BIG BROTHER WATCH

Big Brother Watch's Briefing on the Investigatory Powers (Amendment) Bill for the House of Commons, Committee Stage

March 2024

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

CONTENTS

Introduction

Big Brother Watch welcomes the opportunity to brief Members of Parliament on the Investigatory Powers (Amendment) Bill ahead of Committee Stage in the House of Commons on Thursday 7th March and Tuesday 12th March 2024.

However, we are deeply concerned by the highly restricted time allocated for the Bill to be scrutinised by the Committee. The powers in the Bill relate to the privacy and security of the entire population of Britain and beyond – they deserve the closest examination. We are concerned that, much like some of the powers in the Bill, the Government is undermining normal scrutiny processes.

Big Brother Watch supports the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. However, intrusive investigatory powers must be strictly necessary and proportionate, and have appropriate safeguards and oversight mechanisms, in order to protect rather than harm democracy.

As the Chair of the Intelligence and Security Committee, Julian Lewis MP, said during Second Reading of the Bill:

> **"(...) there are several areas in which the Committee considers that the Bill goes too far. In particular, it does not yet provide the safeguards and oversight that are so essential when it comes to secretive actions that have the potential to intrude on a great many people."**[1]

Sir John Hayes MP, who was the Security Minister responsible for leading the Investigatory Powers Act when it passed through parliament in 2015-6, stated the following about the Investigatory Powers (Amendment) Bill during its Second Reading:

> **"When we consider this Bill, we should test whether its provisions are indeed urgent, targeted and necessary. I am not absolutely convinced that all we see before us passes that test".**[2]

In this briefing we focus on a number of areas in which we believe the proposed powers do not meet the essential tests, and propose amendments accordingly.

1 HC Deb, 19 February 2024, vol. 745, col. 543: https://hansard.parliament.uk/commons/2024-02-19/debates/A82D4C76-9E49-449A-9DA2-8679E216B0F5/InvestigatoryPowers(Amendment)Bill(Lords)

2 HC Deb, 19 February 2024, vol. 745, col. 537:

Our five primary concerns with the Investigatory Powers (Amendment) Bill are that it will:

- weaken safeguards to harvest **bulk datasets of personal information**, potentially collecting millions of facial images and mass social media data
- weaken safeguards for authorities to harvest **communications data**
- harvest **internet connection records** for generalised, mass surveillance
- fail to offer post-notification where **parliamentarians are targeted for surveillance**
- force technology companies, including overseas, to inform the government of plans to adjust security or privacy measures on their platforms so that the government can consider preventing such changes – effectively **transforming private companies into arms of the surveillance state**

Recommendations:

RECOMMENDATION 1: So-called 'low privacy' BPDs should be scrapped; we recommend that Members of the Committee give notice of their intention to oppose the question that Clauses 1 and 2 stand part of the Bill.

RECOMMENDATION 2: The proposed amendment to assert that there is a lawful authority to obtain communications data from operators simply on account of data being publicly or semi-publicly available is wrong. Paragraph (3A)(e) proposed in Clause 12 should be removed from the Bill.

RECOMMENDATION 3: Big Brother Watch recommends that Members reject the expansion of internet connection records powers and oppose Clause 15.

RECOMMENDATION 4: The Bill should be amended to require that the Investigatory Powers Commissioner is informed of, and records in his annual report, the number of warrants authorised each year to permit surveillance of members of relevant domestic legislatures. This would ensure transparency over the rate at which the power is used.

RECOMMENDATION 5: Clauses 22 and 23 should be amended to introduce post-surveillance notification for parliamentarians.

RECOMMENDATION 6: Clauses 18 and 21 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.

Bulk Personal Datasets

Amendment:

We recommend that Members give notice of their intention to oppose the Question that Clause 1 stand part of the Bill.

We recommend that Members give notice of their intention to oppose the Question that Clause 2 stand part of the Bill.

