BIG BROTHER WATCH

Big Brother Watch Briefing on the Data Protection and Digital Information 2.0 Bill for House of Commons Committee Stage

May 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

Big Brother Watch believes that the Data Protection and Digital Information (No. 2) Bill (DPDI2 Bill) threatens to greatly weaken the existing data protection framework and is not fit for purpose. The Bill must be majorly revised in the course of its passage through parliament or revoked in order to protect the individual and collective privacy rights of the British public, safeguard the rule of law, and uphold key rights to equality and non-discrimination.

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 this framework.

DATA RIGHTS: The DPDI2 Bill will dilute protections around personal data processing, thereby reducing the scope of data protected by safeguards within data protection law. We are particularly concerned about the provisions that change the definition of personal data and the purposes for which it can be processed. Essentially, more data will be processed with fewer safeguards as it will no longer meet the threshold of personal data. Such a combination is a serious threat to privacy rights in the UK.

AUTOMATED DECISION-MAKING: Where automated decision-making (ADM) is currently broadly prohibited with specific exceptions, the Bill would permit it except for in a limited set of circumstances. This will strip the right not to be subject to solely automated decisions, which carries severe consequences of exacerbating the high risk of discriminatory outcomes inherent in ADM systems; permitting ADM use in law enforcement and intelligence with few safeguards for special category data; as well as giving the Secretary of State executive control over the ADM regulatory framework through secondary legislation.

DIGITAL IDENTITY FRAMEWORK: The Bill introduces a new regime for digital verification services. It sets out a series of rules governing the future use and oversight of digital identities as part of the government's roadmap towards

digital identity verification. The framework currently lacks important safeguards and human rights principles that prevent the broad sharing of the public's identity data beyond its original purpose.

DEMOCRACY - THE ICO'S INDEPENDENCE AND HENRY VIII POWERS: The DPDI2 Bill threatens the rule of law and risks politicising a key independent regulator. By simultaneously empowering the Secretary of State to issue the ICO with strategic directions and obligating the ICO to consider innovation and competition when carrying out its functions, the Bill completely undermines the impartiality of the UK's data protection watchdog. It further undermines the rule of law by empowering the Secretary of State to make executive exemptions from the data protection framework with minimal levels of democratic scrutiny. These new powers include amending the purposes for which data can be processed outside of its original purpose; making exemptions to the ADM framework; exempting law enforcement from compliance with data protection law under the broad mandate of national security; and changing the way the public's cookies data is collected online.

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",[1] the DPDI2 Bill drastically veers away from the privacy protecting mandate of the current UK data protection framework.[2] In addition to weakening these rights, the Bill permits the use of inherently biased algorithms in high-risk contexts.[3] This will "unleash data discrimination",[4] create barriers to redress, disproportionately impact marginalised individuals and groups, and empower the Secretary of State to shape the regulation and processing of the British public's personal data on an unprecedented level.

3. The Government claims that the DPDI2 Bill would clear up confusion[5] 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**.[6] The government has an opportunity to develop guidance and support to build upon the current established system,

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

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

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

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

5 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

6 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.

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".[7] 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.[8] 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".[9] **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. 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".[10] 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,[11] 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

7 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-brexit-opportunity/

8 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

9 '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-DPDIB-2.pdf 6.

10 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/

11 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

Highbury has noted, this creates "a series of patchwork amendments" which "further complicates what is an overcomplex legislative area".[12]

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)[13], 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.[14] The presumption must rest in favour of protecting these rights.

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 this briefing seeks to draw parliamentarians' attention to the key threats to data protection, equality and human rights that are raised throughout the Bill as the Committee prepares to scrutinise its text at Committee Stage.

12 Lord Collins of Highbury speaking in the House of Lords (23 March 2023) https://parliamentlive.tv/Event/Index/39ad3b3f-46c4-4408-882a-a6d1694496d8
13 See in particular UK GDPR Chapter 2 on principles and Chapter 3 on rights of data subject.
14 The Human Rights Act, EHRC: https://www.legislation.gov.uk/ukpga/1998/42/schedule/1.

DILUTING INDIVIDUAL RIGHTS

Clause 1 – Information relating to an identifiable living individual

Amendment:

Amendment 1: MPs should give notice of their intention to oppose the question that clause 1 stand part.

Effect of the amendment:

The Bill's proposed new definition of personal data in clause 1 is unstable and subjective, and threatens to weaken individual's data rights, encourage increased processing of the public's data, and undermine the entire data protection framework. Leaving out clause 1 would prevent the government from anchoring the definition of personal data to a data processor's capacity - rather than the nature of the data being processed - thereby limiting the circumstances in which a person may be identifiable.

