Joint Briefing on the Investigatory Powers (Amendment) Bill

House of Lords, Report Stage

January 2024

The Snowden revelations and subsequent litigation – 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 stated intent to regulate the rapidly growing surveillance state via a democratic process, the highly controversial Investigatory Powers Act 2016 (IPA) authorised massive, suspicionless surveillance on a scale never seen before, with few safeguards or independent oversight. The Act is subject to ongoing litigation.

Despite these ongoing and serious concerns about the IPA and its implementation by the security services, the government now seeks to rush through significant privacy-weakening changes to the UK's surveillance regime.

Among other things, we are concerned that the Investigatory Powers (Amendment) Bill:

- weakens safeguards when intelligence services collect **bulk datasets of personal information**, potentially allowing them to harvest millions of facial images and social media data;

- expressly permits the harvesting and processing of **internet connection records** for generalised, massive surveillance;

- expands the range of politicians who can authorise the **surveillance of parliamentarians**; and

- would force technology companies, including those based 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 and eroding the security of devices and the internet.**

We are also concerned that many of these powers may be incompatible with the UK's obligations under Article 8 of the European Convention on Human Rights.

We call on Peers to:

- Oppose clauses 1, 2, 14, 17, 18, 19 and 20; and

- Significantly amend Clauses 21 and 22 to (1) emphasise the extraordinary nature of powers to surveil parliamentarians and (2) provide additional safeguards to prevent their abuse, such as a post-notification and annual reporting requirement.

BULK PERSONAL DATASETS

CLAUSES 1 AND 2

1. Part 7 of the IPA permits the intelligence services to harvest 'bulk personal datasets' (BPDs), 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). BPDs represent one of the most controversial capabilities under UK law, expressly intended for generalised mass surveillance intruding on the private lives of people who are not suspected of any crime.

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 the security services decide that the information involves 'low or no reasonable expectation of privacy'. Where it believes that the bulk data involves only 'low privacy' data, an agency will not need to seek the approval of a judicial commissioner to retain the dataset, as long as 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 that broader category. In plain English, this means, for example, that if the security services decide that people have 'low or no reasonable expectation of privacy' in direct messages or voice or video calls made via social media sites, or their face as it appears on CCTV recordings, then it will be able to grab this data for millions of people.

3. The Bill does not define the 'low privacy' BPD category, but, according to the Bill, the government says 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 the UK – in particular, data protection law and human rights law. Such an undefined category requires agencies that want to process such data to determine levels of safeguards according to potentially arbitrary ideas about other people's expectations of privacy over their data. In other areas, the law takes account of the actual sensitivity of the information rather than whether a person has kept their own information strictly secret from every other person or company.

5. The proposal of such a poorly defined 'low privacy' category of BPDs could lead to some of the most intrusive BPDs yet subject to the lowest safeguards. For example, the Bill could be interpreted so that massive databases of 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, under the reasoning that those photos have 'been made public by the individuals'. 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 result in secret government files about billions of people's social networks, sexual orientations, political opinions, religion, health status, and so on. Under the Data Protection Act 2018 (DPA), much of this data qualifies as 'special category data' because it is sensitive and because abuse of the information could have severe consequences for the person affected; the DPA therefore currently requires extra for such data, 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 process 'special category' data (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).[1] 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'.[2] 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 Bill, they would have been considered personal data and possibly subject to the above-mentioned sensitive processing safeguards, under the Data Protection Act 2018.

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 Jewish people recently hacked from a commercial DNA company,[3] be considered a 'low privacy' database under this definition?

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

> *"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."*[4]

However, this is a misunderstanding of the issue. We do not argue 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'. In other words, there are no firm rules. The new Part 7A certainly does not contain any

[1] Data Protection Act 2018, s86
[2] Data Protection Act 2018, Schedule 10
[3] Lily Hay Newman, '23andMe User Data Stolen in Targeted Attack on Ashkenazi Jews', *Wired*, 6 October 2023: https://www.wired.com/story/23andme-credential-stuffing-data-stolen/
[4] HL Deb, 20th November 2023, vol. 834, col. 650-1

clear prohibition on leaked commercial datasets or billions of facial images scraped from the internet being considered 'low privacy' datasets.

10. 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. It may also violate the right to respect for private life as established in Article 8 of the European Convention on Human Rights, as discussed below.

