BIG BROTHER WATCH

Big Brother Watch's Briefing on the Investigatory Powers (Amendment) Bill for the House of Lords, Second Reading

November 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

CONTENTS

Introduction

Big Brother Watch welcomes the opportunity to brief peers on the Investigatory Powers (Amendment) Bill ahead of Second Reading on Monday 20th November 2023. As the Bill was announced in the King's Speech on Tuesday 7th November 2023, and then published with its First Reading on Wednesday 8th November, there has regrettably been little time for civil society groups, or indeed parliamentarians, to afford the level of scrutiny that such serious powers in the Bill require ahead of Second Reading.

Nonetheless, as a group principally concerned with protecting privacy in the UK and that has successfully litigated against the UK Government's excessive mass surveillance powers, we have sought to provide an initial analysis to support parliamentarians' scrutiny in the short time given.

Big Brother Watch supports the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. However, the UK has suffered from unlawful uses of surveillance powers in recent years and now has adopted a strategy of deploying untargeted, intrusive surveillance powers over the general population. The Snowden revelations and subsequent litigation by Big Brother Watch (*Big Brother Watch v UK),* Liberty, Open Rights Group, Privacy International and others – some of which is ongoing – have repeatedly identified unlawful state surveillance by UK agencies that took place absent the knowledge of parliamentarians. 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' system. The Act is subject to ongoing litigation.

It is concerning, but in such an enabling environment perhaps unsurprising, 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 five primary concerns with the Investigatory Powers (Amendment) Bill are:

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

- weaken safeguards for authorities to harvest **communications data**

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

- expand the politicians that can authorise the **surveillance of parliamentarians** and members of other domestic legislative bodies

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

Recommendations:

RECOMMENDATION 1: So-called 'low privacy' BPDs should be reviewed and scrapped; if they are retained, at the very least they must be given a clear, objective definition that accords with relevant existing laws such as the DPA.

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 11 should be removed from the Bill.

RECOMMENDATION 3: Big Brother Watch recommends that parliamentarians reject the expansion of internet connection records powers.

RECOMMENDATION 4: In his review of the operation of the IPA, Lord Anderson recommended that if ICRs are expanded in the way currently proposed in this Bill, that the new conditions are restricted to the intelligence agencies at least in the first instance.[1] Whilst Big Brother Watch rejects the broader premise for the ICR powers, we agree that such a restriction would be an improvement on the present suggestion.

RECOMMENDATION 5: 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 6: The Bill should be amended to introduce post-surveillance notification for parliamentarians.

RECOMMENDATION 7: 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.

1 Independent Review of the Investigatory Powers Act 2016, Lord Anderson KBE KC, 30th June 2023, p.49: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2

Bulk Personal Datasets

1. 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.

2. 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.

3. 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 or other data from social media posts over time.

4. 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.

5. 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.

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

7. 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.

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

8. 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 Jews recently hacked from a commercial DNA company,[5] be considered a 'low privacy' database under this definition?

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

10. 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[6], and David Anderson's 'Report of the Bulk Powers Review' of the same period.[7] Indeed, the collation, retention and processing of records of potentially the entire population is the essence of a surveillance society. BPD appear to be widely used – 177 warrants were sought and approved in 2021[8]. 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.

11. 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

5 https://www.wired.com/story/23andme-credential-stuffing-data-stolen/
6 https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-submission-to-the-Terrorism-Reviewers-Review-of-Bulk-Powers.pdf, pp.14-15
7 https://www.libertyhumanrights.org.uk/wp-content/uploads/2021/04/Libertys-Response-to-the-Report-of-the-Bulk-Powers-Review.pdf, p.16
8 https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf, p.112

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'[9] involving 'several areas of serious concern'.[10] 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.

12. **RECOMMENDATION 1: So-called 'low privacy' BPDs should be reviewed and scrapped; if they are retained, at the very least they must be given a clear, objective definition that accords with relevant existing laws such as the DPA.**

Communications Data

'Public' communications data

13. 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.