Briefing:

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 only qualifies as personal data if it relates to an individual who is identifiable by a data controller/processor by "reasonable means at the time of the processing", or if the data controller/processor ought to "reasonably know" that another person will be able to obtain the information as a result of the processing and identify the individual "by reasonable means" at the time of processing.

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, businesses will be able to process more data than they are currently permitted. 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. Data protection expert Dr Chris Pounder explains how this could increase data processing with minimal safeguards in the context of facial recognition CCTV, as

the threshold for personal data would only be met if the data subject is on a watch-list and therefore identified.[15] If an individual is not on a watchlist and the camera images are deleted instantly after checking the watchlist, then the data may not be considered personal and therefore would not qualify for data protection obligations. This would put the UK completely out of step with the rest of Europe, which is legislating against facial recognition surveillance – not legislating to permit less safe use of it.

13. This new clause would permit the widespread operation of facial recognition CCTV systems across the UK – systems that can be legally operated outside of data protection purview and used "more or less in secret".[16] The new definition could also mean that pe**rsonal photos scraped from the internet and stored to train an algorithm may no longer be seen as personal data, so long as the controller does not recognise the individual; is not trying to identify them; and will not process the data in such a way that others can identify them. The Bill will allow for more information about the public to be processed than ever before, with fewer safeguards and without people's knowledge. This undermines the entire data protection framework.**

14. 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

Amendments:

Amendment 2 : Clause 5, Page 6, leave out lines 15-19

Amendment 3: Clause 5, Page 6, leave out subsections (4), (5), and (6).

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

16 Ibid

Effect of the amendments:

These amendments remove the power for the Secretary of State to create "recognised legitimate interests", thereby removing the power to predefine and preauthorise data processing outside of the usual legally-defined route. Instead, the current test would continue to apply in which personal data can only be processed in pursuit of a legitimate interest, as balanced with individual rights and freedoms. This is important to avoid a two-tier data protection framework in which the SoS can decide that certain processing is effectively above the law.

Briefing:

15. Processing personal data is currently only lawful if it is performed for at least one lawful purpose, one of which is that the processing is for legitimate interests pursued by the controller or by a third party, except where those interests are overridden by the interests or fundamental rights of the data subject. As such, if a data controller relies on their 'legitimate interests' as a legal basis for processing data, they must conduct a balancing test of their interests and those of the data subjects. Clause 5 of the 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.

16. 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.

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

17 DPDI2 Bill, Clause 5.

18. The Bill would give the Secretary of State the power to determine "recognised legitimate interests" through secondary legislation, which is subject to minimal 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 or permitted to do, all based upon the Secretary of State's inclination. **Big Brother Watch is concerned that this Henry VIII power is unjustified and undermines the very purpose of data protection legislation**, which is to protect the privacy of individuals in a democratic data environment, as it vests undue power over personal data rights in the executive.

19. 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.

20. 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 security (subsection 9). Including direct marketing allows businesses to use the public's personal data for profit without necessarily obtaining consent. This appears to be a significant watering down of current standards and is a retrograde step, undoing the significant benefits the public has enjoyed with regards to reducing unwanted junk mail/calls since the introduction of GDPR. This treats the public as commodities, rather than recognising people's rights and controls over their data.

21. 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".[19] However, this is likely to reduce individual protections and disproportionately impact marginalised groups and individuals who already suffer from disproportionate data collection and processing practices, such as

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

19 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

people in the welfare system[20], BAME people in the criminal justice systems[21], or elderly people accessing their pensions. Removing processing protections will only exacerbate this burden.

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

Clause 6 – The purpose limitation

Amendment:

Amendment 4: Clause 6, Page 8, line 34, leave out subsection (5)

Amendment 5: Clause 6, Page 9, line 21, leave out subsection (6)

Amendment 6 : Clause 6, Page 9, line 7, leave out sections 5-8.

Effect of the amendments:

This group of amendments removes the disproportionate power granted to the Secretary of State to amend exemptions from the purpose limitation principle. If left untreated, this power would lead to the public's personal data being processed in ways that are incompatible with human rights and democratic values, and subject to political whim.

Briefing:

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 "when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society"

20 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

21 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/

(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.

24. 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".

25. 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.

Clause 7 – Vexatious or excessive requests by data subjects

Amendment:

Amendment 7: MPs should give notice of their intention to oppose the question that clause 7 stand part.

