WRITTEN EVIDENCE FROM FREEDOM FROM BIG BROTHER WATCH (IPA0008)

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.

INTRODUCTION

Big Brother Watch welcomes the opportunity to brief the Joint Committee on Human Rights on the Investigatory Powers (Amendment) Bill.

Big Brother Watch supports the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. However, the Snowden revelations and subsequent litigation by Big Brother Watch (*Big Brother Watch & Ors v UK),* Liberty, Open Rights Group, Privacy International and others to protect Article 8 and 10 of the European Convention on Human Rights (ECHR) have repeatedly identified unlawful state surveillance by UK agencies.

Whilst we welcomed the intent to regulate the rapidly growing surveillance state via a democratic process, the highly controversial Investigatory Powers Act 2016 (IPA) put mass, suspicionless electronic surveillance powers of a scale never seen before in a democracy onto a statutory footing, including hacking, absent a clear evidence basis to support the strict necessity of such extreme powers, and missed an opportunity for independent judicial

authorisation in favour of a weak 'double lock'. The Act has already been amended following the *Big Brother Watch & Ors* judgment from the Grand Chamber in the European Court of Human Rights.

We are concerned that authorities are seeking to yet further extend already extreme powers less than a decade after they passed, and on a timetable that so far permits only minimal scrutiny from parliamentarians. Our primary concerns with the Investigatory Powers (Amendment) Bill are that it will:

- weaken safeguards for intelligence services to collect **bulk datasets of personal information**, potentially harvesting millions of facial images and mass social media data

- expressly permit the harvesting and processing of **internet connection records** for generalised, mass surveillance

- force technology companies, including overseas, to inform the government of plans to improve security or privacy measures so that the government can consider serving a notice to prevent such changes – effectively **transforming private companies into arms of the surveillance state**

As such, in our written evidence we will respond to questions 1, 5, and 6 from the Committee's call for evidence.

QUESTION 1: BULK PERSONAL DATASETS

Question 1: Does the proposed Part 7A warrant regime for bulk personal data where there is "low or no reasonable expectation of privacy" comply with human rights obligations, particularly Article 8 ECHR?

1. In Big Brother Watch's view, the proposed regime for so-called "low privacy" bulk personal datasets is highly unlikely to comply with the UK's human rights obligations under Article 8 ECHR. We recommend that clauses 1 and 2 are removed from the Bill.

2. Part 7 of the IPA permits the intelligence services to harvest 'bulk personal datasets', defined as 'a set of information that includes personal data relating to a number of individuals' whereby 'the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service in the exercise of its functions' (IPA, s.199). As such, bulk personal datasets (BPDs) represent one of the most controversial capabilities, expressly intended for generalised mass surveillance intruding on the private lives of a majority of innocent people.

3. Clause 2 of the Investigatory Powers (Amendment) Bill introduces a new Part 7A to the IPA, to create a dual authorisation process for a new vague type of BPD where there is deemed to be 'low or no reasonable expectation of privacy'. Where such a type of 'low privacy' BPD applies, an agency need not seek the approval of a judicial commissioner to retain the dataset *if* the agency has already authorised a 'category of bulk personal datasets' (proposed new clause 226BA) that the BPD would come under, and sought the judicial commissioner's approval for such a category.

4. There is no definition for the 'low privacy' BPD category, but its application should be determined by having 'regard' to 'circumstances' including 'in particular' factors such as the 'nature of the data', whether the data 'has been made public by the individuals' or they have 'consented to the data being made public', the 'extent to which the data is widely known about', and if it is published or has 'already been used in the public domain', as set out in Clause 2(3). As Lord Coaker rightly stated at Second Reading, "I believe there will need to be a careful debate about what such a threshold means. What does "low" mean?"[1] We are concerned that such databases could involve mass voice, image, social media posts or other data from social media posts over time.

