>

notification, stating that only “**where appropriate, this may include notifying data subjects after such a decision has been taken**”²⁶ (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.

37. Article 22(B) would maintain a general prohibition on ADM only when decisions process special category personal data e.g. ethnicity or religion.²⁷ 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).
38. 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.
39. 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 DPDI2 Bill in fact puts them at risk. 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 race²⁸ 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

²⁶ 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>

²⁷ DPDI2 Article 22B.

²⁸ ICO, ‘What do we need to do to ensure lawfulness, fairness, and transparency in AI systems?’ (2022) <https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-do-we-ensure-fairness-in-ai/what-about-fairness-bias-and-discrimination/#address>

inevitably led to outcomes being different based on their protected characteristics, including race and sex.”²⁹

The high risk of discriminatory outcomes is a major reason why ADM has always been subjected to a general prohibition – which this Bill would reverse. Indeed, the Public Sector Equality Duty assessment for the DPDI2 Bill states: “The government acknowledges that historically automated decision making has had a disproportionately detrimental effect upon people with protected characteristics, for example on the basis of race.”³⁰

40. Algorithm Watch explains that “automated decision-making is never neutral”.³¹ 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;³² welfare systems to uphold economic disparities;³³ algorithmically generated A-level grades to entrench socio-economic inequalities;³⁴ and recruitment systems to discriminate against women, single mothers, and people with disabilities.³⁵ Many of these kinds of data-driven, automated decisions have a serious impact on people’s lives and require serious safeguards - yet this Bill would significantly deregulate ADM and remove vital safeguards for individuals’ rights, transparency, scrutiny, and accountability.

41. 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 DPDI2 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.³⁶ The impact assessment

²⁹ 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-information-bill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digital-information-no2-bill>

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-information-bill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digital-information-no2-bill>

³¹ Algorithm Watch, ‘The ADM Manifesto’ <https://algorithmwatch.org/en/the-adm-manifesto/>

³² Student Borrower Protection Center, ‘Educational Redlining’ (February 2020)

<https://protectborrowers.org/wp-content/uploads/2020/02/Education-Redlining-Report.pdf>

³³ 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>

³⁴ 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>

³⁵ 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-out-discriminatory-algorithm/>

³⁶ 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-impact->

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”.³⁷ 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.”³⁸ It is unacceptable, irresponsible, and a failure of the state to uphold its rights and equality responsibilities to legislate in a way that invokes serious risks of perpetuating discrimination based on the future publication of pre-legislative plans and vague expectations associated with experimental AI testing. It is, frankly, magical thinking. In sum, we conclude that the Government has, on its own account, introduced serious risks of proliferated discrimination its proposal to significantly expand ADM but has not been able to propose appropriate safeguards.

42. The Government’s view is that ADM will increase particularly in the private sector under the proposed legal changes and that this is not a human rights issue. DSIT states that the increased processing “will be from predominantly private organisations” who, as non-state actors, “will generally not raise ECHR concerns”.³⁹ However, it is common for private sector processing to engage rights obligations (e.g. where it is performed in service of a public sector contract). Furthermore, all organisations that provide services to the public, whether private or public sector, are prohibited from discriminating against people as per the Equality Act 2010. As acknowledged, ADM incurs risks of discrimination, and these risks will increase with the increased use of ADM, particularly in the proposed framework with reduced safeguards.

[assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum](#)

37 Ibid.

38 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-information-bill-impact-assessments/public-sector-equality-duty-assessment-for-data-protection-and-digital-information-no2-bill>

39 DSIT, ‘Impact assessment: Data Protection and Digital Information (No. 2) Bill: European Convention of Human Rights Memorandum’, para. 22 (updated 8 March 2023), <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>

43. Challenging automated decisions is not an easy process. ADM systems are predominantly opaque, shielded by proprietary and security reasoning. Big Brother Watch and other groups including Algorithm Watch and the Centre for Data Ethics and Innovation have called for increased transparency in public sector use of ADM to empower individuals and encourage public scrutiny on the impacts of automated decisions.⁴⁰ However, the 'black box' nature of algorithms means that even when access is granted it is difficult to decipher how decisions have been made.⁴¹ The United Nations Special Rapporteur on the right to privacy outlines these complexities:

"AI systems can have very complex structures between the input and output layers. By mapping several hierarchical processing layers, machine learning can become considerably more efficient (deep learning). That inevitably results in reduced traceability in AI decisions. Due to the complexity of the algorithms and the multitude of arithmetic operations performed by the machine, the deeper processing layers (hidden layers) elude transparency in the decision criteria and their weighting".⁴²

44. System complexities can therefore hinder the public's ability to challenge the arbitrary or discriminatory denial of services or goods as a result of ADM. When ADM is used to make a decision with legal or similar effect, people should be able to understand the underlying reasoning and challenge it when necessary.