Effect:

Removing clauses 1 and 2 would remove the problematic 'low privacy' bulk personal dataset harvesting power from the Bill. Clause 2 contains the new power; Clause 1 contains the consequential amendments required by Clause 2.

Briefing:

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). We are concerned that such databases could involve mass voice, image, social media posts and much more data 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, 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, data protection law 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 c**ould 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.[3] 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.

7. As Joanna Cherry KC MP said during Second Reading of the Bill, clause 2:

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

"seem(s) to be based on a legal misunderstanding that people lose their right to privacy when they happen to share certain information with someone else (...) that runs contrary to the jurisprudence of the European Court of Human Rights".[4]

8. 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).[5] 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'.[6] 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 widely known about', and if it is has 'already been used in the public domain', as set out in Clause 2(3).

9. 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.

10. 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,[7] be considered a 'low privacy' database under this definition?

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

4 HC Deb, 19 February 2024, vol. 745, col. 533: https://hansard.parliament.uk/commons/2024-02-19/debates/A82D4C76-9E49-449A-9DA2-8679E216B0F5/InvestigatoryPowers(Amendment)Bill(Lords)
5 https://www.legislation.gov.uk/ukpga/2018/12/section/86
6 https://www.legislation.gov.uk/ukpga/2018/12/schedule/10
7 https://www.wired.com/story/23andme-credential-stuffing-data-stolen/

processing and new 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[8], and David Anderson's 'Report of the Bulk Powers Review' of the same period.[9] 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[10]. As long as such powers do exist, safeguards and clarity in accordance with the 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 self-approved without specific judicial authorisation. **As Intelligence and Security Committee member Kevan Jones MP said during Second Reading of the Bill:**

> **"(...) here is potential for mission creep without any oversight of what is being authorised. (...) What we are really being asked to do is rely on the good faith of the intelligence services to use the powers in a certain way. I do not think that is strong enough, and no legislation should be solely dependent on good will."**[11]

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

8 https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-submission-to-the-Terrorism-Reviewers-Review-of-Bulk-Powers.pdf, pp.14-15
9 https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-Response-to-the-Report-of-the-Bulk-Powers-Review.pdf, p.16
10 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf, p.112
11 HC Deb, 19 February 2024, vol. 745, col. 547: https://hansard.parliament.uk/commons/2024-02-19/debates/A82D4C76-9E49-449A-9DA2-8679E216B0F5/InvestigatoryPowers(Amendment)Bill(Lords)

[its] capability for monitoring and auditing of systems used to query and analyse BPDs'[12] involving 'several areas of serious concern'.[13] 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 an individual's records without reason.

15. We are concerned that, during the debated in the House of Lords, the government was unable to explain how the concerning examples of unlawful bulk data processing given, such as Clearview's billions of stolen facial images or mass social media data, would not be permitted under "low/no privacy" BPDs. As such, we believe such cases would be possible under the proposed Bill.

16. **RECOMMENDATION 1: So-called 'low privacy' BPDs should be scrapped; we recommend that Members of the Committee give notice of their intention to oppose the question that Clauses 1 and 2 stand part of the Bill.**

12 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf, p.47
13 Ibid. p.49

Communications Data

'Public' communications data

Amendment: Clause 12, page 33, line 16, leave out paragraph (e)

Effect: This amendment would prevent public authorities - spanning councils, police forces, intelligence agencies, government departments including the DWP, HMRC, the Gambling Commission, the Food Standards Agency, and many more - from having 'lawful authority' to obtain and surveil communications data from a telecommunications or postal operator because the information is available to the public or a section of the public (even if only on a commercial basis).

Briefing:

17. Big Brother Watch supports the important role of communications data in supporting missing persons investigations, and preventing and investigating serious crime. It must also be noted that communications data monitoring can be invasive and paint detailed pictures of people's lives and social networks. Communications data is defined in the IPA as data which may be used to identify or assist in identifying the sender, recipient, time, duration, type, method, pattern, or fact of a communication, along with system used to make a communication, its location and the IP address or other identifier of any apparatus used.