Effect of the amendment:

This seeks to preserve the current threshold by which organisations can refuse to respond to subject access requests. In doing so, it seeks to uphold the public's data rights including the right to access, rectification, erasure and restriction of personal data.

Briefing:

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"[22] (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 law[23]) can be rejected but, more vaguely, that requests deemed "vexatious" can be refused. In doing so, it creates an imbalanced power dynamic that 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.

22 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

23 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)

AUTOMATED DECISION-MAKING

Clause 11 - Automated decision-making:

Amendment 8: MPs should give notice of their intention to oppose the question that clause 11 stand part.

Effect of the amendment:

Rejecting clause 11 upholds the right not to be subject to solely automated decisions as provided in Article 22 of the UK GDPR. In doing so, it guards against the high risk of discriminatory outcomes inherent in ADM systems; law enforcement and intelligence agencies using special category data in ADM with little to no safeguards; as well as providing the Secretary of State with the ability to shape the ADM regulatory framework through secondary legislation.

Briefing:

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, amongst 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).[24]

34. Clause 11 of the DPDI2 Bill replaces Article 22 with Article 22A-D, which redefines automated decisions and would enable solely automated decision-making in far wider circumstances. Big Brother Watch welcomes the clarification in Article 22A(1)(a), which we have long called for, defining a decision based on solely automated processing as one that involves "no

24 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

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 notification, stating that only "**where appropriate**, this **may** include notifying data subjects after such a decision has been taken"[25] (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.

25 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

37. Article 22(B) would maintain a general prohibition on ADM only when decisions process special category personal data e.g. ethnicity or religion.[26] 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 race[27] when processed in an algorithm. Indeed, the Public Sector Equality Duty assessment of the Bill acknowledges this issue in its recounting of the automated A-Level grading scandal:

> "Though precautions were taken to prevent bias based on protected characteristics, the profiles of those attending different schools inevitably led to outcomes being different based on their protected characteristics, including race and sex."[28]

40. 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

26 DPDI2 Article 22B.
27 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-fainess-in-ai/what-about-fairness-bias-and-discrimination/#address>
28 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

has had a disproportionately detrimental effect upon people with protected characteristics, for example on the basis of race."[29]

41. Algorithm Watch explains that "automated decision-making is never neutral".[30] 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;[31] welfare systems to uphold economic disparities;[32] algorithmically generated A-level grades to entrench socio-economic inequalities;[33] and recruitment systems to discriminate against women, single mothers, and people with disabilities.[34] 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.

42. 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.[35] The impact assessment also acknowledges that the Bill "will make it more feasible for public authorities processing for law enforcement purpose to make automated decisions" but stated that the framework has "strong safeguards".[36] 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

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

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

32 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

33 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

34 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/

35 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-assessments/data-protection-and-digital-information-no-2-bill-european-convention-on-human-rights-memorandum

36 Ibid.

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."[37] 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.

43. 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".[38] 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.

44. 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. 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

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

38 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

transparency in public sector use of ADM to empower individuals and encourage public scrutiny on the impacts of automated decisions.[39] However, the 'black box' nature of algorithms means that even when access is granted it is difficult to decipher how decisions have been made.[40] 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".[41]

45. 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.

46. 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.

39 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

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

41 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

Law enforcement and ADM

47. 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 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)).

48. We expect that police in England and Wales may rely on a very broad interpretation of ADM "authorised by law" based on common law and a patchwork of laws pre-dating the technological revolution, as South Wales Police and the Metropolitan Police Service[42] 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.

49. 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

42 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)

adverse effects can take place in secret with no safeguards and using special category data that may even pertain to protected characteristics, so long as a human review of the decision takes place at some time after the fact. There are no provisions for any course of action after such secret ADM decisions are made – not even if, for example, the human review finds that an automated decision was wrong. It is worth restating that ADM, according to the proposed definition, "produces an adverse legal effect" or "similarly significant adverse effect for the data subject".

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

> "Currently controllers processing for law enforcement purposes under Part 3 of the DPA rarely make use of automated processing. However, one of the reforms being made will make it more possible for the police and others to use this technology. Currently the requirement to inform an individual whenever automated decision-making takes places limits operational usefulness, as it could tip off people that they are subject to investigation. These reforms will enable the controller to review such a decision after it has been taken, instead of informing the individual at the time (...)".[43]

51. Despite the Information Commissioner's desire to maintain the ICO's status as a "trusted, fair and impartial regulator",[44] clauses 27 and 28 threaten to politicise the UK's data protection watchdog.

52. 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, this further jeopardises its role as an independent regulator.

