WRITTEN EVIDENCE FROM FREEDOM FROM PRIVACY INTERNATIONAL (IPA0004)

Introduction

1. Privacy International (PI) welcomes the opportunity to provide input in relation to the inquiry of the Joint Committee on Human Rights (JCHR) regarding the Investigatory Powers Amendment Bill (IPAB). PI is a charity that researches and advocates globally against government and corporate abuses of data and technology.[1]

2. We are concerned that the IPAB would expand unprecedented and disproportionate surveillance powers in ways that are likely to be detrimental for human rights and the rule of law. In this evidence, we cover the following concerns:

    a. The new "low or no reasonable expectation of privacy" bulk personal dataset (BPD) regime: The proposed provisions include new legal definitions that run counter to longstanding principles of privacy law and omit crucial safeguards to prevent abuse, as required by the ECHR.

    b. The new third-party BPD regime: This may allow intelligence services to access data that has been collected or processed contrary to the law and fails to provide for the proper management of third-party BPDs.

    c. The new notification requirement: This may have the effect of preventing companies from innovating and establishing practices that enhance privacy and security.[2]

3. Analysis of the text of the Bill and accompanying documentation stands in contrast to the government's positioning, which is that the changes set out in the Bill are *"not about expanding the powers but maintaining them, and ensuring their effectiveness, in the modern digital economy",* and that they seek *"to protect the existing capabilities that keep our citizens safe."* [3] We do not consider that the government's proposals can reasonably be characterised in this way.

The "low or no reasonable expectation of privacy" BPD

4. Part 7 of the IPA allows the intelligence services to retain and examine BPDs, which are composed of individuals' personal data, the majority of which are not, and are unlikely to become, of interest to the intelligence services in the exercise of its functions. This is a

[1] https://privacyinternational.org/

[2] For more detail on this point, see our response to the Government consultation on changes to the notices regime: https://privacyinternational.org/advocacy/5088/pi-response-uk-government-consultation-technical-capabilities-notices

[3] https://www.gov.uk/government/consultations/revised-investigatory-powers-act-notices-regimes-consultation/outcome/government-response-to-the-home-office-consultation-on-revised-notices-regimes#executive-summary

mass surveillance power that constitutes a serious interference with the right to privacy as protected by Article 8 ECHR. The Bill will permit the intelligence services to rely on a new type of BPD, 'low privacy BPDs'.

5. The new low privacy BPD would facilitate the mass collection of publicly available data, including social media data such as written posts, videos, and images among other forms of personal data.

6. When assessing what constitutes a low privacy BPD, the intelligence services are able to consider a number of factors – the majority of which relate to the public nature of the data, including the extent to which it is known about and has previously been used (Clause 2 of the IPAB). This creates a false equivalence between the availability of the personal data, including how it is obtained, and the privacy protections it attracts. The equivalence is erroneous for two reasons, which we illustrate using social media data.

    a. Firstly, publicly available social media data will frequently be no less sensitive than that which is obtained through covert social media monitoring. Even if it is made public by an individual, it may contain personal data relating to political opinions (which is likely to be of particular interest to the intelligence services).[4] While Section 226A(3)(a) as inserted by Clause 2 includes consideration of the nature of the data in question, this is one factor weighed against four others[5] that relate to the public quality of the data tilting the balance.

    b. Secondly, an individual's reasonable expectation of how their data will be processed if they publish something publicly is unlikely to include further use by the intelligence services as part of a low privacy BPD. A fact and context specific assessment of the reasonable expectations of a data subject as regards how their data will be used is critical to determine if a measure interferes with data protection principles and the right to privacy.[6] This conception of an individual's reasonable expectation of privacy is at odds with that in IPAB, which assumes that a data subject who publishes data on social media has a low expectation of privacy in relation to that information. This assumption is also not in line with the jurisprudence of the European Court of Human Rights ("ECtHR").[7]

[4] The monitoring of social media by law enforcement authorities has long played a significant role in the policing of protests.

[5] New Sections 226A(3)(b)(i) and (ii); 226A(3)(d) and 226A(3)(e).