45. Article 22 of the UK GDPR is significant because the right to be free from automated decisions is violated if ADM is used, unless predefined conditions are met. This means that people are not burdened with the task of proving discrimination, as the systems are rarely used in contexts of legal or similar effect in the first place.

46. A lack of human oversight fails to account for the nuances of individual circumstances, algorithmic error, and training bias. It is therefore crucial for

⁴⁰ Algorithm Watch, 'Automated Decision-Making System in the Public Sector – Some Recommendations' <https://algorithmwatch.org/en/adm-publicsector-recommendation/>; Centre for Data Ethics and Innovation, 'Review into bias in algorithmic decision-making' (27 November 2020) <https://www.gov.uk/government/publications/cdei-publishes-review-into-bias-in-algorithmic-decision-making>

⁴¹ Caragh Aylett-Bullock, 'Automating Insecurity: Decision Making In Recruitment' (13 March 2022) <https://www.humanrightspulse.com/mastercontentblog/automating-insecurity-decision-making-in-recruitment>

⁴² United Nations General Assembly 'Report of the Special Rapporteur on the right to privacy', (2021) A/HRC/46/37 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/015/65/PDF/G2101565.pdf?OpenElement>

humans to be involved throughout the life cycle of decision-making processes, where the decision is of legal or significant effect.

47. Statistical models will always fall short of the complexities of reality. Removing humans from the life cycle of decisions of legal or significant effect risks exacerbating the impact of algorithmic error and training bias, and fails to prevent the “very complex psychological and emotional processes of human knowledge and decision-making”⁴³ necessary for considering the nuance of context. Despite these risks, Article 22(C) authorises the use of ADM without the consent of people impacted by the decision. Given the already disproportionate impact of ADM on marginalised individuals and groups, critics have warned of the spectre of new forms of social control, arbitrariness and inequality that widespread use of ADM could usher in.⁴⁴
48. By providing new adjudicative powers to the Secretary of State, clause 11 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.
49. 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

50. In the context of law enforcement processing, the potential for people’s rights and liberties to be infringed upon by automated processing is extremely

⁴³ Ibid

⁴⁴ Malcolm Langford. ‘Taming the Digital Leviathan: Automated Decision Making and International Human Rights’, *American Journal of International Law* (27 April 2020) 14, 141.

serious. Clauses 11(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)).

51. 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 Service⁴⁵ 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.

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

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)

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”.

53. 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 place 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 (...).”⁴⁶

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).⁴⁷

54. Overall, the new law enforcement ADM powers will lead to a vast expansion of purely automated decisions with significant adverse impacts on people where personal data is used that, in many cases, will act as a proxy for protected characteristics, particularly race and sex. In any context, this expansion of ADM along with reduced safeguards would be dangerous. However, in a

⁴⁶ 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>

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>

context where UK policing is suffering from well-documented issues with chronic, institutionalised racism and sexism, it is recklessly so.

55. 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.
56. 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 11(3) would introduce a new era of discriminatory, techno-authoritarianism in British policing.

Intelligence services and ADM

57. Clause 11(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 DPDI2 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)).

58. Further, clause 11(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.

59. 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.

60. 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.”⁴⁸

The Minister claimed that the intelligence services may subject an individual to further surveillance as a result of automated decision-making. However,

⁴⁸ Data Protection Bill, Report stage, 2nd day, 13 December 2017 ([https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill\(HL\)](https://hansard.parliament.uk/lords/2017-12-13/debates/9622571E-8F1E-43F8-B018-C409A3129553/DataProtectionBill(HL)))

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.

61. Clause 11 should be removed and Article 22 retained to protect vital safeguards in the context of automated decision making.

Clause 14 – Senior Responsible Individual, Clause 16 – Logging of law enforcement processing & Clause 17 – Assessment of high risk processing

62. The Bill drastically erodes important accountability mechanisms through clauses 14 (Senior Responsible Individual), 16 (logging of law enforcement processing) and 17 (assessment of high risk processing).

63. Pursuant to clause 14, organisations will no longer appoint Data Protection Officers (DPOs). They will be replaced by a Senior Responsible Individual (SRI), who must be a member of senior management. Conflating data protection responsibilities with company objectives creates a conflict of interest, and ultimately reduces independent oversight over data processing activities.

64. Clause 16 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 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.⁴⁹ 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.⁵⁰ 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

⁴⁹ 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>

⁵⁰ Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, p 12.