43 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

44 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/

53. A further proposed addition to the DPA, section 120B, would also oblige the Commissioner to consider the importance of the "prevention, investigation, 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"[45] when respondents to the 'Data: a new direction' consultation raised the risks of politicising an impartial body.

54. 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.

55. 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).[46]

56. Overall, the new law enforcement ADM powers will lead to a vast expansion of purely automated decisions with significant adverse impacts on people where

45 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

46 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

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.

57. 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.

58. **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

59. 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)).

60. 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.

61. 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.

62. 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."[47]

63. 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

47 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))

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.

NATIONAL SECURITY

Clause 24 – National security exemption

Amendment:

Amendment 9: Clause 24, page 40, line 16, leave out subsection (7)

Effect of amendment:

This removes the expansive new powers provided in clause 24(7) that will increase exemptions from data protection law for law enforcement agencies under an exceptionally broad mandate of 'national security', with minimal oversight mechanisms. The DPA (2018) already provides a basis for national security exemptions, which does not need broadening.

Briefing:

64. Clause 24(7) changes and significantly expands the effect of 'national security certificates', currently provided for in s.79 of the Data Protection Act 2018. Under the proposed new system, a national security certificate would give law enforcement a general exemption from the most basic data protection obligations in the Data Protection Act 2018 including: the meaning of sensitive processing (including biometrics); limits on processing beyond a specific, explicit or legitimate purpose; limits on excessive, outdated and inaccurate processing; restrictions on storing data longer than necessary; data security; and a host of data rights that already have balanced, specific national security exemptions (e.g. right to access, rectify and erase personal data). The new restrictions greatly outstrip the existing derogations provided in the DPA and would include "most of the data protection principles, the rights of data subjects, certain obligations on competent authorities and

processors, and various enforcement provisions".[48] The government has provided no explanation as to why they feel it necessary to create a system that is so much more expansive than the current national security exemptions under the DPA – the only explanation given has been to maintain "consistency".[49] Where the DPA allows the possibility of national security exemptions or redactions on the basis of a balancing test, the new powers would give executive power to pre-emptively exempt compliance with data protection rights with no obligation to conduct a balancing test.

65. Currently, a national security certificate can be specific or general (DPA s.79(2)); under the proposed revisions, they would be amended to be solely general. Further, the Secretary of State's issuance of a national security certificate is considered "conclusive evidence" of a national security exemption.

66. This process is underpinned by a lack of oversight, lack of consideration of fundamental principles of necessity and proportionality (which are crucial in considerations of the Article 8 right to privacy), and the broadly indefinite nature of these certificates.[50] This means that law enforcement or intelligence agencies will be able to act above the law, without abiding by the most fundamental data protection principles.

67. Already, national security certificates lack necessity and proportionality tests, prior judicial oversight, or time-limits. These new national security certificates would drastically expand a serious power into an extreme one. **Clause 24 constitutes an unjustified and unexplained major expansion of law enforcement powers to harvest personal data above the law, including genetic and biometric data, health data, data on race, political opinions, trade union membership, religious and philosophical beliefs, and sexuality. It must be opposed.**

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

49 Data Protection And Digital Information (no. 2) Bill - Explanatory Notes, 8th March 2023: https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf 43

50 Big Brother Watch, Data Protection Bill Briefing for the House of Commons- Second Reading (February 2018) https://bigbrotherwatch.org.uk/wp-content/uploads/2018/03/Big-Brother-Watch-Briefing-on-the-Data-Protection-Bill-for-Second-Reading-in-the-House-of-Commons.pdf

THE ICO'S INDEPENDENCE

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

Amendments:

Amendment 10: MPs should give notice of their intention to oppose the question that clause 27 stand part.

Amendment 11: MPs should give notice of their intention to oppose the question that 28 stand part.

Effect of the amendments:

These amendments remove the Bill's new obligations on the ICO to consider innovation and competition when carrying out its functions, as well as the Secretary of State's authority to issue strategic directions. The amendments are therefore designed to protect the independence of the data protection regulator and protect the impartial application of the law.

Briefing:

68. Despite the Information Commissioner's desire to maintain the ICO's status as a "trusted, fair and impartial regulator",[51] clauses 27 and 28 threaten to politicise the UK's data protection watchdog.

69. 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, this further jeopardises its role as an independent regulator.

70. A further proposed addition to the DPA, section 120B, would also oblige the Commissioner to consider the importance of the "prevention, investigation, detection and prosecution of criminal offences" and "the need to safeguard public security and national security". This exacerbates the risks of function

51 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/

creep that are provoked by other sections of the DPDI2 Bill. The government has proceeded with this policy, despite recognising "concerns around independence"[52] when respondents to the 'Data: a new direction' consultation raised the risks of politicising an impartial body.