11. Further, even though the draft Bill provides a list of 'factors' for the security services to consider when assessing whether a BPD is within the 'low privacy' category, it is difficult to envisage how the security services could accurately consider individuals' expectations on such a high level. Such an assessment is likely to be premised on the basis of presumptions and generalisations, as opposed to a concrete assessment of whether the individuals concerned had a reasonable expectation of privacy.

12. In our view, the existing Part 7 powers to retain bulk personal datasets also fail to meet the requirements of necessity and proportionality in accordance with Article 8 of the European Convention on Human Rights. Indeed, the collation, retention and processing of records of potentially the entire population is the essence of a surveillance society. It is also the government's obligation to explain why the changes to the legislation are necessary interferences with our rights. The government has not provided such an explanation when introducing this Bill, instead referring to the idea that the amendments will be 'useful' or 'effective'.[5]

13. This is particularly concerning given how the security services currently use BPDs. In its most recent report, 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

[5] Home Office, 'Investigatory Powers Act 2016: Post Implementation Review', 28 April 2023, pp.14-15: https://assets.publishing.service.gov.uk/media/654cb845b9068c00130e7607/Annex_A_-_2023-04-28_IPA_Review_PIR.pdf

and auditing of systems used to query and analyse BPDs'[6] involving 'several areas of serious concern'.[7] It also found that the agencies were responsible for 29 errors involving BPD, for example, when officers access an individual's records without reason. Rather than remedy the legislation which facilitated those errors, the government has instead decided to grant the security services even greater discretion in how to use BPDs, while removing the already limited safeguards preventing their misuse.

14. The government's focus on whether somebody has a 'reasonable expectation of privacy' will open the door for further errors and misuse of the security services' surveillance powers. In the United States, for example, the 'reasonable expectation of privacy' standard has, as Aliza Hochman Bloom, Assistant Professor of Law at Northeastern University, explains:

> *"maintain[ed] a predictable reasonable person, labeled as "objective,"… [and] excluding an individual's race… contribut[ing] to a reasonableness standard which is increasingly unmoored from reality and subjectively marginalizes groups, particularly Black men."*[8]

Responding to the Committee Stage debate

- Lord Coaker and Lord Fox were among peers who rightly raised concerns about 'low privacy' BPD in the Committee Stage debate including, significantly, the discrepancy between existing data protection and privacy law and the new concept of subjective data privacy 'expectations'. The Minister, Lord Sharpe's, essential defence of this was that the law will change – perhaps a reference to the government's serious dilution of data and privacy rights via the Data Protection and Digital Information Bill, currently going through parliament:

> *"The law concerning the reasonable expectation of privacy is likely to develop over time, and new Section 226A is intended*

[6] IPCO and OCDA, 'Annual Report of the Investigatory Powers Commissioner 2021', HC 910, 20 March 2023, p.47: https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/Annual-Report-2021.pdf
[7] Ibid. p.49
[8] Aliza Hochman Bloom, 'Objective Enough: Race is Relevant to the Reasonable Person in Criminal Procedure' (2023) 19(1) Stanford Journal of Civil Liberties 1, p.6

to be sufficiently flexible to accommodate future changes. (...and) to ensure that the intelligence services can continue to apply the law as it develops."

It is wholly inappropriate to legislate in anticipation of synchronisation with other controversial Bills that have not yet passed into law. Indeed, the Data Protection and Digital Information Bill has not yet even been considered in the House of Lords. This is bad law-making.

- We are concerned that the government was unable to explain how the worrying 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.

We recommend that Peers oppose Clauses 1 and 2.

INTERNET CONNECTION RECORDS

CLAUSE 14

15. Internet Connection Records (ICRs) were a new category of surveillance data, introduced in the IPA and allowing the Home Secretary to require telecommunications operators to generate and retain ICRs 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".[9] No other European or Five Eyes country has surveillance laws that explicitly allow for the compulsory generation and retention of ICRs or 'web logs' for people within their own borders.[10]

16. 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. This approach is targeted and specific. Clause 14 of the Bill would amend s.62 to add a further purpose for which

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

[10] Ibid, p.45

ICRs can be used – for 'target discovery'. That is, generalised surveillance. It does this by adding the condition 'D1' to the existing grounds for using ICRs: "to identify which persons or apparatuses are using one or more specified internet services in a specified period".