18. Clause 12 of the Investigatory Powers (Amendment) Bill amends the s.11 IPA offence of unlawfully obtaining communications data from a telecommunications or postal operator. Whereas the IPA currently defines the offence as 'a relevant person who, without lawful authority, knowingly or recklessly obtains communications data from a telecommunications operator', the Bill would add a list of examples to the Act of what *does* constitute 'lawful authority'.

19. We are concerned about one such example, which is (3A)(e): 'where the communications data has been published before the relevant person obtained it', whereby 'publish' means (3B) 'make available to the public or a section of the public (whether or not on a commercial basis)'.

20. **It is not the case in law that data that is available to the public or a section of the public is, as a result, information that can be subject to surveillance absent a lawful authority.** The public or semi-public nature of the

information does not provide a lawful authority for intrusive surveillance in and of itself. Accordingly, it is well-accepted that a legal basis is required for various types of 'public' surveillance, from social media monitoring to CCTV monitoring.

21. In the case of communications data monitoring, the intrusion can be particularly significant. As the Court of Justice of the European Union (CJEU) stated in the *Digital Rights Ireland* case, "those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."[14]

22. We are concerned that, for example, if an environmental campaigns group were to hold a Zoom call, police may believe they have a lawful authority to obtain the communications data from Zoom solely on account of the data being 'available to a section of the public'. Likewise, membership of and posts on a racial equality group on Facebook is data 'available to a section of the public' and therefore authorities may – wrongly – believe they consequently possess lawful authority to obtain associated communications data from the platform.

23. **RECOMMENDATION 2: The proposed amendment to assert that there is a lawful authority to obtain communications data from operators simply on account of data being publicly or semi-publicly available is wrong. Paragraph (3A)(e) proposed in Clause 12 should be removed from the Bill.**

14 *Digital Rights Ireland* (C-293/12) and *Seitlinger and Others* (C-594/12).

Internet Connection Records

Amendment: We recommend that Members give notice of their intention to oppose the Question that Clause 15 stand part of the Bill.

Effect: This amendment would prevent the purpose expansion of Internet Connection Records whereby they could be obtained for generalised surveillance and target discovery.

Briefing:

24. 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".[15] **No other European or indeed Five Eyes country has surveillance laws that allow for the compulsory generation and retention of ICRs or "web logs"**.[16]

25. Currently, ICRs can be obtained under the IPA (s.62) where the time and use or a service is known or the person's identity is known. Clause 15 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.**

26. Big Brother Watch reminds parliamentarians that 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".[17]

27. 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."[18] The "usefulness" of a power is insufficient to assess whether the power is strictly necessary and

15 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
16 Ibid, p.45
17 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
18 p.13

proportionate, and as such a lawful invasion of individuals' A8 right to privacy. We are concerned that the attempt to expand this power may be a classic case of mission creep. If parliamentarians are asked every few years to "enhance the usefulness" of extraordinary surveillance powers that are already out of step with much of the democratic world, then the surveillance framework could easily grow out of control.

28. Speaking about this proposed power at Committee Stage [HL], 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. (...) Parliament deliberately imposed a high bar for authorising obtaining internet connection records given their potential intrusiveness."[20]

29. 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 effective, proportionate alternative methods for target discovery rather than generalised, mass, suspicionless surveillance which is disproportionate, ineffective and prone to mistakes.[21]

30. The proposed extension of the ICR power is practically unlimited. **As Intelligence and Security Committee (ISC) member Sir Jeremy Wright MP noted during Second Reading, it is "a significant and material increase in intrusion for the population at large" –** he further said**:**

> **"(...) there is no apparent limit on the number of internet services that can be specified or on the length of the specified period,** so the clause could allow an intelligence agency to collect ICR data on a