71. 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.

72. 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.[53]

52 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

53 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/

DIGITAL IDENTITY FRAMEWORK

Amendment:

Amendment 12: Clause 47, page 76, after subsection (2) insert -

(2A) The DVS trust framework must include a description of how the provision of digital verification services are expected to uphold the Identity Assurance Principles.

(2B) Schedule 13A of this Act describes each Identity Assurance Principle and its effect.

Effect of the amendment:

Clause 47(1)-(3) require the Secretary of State to prepare a DVS Trust Framework. This amendment makes sure the Framework includes reference to the Privacy and Consumer Advisory Group's (PCAG) Identity Assurance Principles, which focus on the role of an individual's control and consent in providing identifying information to an Identity Assurance Service. Schedule 13A (the Identity Assurance Principles) are included as an annex to this briefing. This would ensure that the new digital verification ecosystem accounts for well-established, important privacy-respecting principles.

Briefing:

73. Building on the existing framework set out in the UK digital identity and attributes trust framework – beta version,[54] the Bill establishes a regulatory framework for digital identity verification services in the UK and allows public authorities to disclose personal information to "trusted" digital verification services for the purpose of identity verification.[55]

74. It is crucial that digital verification services are designed and implemented around user needs, and reflect important privacy, equality and data protection principles. The Government's trust framework should therefore ensure that digital identity/verification services are built to respect the Identity Assurance Principles.

54 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

55 Data Protection and Digital Information Bill 2022: https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf

75. The 9 Identity Assurance Principles - developed by the Privacy and Consumer Advisory Group which "advises the government on how to provide people with a simple, trusted and secure means of accessing public services"[56] (of which the director of Big Brother Watch is a member) - synthesise and expand upon these concerns through a series of identity principles, offering a framework that seeks to engender trust in the given Identity Assurance Service by giving "real meaning to terms such as 'individual privacy' and 'individual control'".[57]

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

The right to use non-digital ID

Amendment:

Amendment 13: Page 85, line 7, insert new Clause

To move the following Clause -

"The right to use non-digital ID"

(1) Where an organisation utilises a digital verification service, the organisation must make a non-digital alternative method of verification available to the data subjects concerned.

(2) Information about digital and non-digital methods of verification described in (1) must be made available to data subjects prior to the verification process.

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

Effect of the amendment:

This amendment creates the right for data subjects to use non-digital identity verification services as an alternative to digital verification services, thereby preventing digital ID from becoming mandatory in certain settings.

Briefing:

77. Digital identity is not a practical or desired option for everyone, particularly vulnerable and marginalised groups. Individuals and communities need the availability of offline identity options: elderly people are often unfamiliar with new technologies and can face difficulties providing digital or biometric verification; people with lower income may not have access to the necessary technology; and others may wish to use traditional methods of identification out of personal choice or to preserve their privacy.

78. Digital identity systems must therefore always be optional for inclusion, accessibility, user empowerment and privacy. An important part of this is the ability to opt-out and be able to use offline methods of identification without undue disadvantage. Growth in digital identity systems and services should not mean that offline methods are blocked for people who cannot or do not want to use digital ones.

79. It is imperative that services are never contingent on a digital identity check, as this could prevent people from participating in key activities. There should always be an offline alternative for those who do not wish to share their information digitally, so that participation is not coercive and to uphold equal access opportunities. **In creating a digital identity regulatory system, the government should also safeguard individuals' rights to offline alternatives to digital verification processes.**

COOKIES

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

Amendment : MPs should give notice of their intention to oppose the question that clause 79 stand part.

Effect of this amendment: Removing clause 79 would prevent cookies from being stored without user consent in a wider set of circumstances, thereby protecting the principle of informed consent. It would also prevent the Secretary of State from exercising Henry VIII powers to amend how individuals consent to cookie processing online.

Briefing :

80. 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 website[58] and can "store a wealth of data, enough to potentially identify you without your consent".[59]

81. Given the amount of information they contain, cookies can qualify as personal data. They provide companies with information ripe for monetisation, which makes them a resource often exploited by advertising technology and surveillance advertising companies. This supports widespread online surveillance and behavioural profiling for business gain.[60] Open Rights Group has explained that such practices can result in predatory and exploitative targeting of vulnerable groups, such as gambling addicts.[61]

82. 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.[62] Permission to seek additional data is sought by platforms through consent pop-ups, commonly known as cookie banners. Cookie banners

58 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

59 Cookies, the GDPR, and the ePrivacy Directive: https://gdpr.eu/cookies/

60 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

61 Open Rights Group (n8).

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

are broadly criticised as flawed[63] and "irritating"[64], which is one of the key areas the DPDI2 Bill clumsily seeks to address. While acknowledging the problems with 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.