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.

65. 'Data protection impact assessments' (DPIAs) are a method to identify and minimise the privacy and data protection risks of projects involving personal data.⁵¹ Under the UK GDPR, organisations are required to conduct a DPIA for high-risk processing activities such as large scale processing of sensitive data (e.g. health records or personal data relating to convictions) or public monitoring.⁵² Clause 17 replaces DPIAs with 'Assessments of high risk processing' (AHRPs). AHRPs do not require data controllers to conduct proportionality tests, despite these being central to privacy rights assessments. It also removes the requirement to consult with those impacted by data processing activities during the risk assessment, which will lessen understanding of impact on those most affected and potentially prevent individuals from exercising their rights as data and decision subjects.

Clause 27 – The Information Commissioner & Clause 28 – Strategic Priorities

66. Despite the Information Commissioner's desire to maintain the ICO's status as a "trusted, fair and impartial regulator",⁵³ clauses 27 and 28 threaten to politicise the UK's data protection watchdog.

67. Clause 27 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 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.

68. A further proposed addition to the DPA, section 120B, would also oblige the Commissioner to consider the importance of the "prevention, investigation,

⁵¹ ICO, Data protection impact assessments <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

⁵² ICO, When do we need to do a DPIA? <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when2>

⁵³ ICO, 'ICO statement on re-introduction of Data Protection and Digital Information Bill' (8 March 2023) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/03/ico-statement-on-re-introduction-of-data-protection-and-digital-information-bill/>

detection and prosecution of criminal offences” and “the need to safeguard public security and national security”. This exacerbates the risks of function creep that are provoked by other sections of the DPDI2 Bill. The government has proceeded with this policy, despite recognising “concerns around independence”⁵⁴ when respondents to the consultation raised the risks of politicising an impartial body.

69. Clause 28 would introduce new sections 120E and 120F to the DPA, empowering the Secretary of State to set strategic priorities for the ICO, which the ICO must pay regard to when carrying out its core functions. The statement of strategic priorities would only be subject to the negative resolution procedure, which is the weakest process of parliamentary approval. In addition, Schedule 12 seeks to overhaul regulatory oversight of the ICO by designating a new board to oversee its functions. Members may be appointed by the Secretary of State. As the board will oversee the ICO's operations, this constitutes another very concerning levying of political influence on a regulator that is supposed to be independent. Foisting government interests upon the ICO will likely undermine public trust in its impartiality.

70. These changes grant the Secretary of State authority to issue directions to the ICO, influence and interfere with its objectives and endanger the impartial application of the law. It is imperative that clauses 27 and 28 are removed in order to preserve the ICO's independence and protect its role as an office internationally renowned for upholding data and information rights.⁵⁵

PART 2: DIGITAL VERIFICATION SERVICES

71. Building on the existing framework set out in the UK digital identity and attributes trust framework – beta version,⁵⁶ the Bill introduces a new regime for Digital Verification Services (DVS). This sets out the government's vision for the rules governing the future use of digital identities, as part of the wider plans to make it quicker and easier for people to verify themselves using modern technology.

⁵⁴ Data: a new direction – government response to consultation, Department for Digital, Culture, Media & Sport (23 June 2022) <https://www.gov.uk/government/consultations/data-a-new-direction/outcome/data-a-new-direction-government-response-to-consultation#ch5>

⁵⁵ ICO, 'New UK Information Commissioner begins term' (4 January 2022) <https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/01/new-uk-information-commissioner-begins-term/>

⁵⁶ DSIT and DCMS, 'UK digital identity and attribute framework – beta version' (13 June 2022) <https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-beta-version>

Clause 54 – Power of public authority to disclose information to registered person

72. Clause 54 authorises personal data sharing across government for digital identification verification. The Bill’s impact assessment describes what this means in practice:

“the individual will create an online account with that organisation through which they will request the organisation verifies their identity or certain attributes about them against information held by a public authority which can be passed on to the relying party.”⁵⁷

73. 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 58, the Secretary of State will be able to access information that they “reasonably require” to carry out their functions. Big Brother Watch has previously warned⁵⁸ against the slippery slope of pervasive surveillance brought about by such databases. **We strongly oppose mass centralised libraries of digital IDs, as well as any broad data-sharing systems that facilitate the spread of personal identity information beyond the purpose for which it is originally provided.**

PART 4: OTHER PROVISION ABOUT DIGITAL INFORMATION

Clause 79 – Storing information in the terminal equipment of a subscriber or user

74. Clause 79 provides new rules around the use of cookies. Cookies are small text files that can be saved on a user’s device when visiting a website. They “act as a memory” of what has happened when a device interacts with a website⁵⁹ and can “store a wealth of data, enough to potentially identify you without your consent”.⁶⁰

75. Given the amount of information they contain, cookies can qualify as personal data. They provide companies with information ripe for monetisation, which

⁵⁷ DSIT (n29).