19 HL Deb 11th December 2023, vol. 834, col. 1753
20 HL Deb 11th December 2023, vol. 834, col. 1754
21 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

large number of different internet services, and over a long period. **That would inevitably involve data on the activities of a potentially large number of people,** whereas the current law permits only examination of a specific service at a specific time, which carries much less risk of other wholly innocent and uninvolved individuals being caught in the net **(...) this is a significant widening of their powers (...)**

"Many of our constituents would be concerned about their internet activity being scrutinised, even if no action were taken thereafter—and we should bear in mind that the Bill's language does not limit that scrutiny to sites visited which are inherently suspicious. Even everyday online activity may be of interest in the case of individuals of concern, but **this provision would mean that the everyday online activity of many who are not of concern will also be examined.**[22]

31. Clause 15 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 in question but rather can seek 'to identify which persons or apparatuses are using one or more specified internet services in a specified period'.

32. 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."[23]

The explanatory notes also acknowledge the complexity of utilising such broad query powers in practice, and the requirement of:

> "subject matter expertise to formulate appropriate queries to derive the correct subset results. This has a significant reliance on understanding the construct of the ICR data queried, which may differ between TOs [*telecommunications operations]*, understanding of human verses machine generated connections, and

22 HC Deb, 19 February 2024, vol. 745, col. 531-2: https://hansard.parliament.uk/commons/2024-02-19/debates/A82D4C76-9E49-449A-9DA2-8679E216B0F5/InvestigatoryPowers(Amendment)Bill(Lords)

23 p.25, para. 116

understanding of computer logic and the importance of accurate syntax."[24]

The safeguards are essentially that the new Condition is limited to national security and serious crime, as follows.

33. D1 only applies to the intelligence services, who may access ICRs on this basis in interests of national security (including economic well-being of the UK) or for preventing or detecting serious crime, and the National Crime Agency (NCA) who may access ICRs on this basis for the purpose of preventing and detecting serious crime.

34. Clause 15 would also introduce new subsection 5B and condition D2, for the same speculative ICR power but whereby a designated senior officer can authorise access in more limited circumstances than a judicial commissioner under D1. For the intelligence services this is in the interests of national security (including economic well-being of the UK) or crime; for the NCA, it is only for urgent cases of preventing and detecting serious crime.

35. It should be noted that the intelligence agencies already have access to vast stores of internet records via bulk powers.

36. RECOMMENDATION 3: Big Brother Watch recommends that Members reject the expansion of internet connection records powers and oppose Clause 15.

24 Ibid. para. 117.

Surveillance of parliamentarians

Amendments:

After Clause 22

Insert the following new Clause -

"Interception notification for Members of Parliament etc.

After section 26 of the Investigatory Powers Act 2016 (Members of Parliament etc.) insert -

26A Interception notification for Members of Parliament etc.

(1) Upon completion of conduct authorised by a warrant under section 26, or the cancellation of a warrant issued under section 26, a Judicial Commissioner must notify the affected party,

in writing, of –

(a) the conduct that has taken place, and

(b) the provisions under which the conduct has taken place.

(2) The notification under subsection (1) must be sent within thirty days of the completion of the conduct or cancellation of the warrant.

(3) A Judicial Commissioner may postpone the notification under subsection (1) beyond the time limit under subsection (2) if the Judicial Commissioner assesses that notification may defeat the purposes of an on-going serious crime or national security investigation relating to the affected party.

(4) A Judicial Commissioner must consult with the person to whom the warrant is addressed in order to fulfil an assessment under subsection (3).

Effect: This amendment would require that members of a relevant legislation who are targets of interception are notified after the fact, as long as it does not compromise any ongoing investigation.

After Clause 23

Insert the following new Clause -

"Targeted equipment interference notification for Members of Parliament etc.

After section 111 of the Investigatory Powers Act 2016 (Members of Parliament etc.) insert -

111A Targeted equipment interference notification for Members of Parliament etc.