83. 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 an 'opt-in' model of consent to an 'opt-out' model in situations that are considered 'low-risk' to privacy.[65] 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.[66] 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.[67] It goes against the ICO's guidance that consent must be regularly reaffirmed and not "bundled up as a condition of service".[68] Processing increased volumes of personal data without the explicit provision 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.

84. 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 have not visited yet.

63 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
64 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
65 Data Protection and Digital Identity 2.0: Explanatory Notes (2023) https://publications.parliament.uk/pa/bills/cbill/58-03/0265/en/220265env2.pdf 75
66 DPDI2 Bill Explanatory Notes (n50) 76
67 See UK GDPR article 25: https://www.legislation.gov.uk/eur/2016/679/article/25
68 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

85. While the current cookie regime does require reform, this clause is neither an improvement or appropriate replacement. It allows organisations to collect the public's data with a much broader scope, thereby permitting excessive and intrusive surveillance and endangering individual privacy. Clause 79 must be removed in favour of a simplified approach that has individuals' privacy rights at its core. Big Brother Watch would welcome privacy-preserving measures that provide a minimally interruptive experience. Unfortunately, clause 79 satisfies neither of these requirements.[69]

CONCLUSION

86. The DPDI2 Bill fails to codify privacy as a right rather than a privilege, and threatens to purge many key rights put in place to protect the British public. It is not fit for purpose.

87. 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.

69 See, for example: https://noyb.eu/en/new-browser-signal-could-make-cookie-banners-obsolete

ANNEX

Schedule 13A: the Identity Assurance Principles[70]

Part 1: Definitions

1. These Principles are limited to the processing of Identity Assurance Data (IdA Data) in an Identity Assurance Service (e.g. establishing and verifying identity of a Service User; conducting a transaction that uses a user identity; maintaining audit requirements in relation a transaction associated with the use of a service that needs identity verification etc.). They do not cover, for example, any data used to deliver a service, or to measure its quality.

2. In the context of the application of the Identity Assurance Principles to an Identity Assurance Service, "Identity Assurance Data" ("IdA Data") means any recorded information that is connected with a "Service User" including:

- "Audit Data". This includes any recorded information that is connected with any log or audit associated with an Identity Assurance Service.

- "General Data". This means any other recorded information which is not personal data, audit data or relationship data, but is still connected with a "Service User".

- "Personal Data". This takes its meaning from the Data Protection Act 2018 or subsequent legislation (e.g. any recorded information that relates to a "Service User" who is also an identified or identifiable living individual).

- "Relationship Data". This means any recorded information that describes (or infers) a relationship between a "Service User", "Identity Provider" or "Service Provider" with another "Service User", "Identity Provider" or "Service Provider" and includes any cookie or program whose purpose is to supply a means through which relationship data are collected.

3. Other terms used in relation to the Principles are defined as follows:

- "Identity Assurance Service". This includes relevant applications of the technology (e.g. hardware, software, database, documentation) in the possession or control of any "Service User", "Identity Provider" or "Service

70 Note: the text of Schedule 13A is lifted from https://www.gov.uk/government/publications/govuk-verify-identity-assurance-principles/identity-assurance-principles). It is open to Parliament or the Secretary of State to revise the Trust Framework and the Principles – see from clause 47(5)

Provider" that is used to facilitate identity assurance activities; it also includes any IdA Data processed by that technology or by an Identity Provider or by a Service Provider in the context of the Service; and any IdA Data processed by the underlying infrastructure for the purpose of delivering the IdA service or associated billing, management, audit and fraud prevention.

- "Identity Provider". This means the certified individual or certified organisation that provides an Identity Assurance Service (e.g. establishing an identity, verification of identity); it includes any agent of a certified Identity Provider that processes IdA data in connection with that Identity Assurance Service.

- "Participant". This means any "Identity Provider", "Service Provider" or "Service User" in an Identity Assurance Service. A "Participant" includes any agent by definition.

- "Processing". In the context of IdA data means "collecting, using, disclosing, retaining, transmitting, copying, comparing, corroborating, correlating, aggregating, accessing" the data and includes any other operation performed on IdA data.

- "Provider". Includes both "Identity Provider" and/or "Service Provider".