5. The Bill's creation of a vague and nebulous category of information where there is deemed to be 'low or no reasonable expectation of privacy' is a concerning departure from existing privacy law – in particular, A8 and data protection law. Such an undefined category requires agencies who are motivated to process such data to adjust safeguards according to unqualified assertions of other people's expectations of privacy over their data. On the contrary, privacy law requires objective safeguards and

[1]HL Deb, 20th November 2023, vol. 834, col. 626

is constructed according to the sensitivity of the information rather than guesswork as to an individual's 'expectations' of privacy concerning personal information.

6. The proposal of such a poorly defined 'low privacy' category of BPDs could lead to some of the most intrusive BPDs, and yet with the lowest safeguards. For example, it could be argued that databases of mass facial images – such as Clearview AI's database of 30 billion facial images harvested from social media platforms for highly intrusive facial recognition searches – could be considered a 'low privacy' database since the photos have 'been made public by the individuals'. On the contrary, the Information Commissioner's Office found Clearview AI in breach of the Data Protection Act 2018 (DPA) and attempted to fine the company £7.5m.[2] Similarly, a database of all public Facebook or other social media posts could be argued to be a 'low privacy' database, despite the fact it would be a comprehensive database of billions of people's social networks, sexual orientations, political opinions, religion, health status, and so on. Under the DPA, much of this data qualifies as 'sensitive personal data' incurring extra protections when it comes to retention and processing, regardless of whether the information can be considered to be made public. Such datasets also clearly engage A8 – yet commensurate safeguards are absent.

7. Naturally, A8 and the DPA would still apply to the intelligence agencies' processing of 'low privacy' BPDs – but as currently drafted, contradictory standards would apply. Schedule 10 of the DPA sets out the circumstances in which the agencies can conduct sensitive processing (i.e. processing defined in s.86(7) DPA of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; data concerning health or sexual orientation; biometric or genetic data that uniquely identifies an individual; and data regarding an alleged offence by an individual).[3] With regards to 'low privacy' BPD, the relevant circumstance in Sch. 10 DPA is that the 'information contained in the personal data has been made public as a result of steps deliberately taken by the data subject'.[4] That is a different standard to the nebulous threshold in the new BPD category whereby information is considered 'low privacy' according to the 'extent to which the data is

[2]https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

[3]https://www.legislation.gov.uk/ukpga/2018/12/section/86

[4]https://www.legislation.gov.uk/ukpga/2018/12/schedule/10

widely known about', and if it is has 'already been used in the public domain', as set out in Clause 2(3).

8. For example, whereas facial images from public CCTV may be considered as a 'low privacy' BPD under the Investigatory Powers (Amendment) Bill, they would be considered personal data and possibly subject to sensitive processing, under the Data Protection Act 2018. Masses of such data also clearly engages A8 as does subsequent processing which, with modern technologies, can be incredibly intrusive.

9. Another example highlighting the potential divergence is hacked and leaked data that, whilst not made 'deliberately' public as per the DPA requirement, is arguably public and available in the public domain. Would, for example, the genetic data of 1 million Jewish people recently hacked from a commercial DNA company,[5] be considered a 'low privacy' database under this definition?

10. In the Second Reading debate, addressing this aspect of the Bill, Lord Sharpe said:

> "I have noted the recommendation of Big Brother Watch and I read it in some detail. I think it is based on a misunderstanding (…) the datasets would not necessarily be authorised under the new regime in Part 7A solely by virtue of their being publicly or commercially available, and that is particularly important when considering datasets which have been hacked and/or leaked."[6]

However, we have not suggested that datasets would be authorised solely by virtue of being publicly or commercially available – but rather that a vague set of broad and enabling "factors" to which merely "regard must be had", the possibilities are untenably vast. The new Part 7A certainly does not contain any clear prohibition on leaked commercial datasets or billions of facial images scraped from the internet from being considered 'low privacy' datasets.