(1) Upon completion of conduct authorised by a warrant under section 111, or the cancellation of a warrant issued under section 111, a Judicial Commissioner must notify the affected party,

in writing, of –

(a) the conduct that has taken place, and

(b) the provisions under which the conduct has taken place.

(2) The notification under subsection (1) must be sent within thirty days of the completion of the conduct or cancellation of the warrant.

(3) A Judicial Commissioner may postpone the notification under subsection (1) beyond the time limit under subsection (2) if the Judicial Commissioner assesses that notification may defeat the purposes of an on-going serious crime or national security investigation relating to the affected party.

(4) A Judicial Commissioner must consult with the person to whom the warrant is addressed in order to fulfil an assessment under subsection (3).

Effect: This amendment would require that members of a relevant legislation who are targets of hacking are notified after the fact, as long as it does not compromise any ongoing investigation.

After Clause 23

Insert the following new Clause -

"Annual reporting on surveillance of Members of Parliament etc.

(1) Section 234 of the Investigatory Powers Act 2016 is amended as follows.

(2) In subsection (2) -

(a) In paragraph (c), after "information" insert "and Members of Parliament etc."

(b) After paragraph (d), insert new paragraph (da) -

(da) information in particular about warrants issued, considered or approved that are targeted interception warrants or targeted examination warrants of the kind referred to in section 26 and section 111 (Members of Parliament etc.)

Effect: This amendment would ensure that the Investigatory Powers Commissioner's annual reports provide (1) information about the operation of safeguards in relation to surveillance of Members of Parliament etc., (as is already required for journalists) and (2) information in particular about the warrants considered or approved targeted at Members of Parliament etc. (further to the general requirement to provide information on general targeted interception and hacking warrants).

Briefing:

37. The IPA permits the interception or hacking of parliamentarians (or members of other domestic legislative bodies) via a 'triple lock' system, whereby the Secretary of State cannot issue a warrant without the approval of the Prime Minister, as per s.26(2) and s.111(3).

38. Clause 22 of the present Bill seeks to permit the Prime Minister to appoint another Secretary of State to approve such exceptional warrants should they be unable (due to incapacity or inability to receive secure communications) to do so, by amending s.26(2) and s.111(3) of the IPA.

39. The motivation for this change stems from the hospitalisation of former Prime Minister Boris Johnson in April 2020 during the Covid-19 pandemic.[25] Big Brother Watch is concerned that this suggests the power may have been sought during this time.

40. Politicians are not above the law. However, Big Brother Watch has always been deeply concerned by powers to spy on domestic parliamentarians given their important constitutional role.

41. Until October 2015, it was widely understood that the **communications of MPs were protected from interception by the Wilson Doctrine.** On the 17th November 1966 the then Prime Minister, Mr Harold Wilson, said in a statement in the House of Commons:

> *"As Mr Macmillan once said, there can only be complete security with a police state, and perhaps not even then, and there is always a difficult balance between the requirements of democracy in a free society and the requirements of security. With my right hon. Friends, I reviewed the practice when we came to office and decided – on balance – and the arguments were very fine – that the balance should be tipped the other way and that I should give this instruction that there was to be no tapping of telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it. I am aware of all the considerations which I had to take into account and I felt that it was right to lay down the policy of no tapping of telephones of Members of Parliament."*[26]

42. This protection, extended to members of the House of Lords in 1966, was repeated in unequivocal terms by successive Prime Ministers. Tony Blair clarified in 1997 that the policy "applies in relation to telephone interception and to the use of electronic surveillance by any of the three Security and Intelligence Agencies."[27]

25 Independent Review of the Investigatory Powers Act 2016, Lord Anderson KBE KC, 30th June 2023, para. 8.13, p.73: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2
26 HC Deb 17 November 1966 Vol 736, cols 634-641.
27 HC Deb 4 December 1997 Vol 302, Col 321.