- "Service Provider". This means the certified individual or certified organisation that provides a service that uses an Identity Provider in order to verify identity of the Service User; it includes any agent of the Service Provider that processes IdA data from an Identity Assurance Service.

- "Service User". This means the person (i.e. an organisation (incorporated or not) or an individual (dead or alive) who has established (or is establishing) an identity with an Identity Provider; it includes an agent (e.g. a solicitor, family member) who acts on behalf of a Service User with proper authority (e.g. a public guardian, or a Director of a company, or someone who possesses power of attorney). The person may be living or deceased (the identity may still need to be used once its owner is dead, for example by an executor).

- "Third Party". This means any person (i.e. any organisation or individual) who is not a "Participant" (e.g. the police or a Regulator). Note: we think it helpful to create a link to the language from the National Strategy for Trusted Identities in Cyberspace (NSTIC) which defines participants as "the collective subjects, identity providers, attribute providers, relying parties, and identity media taking part in a given transaction". This way, Third Parties are not Participants.

Part 2: The Nine Identity Assurance Principles

Any exemptions from these Principles must be specified via the "Exceptional Circumstances Principle. (See Principle 9).

1. User Control Principle

Statement of Principle: "I can exercise control over identity assurance activities affecting me and these can only take place if I consent or approve them."

1.1 An Identity Provider or Service Provider must ensure any collection, use or disclosure of IdA data in, or from, an Identity Assurance Service is approved by each particular Service User who is connected with the IdA data.

1.2 There should be no compulsion to use the Identity Assurance Service and Service Providers should offer alternative mechanisms to access their services. Failing to do so would undermine the consensual nature of the service.

2. Transparency Principle

Statement of Principle: "Identity assurance can only take place in ways I understand and when I am fully informed."

2.1 Each Identity Provider or Service Provider must be able to justify to Service Users why their IdA data are processed. Ensuring transparency of activity and effective oversight through auditing and other activities inspires public trust and confidence in how their details are used.

2.2 Each Service User must be offered a clear description about the processing of IdA data in advance of any processing. Identity Providers must be transparent with users about their particular models for service provision.

2.3 The information provided includes a clear explanation of why any specific information has to be provided by the Service User (e.g. in order that a particular level of identity assurance can be obtained) and identifies any obligation on the part of the Service User (e.g. in relation to the User's role in securing his/her own identity information).

2.4 The Service User will be able to identify which Service Provider they are using at any given time.

2.5 Any subsequent and significant change to the processing arrangements that have been previously described to a Service User requires the prior consent or approval of that Service User before it comes into effect.

2.6 All procedures, including those involved with security, should be should be made publicly available at the appropriate time, unless such transparency presents a security or privacy risk. For example, the standards of encryption can be identified without jeopardy to the encryption keys being used.

3. Multiplicity Principle

Statement of Principle: "I can use and choose as many different identifiers or identity providers as I want to."

3.1 A Service User is free to use any number of identifiers that each uniquely identifies the individual or business concerned.

3.2 A Service User can use any of his identities established with an Identity Provider with any Service Provider.

3.3 A Service User shall not be obliged to use any Identity Provider or Service Provider not chosen by that Service User; however, a Service Provider can require the Service User to provide a specific level of Identity Assurance, appropriate to the Service User's request to a Service Provider.

3.4 A Service User can choose any number of Identity Providers and where possible can choose between Service Providers in order to meet his or her diverse needs. Where a Service User chooses to register with more than one Identity Provider, Identity Providers and Service Providers must not link the Service User's different accounts or gain information about their use of other Providers.

3.5 A Service User can terminate, suspend or change Identity Provider and where possible can choose between Service Providers at any time

3.6 A Service Provider does not know the identity of the Identity Provider used by a Service User to verify an identity in relation to a specific service. The Service Provider knows that the Identity Provider can be trusted because the Identity Provider has been certified, as set out in GPG43 – Requirements for Secure Delivery of Online Public Services (RSDOPS).

4. Data Minimisation Principle

Statement of Principle: "My interactions only use the minimum data necessary to meet my needs."

1 Identity Assurance should only be used where a need has been established and only to the appropriate minimum level of assurance.

2 Identity Assurance data processed by an Identity Provider or a Service Provider to facilitate a request of a Service User must be the minimum necessary in order to fulfil that request in a secure and auditable manner.

3 When a Service User stops using a particular Identity Provider, their data should be deleted. Data should be retained only where required for specific targeted fraud, security or other criminal investigation purposes.

5. Data Quality Principle

Statement of Principle: "I choose when to update my records."