11. At a time when our data footprints and data traces are arguably 'made public' by individuals simply living modern, everyday lives, and such data can be transformed into powerful, harmful, intrusive surveillance through processing and new

[5]https://www.wired.com/story/23andme-credential-stuffing-data-stolen/
[6]HL Deb, 20th November 2023, vol. 834, col. 650-1

technologies, the 'low privacy' BPD category is frankly illogical, discordant with preceding privacy and data laws, and wholly inappropriate for the digital age.

12. In Big Brother Watch's view, Part 7 powers to retain bulk personal datasets fail to adequately provide the thresholds of genuine necessity and proportionality in accordance with Article 8 of the European Convention on Human Rights. This is a view that has been shared by Liberty, which assessed the Government's case for bulk powers in 2016 during the passage of the (then) Investigatory Powers Bill[7], and David Anderson's 'Report of the Bulk Powers Review' of the same period.[8] Indeed, the collation, retention and processing of records of potentially the entire population is the essence of a surveillance society.

13. BPD appear to be widely used – 177 warrants were sought and approved in 2021[9]. As long as such powers do exist, safeguards and clarity in accordance with existing law are vital. However, if this Bill passes without amendments, in future we will not even know the number of annual BPD warrants as it will create a route by which 'low privacy' BPDs can be sought and approved by the agencies themselves, without judicial authorisation.

14. The risks are not only to the health of our democratic society and the rights and freedoms of the public within it, but to individuals who are at risk of personal intrusion. In its most recent report, covering a period of 2021 which is at least five years after the passing of the Investigatory Powers Act, the Investigatory Powers Commissioner's Office (IPCO) found that the Secret Intelligence Service (SIS, aka MI6) had retained bulk personal datasets 'in error and without a warrant' and had 'serious gaps in [its] capability for monitoring and auditing of systems used to query and analyse BPDs'[10] involving 'several areas of serious concern'.[11] It also found that the agencies were responsible for 29 errors involving BPD – the second highest area of investigatory powers for errors. Errors can include, for example, officers accessing

[7]https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-submission-to-the-Terrorism-Reviewers-Review-of-Bulk-Powers.pdf, pp.14-15
[8]https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-Response-to-the-Report-of-the-Bulk-Powers-Review.pdf, p.16
[9]https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf, p.112
[10]https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf, p.47
[11]Ibid. p.49

an individual's records without reason. Such datasets risk breaching our collective privacy rights and also individual's privacy rights.

15. Therefore, the proposed powers to harvest 'low privacy' bulk personal datasets under a lighter-touch regulatory regime should be removed from the Bill to ensure that bulk data harvesting is subject to the existing safeguards and regulatory regime.

QUESTION 5: SECRET NOTICES FOR TECH COMPANIES

Question 5: Does the introduction of a notification requirement requiring operators to inform the Secretary of State if they propose to make changes to their products or services that would negatively impact existing lawful access capabilities raise any human rights concerns?

16. On Big Brother Watch's analysis, the radical change to the IPA proposed by Part 4 of the Bill on notices, whereby companies would be obliged to inform the Home Office in advance about any security or privacy improvements or changes they are considering making to their platforms, raises significant human rights concerns, principally in relation to A8 and A10. We recommend that Clauses 17 to 20 are removed from the Bill.

17. These changes are widely understood[12] to be aimed at making companies forewarn the government of any plans to increase privacy and security measures such as encryption, so that the government can intervene and issue notices that would circumvent or block such changes to ensure mass state monitoring capabilities. Encryption is widely understood to be a technology that is vital in technologically protecting individuals' right to privacy.