43. Despite this clear and unambiguous statement that MPs and Peers would not be placed under electronic surveillance, an October 2015 decision by the Investigatory Powers Tribunal held that the doctrine had been unilaterally rescinded by the Executive. Big Brother Watch and other rights groups dispute this finding.

44. In our first past the post voting system, the relationship between constituents and our elected representatives is the constitutional foundation of our representative democracy and has long been subject to the convention of confidential communications. We believe that there remains a reasonable expectation on the part of parliamentarians and their constituents that their correspondence is protected.

45. In any event, whilst we welcome any safeguards, we do not believe that the risks of unjustified political surveillance of parliamentarians are satisfactorily mitigated by further political sign off.

46. The widening of the safeguard against the surveillance of politicians provides an opportunity to consider what further safeguards are necessary.

47. Post-surveillance notification would mean that Judicial Commissioners have a mandatory statutory duty to notify parliamentarians subjected to surveillance once a particular operation or investigation has ended. This is a vital safeguard to protect rights and democracy, as it is the only way by which individuals can seek a remedy to protect their A8 rights – as stated by the European Court of Human Rights in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006:

> *"The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".*[28]

48. In Committee Stage [HL] responding to other peers' advocacy for a post-notification process for parliamentarians, Baroness Manningham-Buller, former head of MI5, spoke against the proposal even in circumstances

28 *Weber and Saravia v Germany, 2006*, application 54934/2000, para. 135.

where such notifications would not obstruct an ongoing investigation, stating "We cannot at any stage tell [a parliamentarian] because it risks sources and methods."[29] This is not the case. Post-notification can inform an individual of the fact of prior surveillance without disclosing the type, method, subject of interest, any sources, or other compromising details.

49. For example, the German surveillance system has a post-notification process, and notification is only given when it would not jeopardise the purpose of the original interference. Article 101 (4) of the German Criminal Code does not only confer a duty to notify the individual targeted by surveillance, but also other persons who may have also been concerned by the surveillance measures.[30] It is seen as a vital tool to enable individuals to seek redress, and to prevent abuse of secret powers. Notification must be give both into relation to traditional forms of surveillance (e.g. surveillance through undercover agents) and newer surveillance methods such as the use of IMSI-catchers.[31]

50. The Minister, Lord Sharpe, argued that the proposed post-notification safeguard of a Judicial Commissioner being able to postpone notification until it is safe to do so "would inappropriately afford the judicial commissioners an operational decision-making power."[32] This argument is misguided. Firstly, notifications would only occur there is no longer a surveillance operation active. Secondly, a post-notification system could also include a requirement for the Judicial Commissioner to consult the individual who applied for the warrant before issuing one. Of course, the government could adapt this further should they wish, as long as it does not detract from the principle of post-notification.

51. Lord Sharpe also recommended that parliamentarians who are concerned that they may have been affected by unlawful surveillance apply to the Investigatory Powers Tribunal:

29 HL Deb 13 December 2023, vol. 834, col. 1907: https://hansard.parliament.uk/lords/2023-12-13/debates/51FB9FCF-6913-4E43-9A13-FE370A990654/InvestigatoryPowers(Amendment)Bill(HL)
30 The Rights of Notification after Surveillance is Over: Ready for Recognition? Prof Paul de Hert, Dr. Franziska Boehm: https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Boehm_DeHert_Rights_of_notification_5d1bed8.pdf
31 The Rights of Notification after Surveillance is Over: Ready for Recognition? Prof Paul de Hert, Dr. Franziska Boehm: https://www.zar.kit.edu/DATA/veroeffentlichungen/237_Boehm_DeHert_Rights_of_notification_5d1bed8.pdf
32 HL Deb 13 December 2023, vol. 834, col. 1913: https://hansard.parliament.uk/lords/2023-12-13/debates/51FB9FCF-6913-4E43-9A13-FE370A990654/InvestigatoryPowers(Amendment)Bill(HL)