14. Clause 11 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'.

15. We are concerned about one such example, which is (3A)(e): 'where the communications data has been published before the relevant person

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

obtained it', whereby 'publish' means (3B) 'make available to the public or a section of the public (whether or not on a commercial basis)'.

16. 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.

17. 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."[11]

18. We are concerned that, for example, if an environmental campaigns group such as Extinction Rebellion 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.

19. **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 11 should be removed from the Bill.**

Location data

20. Clause 12 of the Bill would amend the IPA definition of communications data at s.261 to include entity data that identifies or assists in the

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

identification of an entity and that entity's location. This is ostensibly to address a claimed lack of clarity as to whether subscriber data is communications data or content – the explanatory notes state that the proposal "would have the practical effect of clarifying that this [subscriber] data is communications data rather than content."[12]

21. The IPA defines three different types of relevant communications data: entity data, events data and internet connection records. In essence, 'entity' data is data about an individual and what telecommunications services they use, and 'events' data is about activity/how the telecommunications service is used.

22. A higher threshold applies to obtain events data than to obtain entity data, due to the intrusiveness of the former. Under s.60A(8)(a) of the IPA, events data can only be obtained in the context of crime where it is for the purpose of 'preventing or detecting **serious** crime' (emphasis added), but there is no requirement of seriousness to obtain entity data, which can be obtained for 'the purpose of preventing or detecting crime or of preventing disorder' (s.60A(8)(b)).

23. The different thresholds applying to different types of communications data followed litigation initiated by British parliamentarians aiming to defend the right to privacy, David Davis MP and former MP Tom Watson, and the CJEU's subsequent judgment of 21 December 2016 on the joined cases *R (Watson) v Secretary of State for the Home Department* (Case C-698/15) ("*Watson*") and *Tele2 Sverige AB v Post- och telestyrelsen* (Case C-203/15). The judgment specified a number of requirements that need to be in place for a Member State's data retention regime to be compliant with EU data protection law and the European Charter of Fundamental Rights – notably, that the general and indiscriminate retention of communications data is unlawful, and that communications data may only be retained and accessed in relation to fighting serious crime, after independent authorisation has been granted, in addition to other safeguards.

24. The UK Government argued that "The CJEU judgment refers to only certain types of communications data - traffic data and location data, as defined in Directive 2002/58/EC ('the ePrivacy Directive')" and that as such, "the CJEU's judgement should be read as applying to 'events data' but does not

12 p.42, para 252

apply to the retention or acquisition of 'entity data'"[13] under the IPA. As such, the Government responded by only applying a higher threshold to obtain events data, as it relates to traffic and location data, but not entity data.

25. Big Brother Watch has always maintained that *Watson* required that higher thresholds should be applied to the communications data regime as a whole. The judgment also recited Directive 2006/24/EC, which applies "to **traffic and location data** on both legal entities and natural persons and to the **related data necessary to identify the subscriber or registered user.**"[14] Even if one were to accept the UK Government's interpretation of the judgment, the separation of 'events' and 'entity' data does not even serve the purpose of separating the more sensitive traffic and location from less sensitive identifying data in the way the Government claims it does via these two definitions, as 'entity' data in the IPA can include 'data which identifies or describes the entity (whether or not by reference to the entity's location)' (s.261(3)(b)). That is, 'entity' data can include location data.

26. However, the change proposed in the present Bill goes even further to include location data in the definition of 'entity' data, and so further undermines the *Watson* judgment. Clause 12 of the Bill would introduce a new subsection 5A to s.261 IPA, whereby entity data expressly includes data that 'may be used to identify, or assist in identifying, the location of that entity.' This contrasts the existing definition of entity data which can include location data only insofar as that data identifies or describes the entity – it cannot include data that otherwise locates an entity, which would be 'events' data.