18. Clause 20 would introduce s.258A to the IPA, whereby any telecommunications or postal operator that provides or has provided assistance in relation to *any* warrant, authorisation or notice under the IPA may be issued with a notice by the Secretary of State, 'requiring the operator to notify the Secretary of State of any proposals of the

[12]For example, *Tech groups fear new powers will allow UK to block encryption* – Anna Gross and Cristina Criddle, Financial Times, 7 November 2023: https://www.ft.com/content/b9f92f62-9895-4ff4-9e4a-659d217dc9af

operator to make any relevant changes specified in the notice' (s.258A(1)). A 'relevant change' is defined in a circular manner, i.e. it is any change to the operator's service or system specified by the Secretary of State (s.258A(2)-(3)) though it is clear that the intention is for companies to notify the Secretary of State if they improve privacy and security measures in such a way that could affect a company's capability to assist with *any* surveillance warrant, authorisation or notice that could be issued under the Act (s.258A(4)). Given the very broad powers in the Act, such a notice could be used to force companies to proactively report many of their product improvement plans to the Government.

19. An operator who receives such a notice must not disclose possession of this secret notice to anyone, at all, without permission (s.258(8)); and they must comply with the notice 'a reasonable time' before making the changes (s. 258A(9)).

20. Clause 16 further claims extra-territorial application of data retention notices, as is the case for technical capability notices.

21. Clause 17 would create several amendments to further require that operators do not make any relevant changes to their services or systems if they have been issued with a data retention, national security or technical capability notice, even if that notice is under review and has not yet been fully imposed. This could mean that a company is prevented from attending to security issues, and could even incur liabilities on those companies, on account of having to comply with a surveillance state - despite no actual notice being in force and, therefore, no solid case of necessity or proportionality justifying the privacy infringement. We find this concerning from a rule of law perspective.

22. Taken together, these proposed changes effectively attempt to make technology companies around the world proactive arms of the British surveillance state. In addition to compelling the companies to generate and retain data, and potentially even technologically adapt their systems to provide greater surveillance capabilities (under secret 'technical capability notices'), this new Clause would seek to further compel companies to proactively consult the British government on their privacy and security measures with a view to ensuring state surveillance capabilities. This is concerning not only from the perspective of the UK upholding its obligations under the ECHR,

but in terms of the consequential impact such powers will have on other states' approaches to controls on technology providers, particularly less democratic states.

23. The proposal is a chilling reflection of the Government's attitude towards the protected rights to privacy and freedom of expression. Telecommunications operators exist to allow individuals to communicate freely – not to perform state surveillance. By analogue example, this extraordinary requirement is akin to demanding locksmiths and construction companies inform the government of the strength or their doors, windows and walls so that the government can either break in or build trapdoors for secret access, 'just in case'. It would be akin to forcing Alexander Graham Bell to consult with the government before inventing the telephone, to ensure the government could tap phone calls before anyone were allowed to make one.

24. Big Brother Watch is not aware of any country in the world that imposes such onerous and disproportionate obligations on private companies. The proposal has been met with widespread condemnation from technology companies and human rights groups.[13]

25. Part 4 of the Bill, particularly clauses 17 and 20, should be removed from the Bill to prevent requiring technology companies around the globe to effectively seek the British government's permission before introducing security and privacy measures to their services.

QUESTION 6: INTERNET CONNECTION RECORDS

[13]For example, *Tech groups fear new powers will allow UK to block encryption* – Anna Gross and Cristina Criddle, Financial Times, 7 November 2023: https://www.ft.com/content/b9f92f62-9895-4ff4-9e4a-659d217dc9af; see also responses to the summer 2023 consultation

Question 6: Are the provisions expanding access to Internet Connection Records compatible with Article 8 ECHR? Do the provisions contain sufficient safeguards to ensure compatibility?

26. We are concerned that the proposal to expand access to Internet Connection Records, which is designed for generalised surveillance and 'target discovery', is at risk of non-compliance with the UK's obligations to protect and promote A8 rights to privacy. We believe Clause 14 should be removed from the Bill.

27. Internet Connection Records (ICRs) were a new category of surveillance data, introduced in the IPA, that the Home Secretary can require telecommunications operators to generate and retain for a multitude of public authorities to access. ICRs are essentially 'web logs' that "contain rich data about access to internet services" and "can reveal appreciably more about [individuals] than their telephony records".[14] No other European or indeed Five Eyes country has surveillance laws that allow for the compulsory generation and retention of ICRs or "web logs".[15]

28. Currently, ICRs can be obtained under the IPA (s.62) where the time and use of a service is known or the person's identity is known. Clause 14 of the Bill would amend s.62 IPA to add a further purpose for which ICRs can be used – for 'target discovery'. That is, generalised surveillance.