5.1 Service Providers should enable Service Users (or authorised persons, such as the holder of a Power of Attorney) to be able to update their own personal data, at a time at their choosing, free of charge and in a simple and easy manner.

5.2 Identity Providers and Service Providers must take account of the appropriate level of identity assurance required before allowing any updating of personal data.

6. Service User Access and Portability Principle

Statement of Principle: "I have to be provided with copies of all of my data on request; I can move/remove my data whenever I want."

6.1 Each Identity Provider or Service Provider must allow, promptly, on request and free of charge, each Service User access to any IdA data that relates to that Service User.

6.2 It shall be unlawful to make it a condition of doing anything in relation to a Service User to request or require that Service User to request IdA data.

6.3 The Service User must be able to require an Identity Provider to transfer his personal data, to a second Identity Provider in a standard electronic format, free of charge and without impediment or delay.

7. Certification Principle

Statement of Principle: "I can have confidence in the Identity Assurance Service because all the participants have to be certified against common governance requirements."

7.1 As a baseline control, all Identity Providers and Service Providers will be certified against a shared standard. This is one important way of building trust and confidence in the service.

7.2 As part of the certification process, Identity Providers and Service Providers are obliged to co-operate with the independent Third Party and accept their impartial determination and to ensure that contractual arrangements:

- reinforce the application of the Identity Assurance Principles

- contain a reference to the independent Third Party as a mechanism for dispute resolution

7.3 There will be a certification procedure subject to an effective independent audit regime that ensures all relevant, recognised identity assurance and technical standards, data protection or other legal requirements, are maintained by Identity Providers and Service Providers.

7.4 In the context of personal data, certification procedures include the use of Privacy Impact Assessments, Security Risk Assessments, Privacy by Design concepts and, in the context of information security, a commitment to using appropriate technical measures (e.g. encryption) and ever improving security management. Wherever possible, such certification processes and security

procedures reliant on technical devices should be made publicly available at the appropriate time.

7.5 All Identity Providers and Service Providers will take all reasonable steps to ensure that a Third Party cannot capture IdA data that confirms (or infers) the existence of relationship between any Participant. No relationships between parties or records should be established without the consent of the Service User.

7.6 Certification can be revoked if there is significant non-compliance with any Identity Assurance Principle.

8. Dispute Resolution Principle

Statement of Principle: "If I have a dispute, I can go to an independent Third Party for a resolution."

8.1 A Service User who, after a reasonable time, cannot, or is unable, to resolve a complaint or problem directly with an Identity Provider or Service Provider can call upon an independent Third Party to seek resolution of the issue. This could happen for example where there is a disagreement between the Service User and the Identity Provider about the accuracy of data.

8.2 The independent Third Party can resolve the same or similar complaints affecting a group of Service Users.

8.3 The independent Third Party can co-operate with other regulators in order to resolve problems and can raise relevant issues of importance concerning the Identity Assurance Service.

8.4 An adjudication/recommendation of the independent Third Party should be published. The independent Third Party must operate transparently, but detailed case histories should only be published subject to appropriate review and consent.

8.5 There can be more than one independent Third Party.

8.6 The independent Third Party can recommend changes to standards or certification procedures or that an Identity Provider or Service Provider should lose their certification.

9. Exceptional Circumstances Principle

Statement of Principle: "Any exception has to be approved by Parliament and is subject to independent scrutiny."

9.1 Any exemption from the application of any of the above Principles to IdA data shall only be lawful if it is linked to a statutory framework that legitimises all Identity Assurance Services, or an Identity Assurance Service in the context of a specific service. In the absence of such a legal framework then alternative measures must be taken to ensure, transparency, scrutiny and accountability for any exceptions.

9.2 Any exemption from the application of any of the above Principles that relates to the processing of personal data must also be necessary and justifiable in terms of one of the criteria in Article 8(2) of the European Convention of Human Rights: namely in the interests of national security; public safety or the economic well-being of the country; for the prevention of disorder or crime; for the protection of health or morals, or for the protection of the rights and freedoms of others.

9.3 Any subsequent processing of personal data by any Third Party who has obtained such data in exceptional circumstances (as identified by Article 8(2) above) must be the minimum necessary to achieve that (or another) exceptional circumstance.

9.4 Any exceptional circumstance involving the processing of personal data must be subject to a Privacy Impact Assessment by all relevant "data controllers" (where "data controller" takes its meaning from the Data Protection Act).

9.5 Any exemption from the application of any of the above Principles in relation to IdA data shall remain subject to the Dispute Resolution Principle.