27. The ePrivacy Directive defines location data as 'any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.' The Government responded to *Watson* by claiming that "data covered by the definition of 'events data' in section 261 of the IPA includes the data covered by the definitions of 'traffic data' and

13 Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.10-11 https://assets.publishing.service.gov.uk/media/5a81bf17ed915d74e33ffd5c/November_2017_IPA_Consultation_-_consultation_document.pdf

14 European Union Directive 2006/24/EC, (Data Retention Directive), 15 March 2006 (emphasis added)

'location data' in the ePrivacy Directive".[15] However, the amendment proposed in this Bill would seem to expressly include location data. There is nothing in the new proposed definition that would clearly distinguish between location data within entity or events data.

Internet Connection Records

28. 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".[16] No other European or indeed Five Eyes country has surveillance laws that allow for the compulsory generation and retention of ICRs or "web logs".[17]

29. 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 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.

30. 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".[18] 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."[19] The "usefulness" of a power is insufficient to assess whether the power is strictly necessary and proportionate, and as such a lawful invasion of individuals' A8 right to privacy. We are concerned that the attempt to

15 Investigatory Powers Act 2016: Consultation on the Government's proposed response to the ruling of the Court of Justice of the European Union on 21 December 2016 regarding the retention of communications data, November 2017, p.11 https://assets.publishing.service.gov.uk/media/5a81bf17ed915d74e33ffd5c/November_2017_IPA_Consultation_-_consultation_document.pdf

16 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

17 Ibid, p.45

18 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

19 p.13

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, via rushed legislation, then the surveillance framework could easily grow 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.[20]

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

33. 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 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 understanding of computer logic and the importance of accurate syntax."[22] The safeguards are essentially that the new Condition is limited to national security and serious crime, as follows.

20 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
21 p.25, para. 116
22 Ibid. para. 117.

34. 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.

35. Clause 14 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) and only for the prevention and detection of serious crime in urgent cases; for the NCA, it is only for urgent cases of preventing and detecting serious crime.

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

37. **RECOMMENDATION 3: Big Brother Watch recommends that parliamentarians reject the expansion of internet connection records powers.**

38. **RECOMMENDATION 4: In his review of the operation of the IPA, Lord Anderson recommended that if ICRs are expanded in the way currently proposed in this Bill, that the new conditions are restricted to the intelligence agencies at least in the first instance.[23] Whilst Big Brother Watch rejects the broader premise for the ICR powers, we agree that such a restriction would be an improvement on the present suggestion.**

Surveillance of parliamentarians

39. 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).

23 Independent Review of the Investigatory Powers Act 2016, Lord Anderson KBE KC, 30th June 2023, p.49: https://www.gov.uk/government/publications/independent-review-of-the-investigatory-powers-act-2016--2

40. Clause 21 of the present Bill seeks to permit the Prime Minister to appoint another Secretary of State to approve such exceptional warrants should they be 'unavailable' to do so, by amending s.26(2) and s.111(3) of the IPA. Clause 21 does not define what precisely is meant by 'unavailable'.

41. The motivation for this change stems from the hospitalisation of former Prime Minister Boris Johnson in April 2020 during the Covid-19 pandemic.[24] Big Brother Watch is concerned that this suggests the power may have been sought during this time.

42. 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.

43. 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."[25]

44. 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

24 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

25 HC Deb 17 November 1966 Vol 736, cols 634-641.

interception and to the use of electronic surveillance by any of the three Security and Intelligence Agencies."[26]

45. 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.

46. 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.

47. 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.

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

49. RECOMMENDATION 5: 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.

50. RECOMMENDATION 6: The Bill should be amended to introduce post-surveillance notification for parliamentarians.

51. 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:

26 HC Deb 4 December 1997 Vol 302, Col 321.

"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".[27]

Secret notices for tech companies

52. 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[28] 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.[29]

53. 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 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.

27 *Weber and Saravia v Germany, 2006*, application 54934/2000, para. 135.
28 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
29 https://bigbrotherwatch.org.uk/wp-content/uploads/2023/08/IPA-notices-consultation.pdf

54. 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)).

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

56. 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.

57. 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.

58. 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.

59. 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.[30]

60. **RECOMMENDATION 7: 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.**

30 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