29. In 2015-6, the Government made the operational case for ICRs on the basis that it was a specific data retention power filling a specific gap in capabilities, for the sole purposes of "identifying suspects, victims and activity relevant to the [specific] investigation".[16] However, the explanatory notes accompanying the present Bill are explicit that the "intention of this [*expansion of the ICR power*] is to improve target detection, enhancing the usefulness of the power" and "to assist in detecting new subjects of interest."[17] The "usefulness" of a power is insufficient to assess whether

[14]Independent Review of the Investigatory Powers Act 2016, Lord Anderson KBE KC, 30th June 2023, p.44: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2

[15]Ibid, p.45

[16]Operational Case for the Retention of Internet Connection Records – Home Office, 1st March 2016, p.9: https://assets.publishing.service.gov.uk/media/5a751224e5274a3cb28696be/Operational_Case_for_the_Retention_of_Internet_Connection_Records_-_IP_Bill_introduction.pdf

[17]p.13

the power is strictly necessary and proportionate, and as such a lawful engagement with individuals' A8 right to privacy.

30. The attempt to expand this power is a classic case of mission creep. If parliamentarians are asked every few years to "enhance the usefulness" of extraordinary surveillance powers that parliament permitted for specific and restricted purposes – and that are already out of step with much of the democratic world – then the UK's surveillance framework will grow further out of control.

31. Target discovery is the discovery of new targets and subjects of interest who may warrant further investigation. It is a reversal of the long-held, important principle in Britain whereby suspicion precedes surveillance and, without the strongest safeguards, often involves speculative and suspicionless surveillance to determine 'suspicious' behaviour and generate subjects of interest. It has long been Big Brother Watch's view, shared by many experts, that targeted surveillance orientated to sites of suspicion and contact chaining are suitable, proportionate alternative methods for target discovery rather than generalised, mass, suspicionless surveillance which is not only disproportionate but ineffective and prone to mistakes.[18]

32. Speaking about this proposed power at Committee Stage, Lord West of the Intelligence and Security Committee (ISC) said it was the ISC's view that it is "significantly more intrusive than existing provisions".[19] He expanded:

> "Target discovery is a great deal more intrusive than target development, potentially intruding on the privacy of a great number of innocent individuals. This is why we must tread very cautiously in this area and be quite satisfied of the need for the power, and that it is tightly drawn and properly overseen (…) Parliament deliberately imposed a high bar for authorising obtaining internet connection records given their potential intrusiveness."[20]

33. Clause 14 would add the condition 'D1' to the existing conditions for using ICRs. Unlike the other conditions, the applicant need not know the person or use of a service

[18]Bulk Collection of Signals Intelligence: Technical Options – Committee on Responding to Section 5(d) of Presidential Policy Directive 28, 2015 (The National Academies Press), p.43
[19]HL Deb 11th December 2023, vol. 834, col. 1753
[20]HL Deb 11th December 2023, vol. 834, col. 1754

in question but rather can seek ‘to identify which persons or apparatuses are using one or more specified internet services in a specified period’.

34. The explanatory notes acknowledge the risks of such open-ended powers:

> “it is recognised that such queries are highly susceptible to imprecise construction. As a result, additional safeguards are proposed in this Bill with the intention of managing access to this new Condition and mitigating public concerns.”[21]

The safeguards are essentially that the new Condition is limited to national security and serious crime, as follows. However, a legitimate purpose does not justify engagements of privacy rights that are unnecessary or disproportionate.

35. Clause 14 should be removed to protect A8 rights and prevent the expansion of internet connection records powers and their use for suspicionless, generalised surveillance.

(22 January 2024)

[21] p.25, para. 116