[6] See for example *Halford v. UK*, App. No. 20605/92, §45 in which the ECtHR underlined that "*a reasonable expectation of privacy is a significant though not necessarily conclusive factor*" in deciding whether there has been an interference with the right to privacy.

[7] See *Peck v. UK* App. No. 44647/98, §§61-62, in which the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras constituted a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. It is notable that this assessment rested on the assumption that the Applicant could not reasonably have expected that his data would be used this way even if their actions were "*already in the public domain*"; see also PI's intervention in *Butt v. UK* App. No. 32946/20, https://privacyinternational.org/legal-action/salman-butt-v-united-kingdom .

7. The retention and examination of social media data within a BPD interferes with an individual's right to privacy. Whether such an approach complies with Article 8 ECHR turns on whether it is in accordance with the law, necessary, and proportionate. *In BBW and others v the UK*, the ECtHR articulated the need for *"'end-to-end safeguards' to provide adequate and effective guarantees against arbitrariness and the risk of abuse*" in the context of bulk surveillance.[8]

8. The proposed low privacy BPD regime lacks such safeguards, lowering the already insufficient protections applied to regular BPDs in the IPA. Among other things, it weakens the judicial authorisation process by allowing an intelligence service to seek 'category authorisations' to retain and examine whole categories of BPDs without further independent authorisation for each BPD obtained (S226BA). Even where individual authorisation is sought for a low privacy BPD, the authorising Judicial Commissioner (JC) is reduced to determining only whether a BPD falls into the low privacy category (S226BB(1)). Section 226BB(2) states that the JC must apply judicial review principles in this assessment. An assessment limited to the question of whether a BPD meets the low privacy definition is too narrow to incorporate judicial review principles, which would for example require considering whether the collection of a BPD is necessary and proportionate. For these reasons, low privacy BPDs do not meet the requirements of Article 8.

Third-party BPDs

9. We are concerned that third-party BPDs could detrimentally impact the right to privacy. The Bill is likely to facilitate the purchase of or direct access to the personal data of unlimited numbers of people from data brokers and other actors.[9]

10. This practice, which is already deployed by public authorities in the US for example[10] is extremely intrusive given the extensive and granular nature of personal data collected by actors such as data brokers. Such data can include an individual's real time location, their IP address, or sensitive information relating to the websites a person visits (such as if they visit a website about the provision of abortion services).[11] Data examined through a third-party BPD warrant can therefore also constitute a serious interference with the right to privacy.

11. It is doubtful whether this provision can meet the in accordance with the law requirement for the purposes of Article 8. We note that the personal information covered by this BPD

[8] *BBW and others v. UK* App. Nos. 58170/13, 62322/14 and 24960/15, §§ 425, 348-364.

[9] See Paragraph 25 of the IPAB's Explanatory Notes: "*Many commercial companies acquire various datasets as part of their own business objectives and offer access to these to a variety of customers. Access to such datasets may offer the intelligence services different capabilities and insights to support them in carrying out their statutory functions*".

[10] For example, the US Immigration and Customs Enforcement bought personal and criminal justice data of individuals without immigration status from data brokers in order to facilitate their deportation - https://www.theguardian.com/us-news/2022/apr/19/us-immigration-agency-data-loophole-information-deportation-targets.

[11] https://privacyinternational.org/long-read/4398/companies-control-our-secret-identities.

may have been processed contrary to the law. Below are two examples of how this may occur:

a. Following our 2018 complaint to the Information Commissioner's Office ("ICO") against the data broker credit reference agency Experian, the ICO issued an enforcement notice to Experian. The ICO found that Experian unlawfully used data it obtained via a number of sources, including the credit reference arm of its business and the Open Electoral Register, to screen, profile, and enhance people's personal data to provide direct marketing services.[12] It found "*widespread and systemic data protection failings across the sector*".[13] On appeal, the First-Tier Tribunal found that the data acquired via open sources had been processed contrary to a number of data protection principles, including transparency, fairness, and lawfulness.[14]

b. There is nothing on the face of the Bill preventing the purchase of hacked and stolen data by the intelligence services under the proposed third-party BPD. During the Second Reading debate in the House of Lords, the government minister referred to hacked and stolen in the context of the low privacy BPDs, but not third-party BPDs.[15]

12. The possibility of unlawfully collected data comprising part or the entirety of a third-party BPD has profound implications for the in accordance with the law requirement as well as public law principles.