> "There are existing accountability routes that allow any individual, whether or not they are a Member of a relevant legislature, to challenge the activities of the intelligence services. Foremost among these is the Investigatory Powers Tribunal, which provides a cost-free right of redress to anyone who believes that they have been the victim of unlawful action by a public authority using covert investigative techniques."[33]

52. However, such steps are often not feasible, both legally and practically, following the Investigatory Powers Tribunal's judgment in the *Human Rights Watch & Others* case, in which the Tribunal introduced an evidentiary hurdle for applicants whereby they must show that "due to their personal situation, [they are] personally at risk of being subject to such [investigatory powers] measures".[34] **Without post-notification, it is not feasible that a parliamentarian would be able to seek redress** and they cannot practically meet such an evidentiary threshold and as such it is practically impossible for them to successfully apply to the Tribunal. **As Stuart McDonald MP said during Second Reading of the Bill:**

> **"Our role of representing our constituents, interrogating legislation and holding the Government to account should not be interfered with lightly. We should take the chance to consider post-surveillance notification of MPs who have been spied upon, by judicial commissioners, once investigations are completed. As matters stand at the moment, redress is almost impossible to obtain".**[35]

53. **RECOMMENDATION 4: The Bill should be amended to require that the Investigatory Powers Commissioner is informed of, and records in his annual report, the number of warrants authorised each year to permit surveillance of members of relevant domestic legislatures. This would ensure transparency over the rate at which the power is used.**

54. **RECOMMENDATION 5: Clauses 22 and 23 should be amended to introduce post-surveillance notification for parliamentarians.**

33 Ibid.
34 UK IPTrib 15_165-CH [2016] available at http://www.iptuk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf
35 HC Deb, 19 February 2024, vol. 745, col. 536: https://hansard.parliament.uk/commons/2024-02-19/debates/A82D4C76-9E49-449A-9DA2-8679E216B0F5/InvestigatoryPowers(Amendment)Bill(Lords)

Secret notices for tech companies

Amendment: We recommend that Members give notice of their intention to oppose the Question that Clause 18 stand part of the Bill.

Effect: This would prevent telecommunications operators from being unable to make technical changes to their services, such as improving privacy and security measures, whilst no relevant notice is in force.

Amendment: We recommend that Members give notice of their intention to oppose the Question that Clause 21 stand part of the Bill.

Effect: This would prevent telecommunications operators from having a duty to notify the Secretary of State of possible changes to their technical infrastructure.

55. A radical change to the IPA is 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. This is widely understood[36] 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. Big Brother Watch responded to the consultation on the proposed changes.[37]

56. Clause 21 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 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**

36 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

37 https://bigbrotherwatch.org.uk/wp-content/uploads/2023/08/IPA-notices-consultation.pdf

could be used to force companies to proactively report many of their product improvement plans to the Government.

57. 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)).

58. Clause 17 further claims extra-territorial application of data retention notices, as is the case for technical capability notices.

59. Clause 18 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.**

60. 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.

61. 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.

62. **Big Brother Watch is not aware of any country in the world that imposes such onerous and disproportionate obligations on private companies.**

63. **The proposal has been met with widespread condemnation from technology companies and human rights groups.[38] Big Brother Watch joined Liberty, Privacy International, Open Rights Group, Internet Society, and Rights and Security International in January in rallying against the proposed powers.[39] Last month, 27 security experts from around the world condemned the "disastrous consequences" of the proposals, including an increased risk of cybercrime, in a joint letter to the Home Secretary.**

64. **RECOMMENDATION 6: Clauses 18 and 21 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.**

38 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

39 https://bigbrotherwatch.org.uk/wp-content/uploads/2024/01/Joint-NGO-Briefing-on-Investigatory-Powers-Amendment-Bill-House-of-Lords-Report-Stage-17-1-24.pdf