17. In 2015-6, the then-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".[11] However, the government now wishes to go beyond what Parliament authorised. The explanatory notes accompanying the present Bill explain 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."[12]

18. 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 – potentially through the use of problematic algorithmic decision-making, also known as 'predictive policing' – even when there is no reason to believe that the person has engaged in any wrongdoing. Generalised, mass, suspicionless surveillance like this is ineffective and prone to mistakes, and focuses on supposed 'pre-crime' in a way that is not consistent with the principles of a democratic society.[13]

19. 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".[14] He further explained:

[11] Home Office, 'Operational Case for the Retention of Internet Connection Records', 1 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

[12] p.13

[13] Committee on Responding to Section 5(d) of Presidential Policy Directive 28, 'Bulk Collection of Signals Intelligence: Technical Options', The National Academies Press, 2015, p.43

[14] HL Deb 11th December 2023, vol. 834, col. 1753

> *"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."*[15]

20. This shift in focus towards using ICRs as a method of target discovery also means that people who have done nothing wrong, and are not suspected of doing anything wrong, are likely to get caught up within the surveillance infrastructure, and wind up with permanent, secret government dossiers about their private lives.

21. 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.

22. We must also remember that a 'useful' power is not the same as a strictly necessary one.[16] As noted above, in order for an interference with an individual's Article 8 right to privacy to be lawful, the government must justify its necessity to protect national security. The government's failure to provide such an explanation is, in our view, because it cannot.

23. The government is also aware of the privacy harms that will likely result from implementing Clause 14. The Bill's 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*

[15] HL Deb 11th December 2023, vol. 834, col. 1754
[16] E.g. App. No. 47173/06, *Zakharov v. Russia*, 4 December 2015, paras. 229-232; App. No. 8691/79, *Malone v. the United Kingdom*, 2 August 1984, para. 68

proposed in this Bill with the intention of managing access to this new Condition and mitigating public concerns."[17]

But the government also recognise the fallibility of using ICRs on D1 grounds. The explanatory notes 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."*[18]

24. In sum, the additional powers introduced in Clause 14 are harmful, unnecessary and susceptible to error.

We call on Peers to oppose Clause 14.

SURVEILLANCE OF PARLIAMENTARIANS

CLAUSES 21 and 22

25. The IPA permits the interception or hacking of parliamentarians' (or members of other domestic legislative bodies) communications subject to a 'triple lock' authorisation process, 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).

26. Clause 21 of the present Bill seeks to permit the Prime Minister to appoint another Secretary of State to approve such exceptional interception warrants should they be 'unavailable' to do so, by amending s.26; Clause 22 does the same with regards to

[17] p.25, para. 116
[18] Ibid, para. 117

targeted equipment interference (hacking) warrants by amending and s.111 of the IPA. Clause 21 does not define what 'unavailable' means.

27. Politicians are not above the law. However, we have always been deeply concerned by powers to spy on domestic parliamentarians given their important constitutional role. Until October 2015, it was widely understood that the communications of MPs were protected from interception by the Wilson Doctrine, based on the then Prime Minister, Harold Wilson's, 17th November 1966 statement to the House of Commons.[19]

28. 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."[20]

29. 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. Human rights groups dispute this finding.

30. 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.

31. This proposed widening of the safeguard against the surveillance of politicians provides an opportunity to consider what further safeguards are necessary. We believe that, at minimum, the Bill should be amended to require that the Investigatory Powers Commissioner records in their 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.

32. Further, the Bill should be amended to introduce post-surveillance notification for parliamentarians. Post-surveillance notification would mean that Judicial Commissioners have a mandatory statutory duty to notify parliamentarians who have

[19] HC Deb 17 November 1966 Vol 736, cols. 634-641
[20] HC Deb 4 December 1997 Vol 302, col. 321

been subjected to surveillance once the 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 learn about potential rights violations and seek a remedy under Article 8 – as repeatedly stated by the European Court of Human Rights.[21]

Responding to the Committee Stage debate:

- Lord Fox tabled new clauses that would provide for a post-notification process for parliamentarians affected by surveillance, when it is safe to do so.

- Baroness Manningham-Buller, former head of MI5, spoke against post-notification for parliamentarians, even in circumstances where such notifications would not obstruct an ongoing investigation, stating "We cannot at any stage tell [a parliamentarian] because it risks sources and methods." [22] However, this is not the case. Post-notification can inform an individual of the fact of surveillance without disclosing the type, method, subject of interest, any sources, or other compromising details.