13. Furthermore, the scope and manner of exercise of the powers relating to third-party datasets are not set out with sufficient clarity. The intelligence services are already required to follow strict safeguards controlling BPDs' retention, examination, and deletion when no longer necessary. How and if these safeguards would be enforced against the holders of third-party BPDs is not clarified in the IPAB or the Explanatory Notes. Given that the intelligence services themselves have struggled to comply effectively with these safeguards,[16] it seems unlikely they could enforce them consistently with third parties. Relying on third parties to hold BPDs for government access decreases government accountability and increases the risk of arbitrariness.

The notification requirement

14. The notification requirement (proposed new Section 258A as inserted by Clause 20) raises compatibility issues with Article 8 ECHR and the right to an effective remedy enshrined in Article 13 ECHR.

[12] https://privacyinternational.org/frequently-asked-questions/4258/qa-uk-regulators-action-data-brokers.
[13] As above.
[14] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/02/tribunal-rules-on-experian-appeal-against-ico-action/
[15] HL Deb, 20th November 2023, vol. 834, col. 650-1.
[16] https://privacyinternational.org/press-release/5027/press-landmark-ruling-exposes-years-rule-breaking-mi5

15. Notices issued under new Section 258A would require operators to notify the Secretary of State of any proposed 'relevant changes' specified in the notice. Future secondary legislation will set out what 'relevant changes' would require notification. We are concerned about the government's suggested examples of 'relevant changes',[17] which include changes in the capabilities of an operator to provide the intelligence services with communications data and/or content.

16. Information that has 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 and crucial security patches, whose main purpose is to keep devices and data infrastructure secure.[18]

17. The failure to implement critical security updates and changes will impact all users of the service or system in question rendering their data more vulnerable to hacking by third party actors.[19] The exercise of the powers in Clause 20 also lacks prior independent authorisation. Where the interference with privacy is significant and wide-ranging, the ECHR requires a system of prior independent authorisation.[20] This applies to Clause 20 because, while the information in question relates to the operation of services and systems deployed by companies, it has significant implications for the privacy of any individuals whose data is held and processed by that company.

18. We are further concerned that Clauses 17[21] and 20 could be used in tandem to give the government an effective veto over privacy and security updates brought in by companies. There would be nothing preventing the government from requesting information under Clause 20, such as a change in a company's data retention period, before issuing a technical capability, data retention, and/or national security notice once it has the information. Clause 17 could then be used to prevent the company from making the relevant change to the system or service in question while the notice is under review for a potentially indefinite period. This would significantly impact anyone whose data is held by the company who would not benefit from the deletion of their data in the event its retention period is shortened. In the case of data retention, it is unclear what would happen if a decision by the courts or the ICO required a company to shorten its retention period while it was subject to a notice review under Clause 17.

19. Moreover, in respect of the notices regime – a company has recourse to the review procedure. There is no way for a company to challenge a request to provide information and/or not to make a relevant change while the review process is in place. The notification requirement is also subject to an obligation not to disclose the existence of

[17] https://www.gov.uk/government/publications/investigatory-powers-amendment-bill-policy-statement
[18] https://privacyinternational.org/explainer/4635/introduction-software-updates-and-why-they-matter
[19] https://privacyinternational.org/advocacy/5088/pi-response-uk-government-consultation-technical-capabilities-notices
[20] *Big Brother Watch and others v UK* (Applications nos. 58170/13, 62322/14 and 24960/15, 25 May 2021) §42
[21] This creates several amendments that require that operators not to 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.

the notice to anyone (proposed new Section 258(8)). The government has not announced whether (and how) there will be a public accounting by either the Secretary of State or the Investigatory Powers Commissioner concerning the number of notification notices issued in a given period. The failure to extend the double lock, the lack of transparency, and the impossibility of challenging these surveillance measures point to a denial of Articles 13 and 8 ECHR.

(19 January 2024)