⁵⁸ 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

⁵⁹ DCMS, ‘Research into consumer understanding and management of internet cookies and the potential impact of the EU Electronic Communications Framework’ (April 2011) <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/77641/PwC_Internet_Cookies_final.pdf> 1

⁶⁰ Cookies, the GDPR, and the ePrivacy Directive: <https://gdpr.eu/cookies/>

makes them a resource often exploited by advertising technology and surveillance advertising companies. This supports widespread online surveillance and behavioural profiling for business gain.⁶¹ Open Rights Group have explained that such practices can result in predatory and damaging targeting of vulnerable groups, such as gambling addicts.⁶²

76. Under the UK GDPR and PECR, cookies and other similar technologies can only be used to store or access information on a person's terminal equipment without consent where it is "strictly necessary", e.g. website functionality or security purposes.⁶³ These permissions are actioned by platforms through consent pop-ups, commonly known as cookie banners. Cookie banners are broadly criticised as flawed⁶⁴ and "irritating"⁶⁵, which is one of the key areas the DPDI2 Bill clumsily seeks to address. While acknowledging the imperfectness of the current cookie system and the reasoning behind attempts to address it, it is imperative that vital data protection and privacy rights are not sacrificed on the false promise of convenience.

77. Clause 79 widens the situations where cookies and other similar technologies can be used without a person's consent, thereby weakening protections against online surveillance. It moves from a 'opt-in' model of consent to an 'opt-out' model in situations that are considered 'low-risk' to privacy.⁶⁶ This includes, but is not limited to, improving a service via web analytics, installing automatic software and security updates, improving platform functionality and identifying a person's geo-location in an emergency.⁶⁷ It remains to be seen how function creep will be discouraged in the broad scope of exceptions granted to the requirement for explicit consent. An 'opt-out' model treats consent as tacit, contravening the important principle of data protection by design and default.⁶⁸ It goes against the ICO's guidance that consent must be regularly reaffirmed and not "bundled up as a condition of service".⁶⁹ Processing increased volumes of personal data without the explicit provision

61 Privacy International, 'Most cookie banners are annoying and deceptive. This is not consent' (21 May 2019) <https://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent>

62 Open Rights Group (n8).

63 Article 4(11) of the Privacy and Electronic Communications (EC Directive) Regulations 2003: <https://www.legislation.gov.uk/ukxi/2003/2426>

64 See for example, 'EDPB adopts Guidelines on Right of Access and letter on cookie consent' European Data Protection Board (19 January 2022) https://edpb.europa.eu/news/news/2022/edpb-adopts-guidelines-right-access-and-letter-cookie-consent_en

65 Matt Warman, 'Data Protection and Digital Information Statement', Transcript of statement delivered in the House of Commons (18 July 2022) <https://questions-statements.parliament.uk/written-statements/detail/2022-07-18/hcws210>

66 Data Protection and Digital Identity 2.0: Explanatory Notes (2023) <https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf> 75

67 DPDI2 Bill Explanatory Notes (n50) 76

68 See UK GDPR article 25: <https://www.legislation.gov.uk/eur/2016/679/article/25>

69 ICO, 'Lawful Basis for Processing: Consent' (22 March 2018) <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent-1-0.pdf>

of proper and informed consent is deeply worrying, as it will see an increase in unwanted data harvesting. This is particularly concerning where data relates to vulnerable groups who may be more susceptible to data exploitation and targeted marketing e.g. children, elderly people, people with disabilities, or people with mental health conditions.

78. Clause 79(3) enables the Secretary of State to issue regulations requiring providers of services, such as web browsers, to allow people to express their cookie consent preferences to all websites in a one-off agreement. It is difficult to suggest that any general agreement provided by a user could satisfy informed consent requirements, as people cannot possibly know what cookies they are agreeing to for websites they haven't visited yet.

79. We believe that Clause 79 must be withdrawn and revised with stronger protections to remove its insufficient approach to obtaining consent.

CONCLUSION

80. The ICO UK Information Commissioner, John Edwards, has said that "privacy is a right, not a privilege".⁷⁰ The DPDI2 Bill fails to codify this, instead threatening 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.

81. 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 provision of measures that grant the Secretary of State excessive powers across the board. It is vital that the legislation is substantially altered in order to mitigate the most damaging elements for the public's rights.

⁷⁰ ICO (n55)