- For example, German surveillance practices entail a post-notification process, and notification is only given at a point when it would not jeopardise the purpose of the original interference. It is seen as a vital tool to enable individuals to seek redress, and to prevent abuse of secret powers. Notification must be given 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.[23]

- Baroness Manningham-Buller also opposed post-notification for parliamentarians because she believed it could stimulate an expectation of post-notification among the general public:

> *"(…) it raises the question of why Members of legislatures should have the privilege of being told that they have been subject to interception when members of the public never are. It*

[21] E.g. App. No. 54934/00, *Weber and Saravia v. Germany*, 29 June 2006, para. 135
[22] HL Deb 13 December 2023, vol. 834, col. 1907
[23] Paul de Hert and Franziska Boehm, 'The Rights of Notification after Surveillance is over: Ready for Recognition?', in Jacques Bus et al, Digital Enlightenment Yearbook 2012 (IOS Press, 2012), 19-39

is wrong, as it was, to treat parliamentarians as a particularly special case."[24]

- We believe all individuals should have the right to post-notification of surveillance. Indeed, in Germany, Article 101 (4) of the German Criminal Code establishes a duty to notify not only the individual targeted by surveillance, but also other persons who may have been caught up in the surveillance measures.[25]

- 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."[26] This argument is misguided. Firstly, notifications would only occur when the surveillance operation is no longer 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. Other solutions may be possible, as long as they respect the Convention and do not detract from the principle of post-notification.

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

> *"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."*[27]

- 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,

[24] Ibid
[25] Ibid
[26] HL Deb 13 December 2023, vol. 834, col. 1913
[27] Ibid

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". [28] Without post-notification, it is not feasible that a parliamentarian would be able to meet such an evidentiary threshold and as such it would be practically impossible for them to successfully apply to the Tribunal.

We call on Peers to significantly amend Clauses 21 and 22 to emphasise the extraordinary nature of powers to surveil parliamentarians while also introducing additional safeguards to prevent their abuse, such as a post-notification and annual reporting requirement.

SECRET NOTICES FOR TECH COMPANIES

CLAUSES 17-20

33. The government proposes a radical change to the IPA with 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 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.[29]

34. 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 them to notify the Secretary of State if they propose 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)) through secondary legislation 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

[28] *Human Rights Watch Inc. & Others v. Secretary of State for the Foreign & Commonwealth Office & Others* [2016] UKIPTrib15_165-CH, 16 May 2016

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

to assist with *any* surveillance warrant, authorisation or notice that could be issued under the Act (s.258A(4)).

35. The government's policy statement regarding the future regulations that will define what constitutes a 'relevant change' (published on 5 December 2023) gives several examples of what are likely to be relevant changes for the purposes of Clause 20.[30] We are very concerned about the suggested examples, which include any change to a business's data retention period as well as changes in the capabilities of an operator to provide the intelligence services with communications data and/or content.

36. Companies regularly change their data retention policies often with significant implications for the individuals whose data they process. (For example, they may shorten their retention period in response to a data protection complaint.) The inclusion of this example suggests that the government intends to use this surveillance power frequently. The new power, with its implications for the government's ability to access communications data and/or content from a particular system or service, appears to be squarely aimed at innovations and updates to encryption technology as well as security patches. In relation to the latter, the policy statement denies that security patches could be subject to the notification requirement. However, it also does not rule out the surveillance power being used to gather this information, stating instead that: *"we cannot foresee a circumstance in which a security patch would have such a sweeping effect on lawful access capabilities"*. Should such a circumstance come to pass, it is unclear whether the intelligence services would demand changes to such routine, but integral information security measures that underpin the security of all data processing operations.

37. An operator who receives such a notice will be forbidden from disclosing possession of this secret notice to anyone, at all, without permission (s.258(8)); and they will be required to comply with the notice within 'a reasonable time' before making the changes (s. 258A(9)). There would therefore be a complete lack of transparency around the exercise of a substantial surveillance power. This should be seen in the context of a provision that does not include any independent judicial authorisation

[30] Home Office, 'Policy statement on draft regulations for the notification of proposed changes to telecommunications services', 5 December 2023: https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-policy-statement

and oversight as well as no clear route for companies to challenge such a notification requirement – in contrast to the notices regime, which includes judicial authorisation and a mechanism to challenge the imposition of a notice. Requiring notification 'a reasonable time' before making changes may also unreasonably delay important security updates.

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

39. 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 impose 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 justifying the privacy infringement.

40. 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'), the new Clauses 17 and 20 would seek to further compel companies to proactively consult – and be bound by -- the government on their privacy and security measures with a view to ensuring state surveillance capabilities.

41. As Lord Fox warned during Committee Stage of the Bill:

> *"This modified process would stifle attempts to innovate encryption technology and would prevent companies responding quickly to growing data security threats—I would emphasise more the latter than the former. It empowers the Secretary of State effectively to issue an unreviewable extrajudicial injunction to prohibit the release of a new technology, and it would force companies to withhold end-to-end encryption features or other*

new technologies from users, even in the light of evolving threats to their users' data services."[31]

42. In addition to stifling innovation and reducing the security of the processing of personal data on which the digital economy and everyday life depends, the changes proposed at Clauses 17 and 20 may also imperil the EU's 2021 Adequacy Decision, which enables the seamless flow of personal data from the EU to the UK. The European Commission relied heavily on the existence of safeguards under UK law, which would be undermined by Clauses 17 and 20. Protections such as the double lock (to which neither of these two provisions are subject) as well as foreseeability as to how data is likely to be processed were cited in the European Data Protection Board's Opinion regarding the adequacy decision.[32] We note that the adequacy decision contains a sunset clause expiring in 2025 ensuring that the decision would be reversed if the UK does not ensure an adequate level of data protection. As per a 2020 UCL report, *The Cost of Inadequacy: the Economic Impacts of the UK Failing to Secure an EU Adequacy Decision* (prepared prior to the 2021 adequacy decision), the failure to have an adequacy framework in place could impact the UK economy significantly including through:[33]

    1. Increased cost of doing business, due to new compliance requirements.
    2. Increased risk of GDPR fines.
    3. Reduction in EU-UK trade and digital trade.
    4. Reduced investment (both domestic and international).
    5. Relocation of business functions, infrastructure, and personnel to outside the UK.

[31] HL Deb 11 December 2023, vol. 834, col. 1764

[32] EDPB, Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom, 13 April 2021, https://edpb.europa.eu/system/files/2021-04/edpb_opinion142021_ukadequacy_gdpr.pdf_en.pdf

[33] UCL and the New Economics Foundation, 'The Cost of Inadequacy: the Economic Impacts of the UK Failing to Secure an EU Adequacy Decision', November 2020, p.21: *https://www.ucl.ac.uk/european-institute/sites/european_institute/files/ucl_nef_data-inadequacy.pdf*

43. In all, the proposal is a chilling reflection of the government's attitude towards the legally protected rights to privacy and freedom of expression as well as a blow to technical innovation and cybersecurity. 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' – and, potentially forbidding locks altogether.

44. We are not aware of any country in the world that legally imposes such onerous and disproportionate obligations on private companies. The proposal has been met with widespread condemnation from technology companies and human rights groups.[34]

We recommend that Peers oppose Part 4 of the Bill.

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

CONTACT

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.

Silkie Carlo, Director, 02080758478, silkie.carlo@bigbrotherwatch.org.uk

Internet Society

The Internet Society is a global non-profit organization founded in 1992 by some of the Internet's early pioneers. We believe the Internet is a force for good and we are working towards an open, globally connected, secure and trustworthy Internet that benefits everyone. With 110 active chapters across six continents, of which 28 are in Europe, and more than 100.000 individual users supporting our activities, the Internet Society is a significant stakeholder, and a reliable, technically informed civil society interlocutor for Internet governance issues.

Robin Wilton, Director of Internet Trust, wilton@isoc.org

Liberty

Liberty is an independent membership organisation. We challenge injustice, defend freedom and campaign to make sure everyone in the UK is treated fairly. We are campaigners, lawyers and policy experts who work together to protect rights and hold the powerful to account. Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, inquiries and other policy fora, and undertake independent, funded research. Liberty's policy papers are available at libertyhumanrights.org.uk/policy.

Emmanuelle Andrews, Policy and Campaigns Manager, EmmanuelleA@libertyhumanrights.org.uk

Open Rights Group

Open Rights Group is the UK's largest grassroots digital rights campaigning organisation with over 20,000 supporters across the country. ORG fights for a fair digital environment where technology supports justice,

equality, and freedom. We work to protect everyone's rights to privacy and free speech online through public campaigns, media commentary, legal actions, and policy interventions.

Abby Burke, Programme Manager – Platform Power, aburke@openrightsgroup.org

Privacy International

Privacy International is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology.

Caroline Wilson Palow, Legal Director and General Counsel, caroline@privacyinternational.org

Rights & Security International

Rights & Security International is a London-based charity working to eliminate human rights abuses committed in the name of national security. We challenge religious, racial and gender bias in national security policies, and advocate for justice and transparency for victims of human rights abuses.

Jacob Smith, UK Accountability Team Leader, 07919435371, jsmith@rightsandsecurity.org