Opening the door to abusive US-style surveillance in the UK: Rights & Security International's briefing on the Investigatory Powers (Amendment) Bill

Clauses 2 and 5

There are many aspects of the Investigatory Powers (Amendment) Bill (IPAB) for MPs to be concerned about.[1] However, MPs may not be aware that the government appears to be copying legal language from the US that has given intelligence agencies and police there the power to conduct massive, unaccountable or otherwise abusive surveillance.

The government is doing this in two of the Bill's clauses:

- Clause 2 would remove already minimal safeguards when the UK's intelligence services want to gain access to 'bulk personal datasets' (BPDs) – large collections of data defined by the fact that the majority of the people included in them are not, and never will be, suspected of involvement in a crime.[2] Clause 2 would remove these protections in circumstances in which the government or the security services decide that people have 'low or no reasonable expectation of privacy' and introduce the idea that people can 'consent' to be spied on. Legally, when determining what protections our data should have, this would shift the focus from how sensitive the information is to whether we have literally kept it secret all our lives. If we have not, then police and spies could regard information about our health, sexuality, gender identity, and family relationships as fair game. If facial recognition or mobile location data are included, as they easily could be, then the police could map our every movement.

- Clause 5 would allow the security services to buy access to 'third-party BPDs' held by private companies – which could include any information we have ever entered into a search engine, social media site, online retailer, dating app, web- or chat-based helpline, library catalogue or our phones. It could also include facial recognition data or marketing profiles that tech companies have created of us, covering our every belief, opinion, point of curiosity or purchase (potentially inaccurately). If the government collects this information at a large scale, it could use AI or other tools to engage in predictive policing, a practice that often entails *de facto* racial profiling. Such information would also give police and security agencies the power to compile extensive dossiers about our personal lives, just as the tech companies do. Historical experience shows that governments tend to use such powers to repress minorities, activists and dissidents.

The language in these clauses is so broad that Parliament may not understand what the government is asking it to authorise. With the Bill scheduled to have its Committee Stage on the 7th March 2024 Parliament needs

[1] For a summary, see Rights & Security International, 'Snooper's Charter 2.0: More snooping, fewer safeguards – Rights & Security International's briefing on the Investigatory Powers (Amendment) Bill' (December 2023); Big Brother Watch, Internet Society, Liberty, Open Rights Group, Privacy International and Rights & Security International, 'Joint Briefing on the Investigatory Powers (Amendment Bill): House of Lords, Report Stage' (January 2024); Rights & Security International, 'Snooper's Charter 2.0 leaves trade unions vulnerable to surveillance' (February 2024).

[2] As defined in the Investigatory Powers Act 2016, s199.

to be aware of how laws like these have caused extensive harms in the US, and what they could do in the UK.

We call on the MPs to reject the government's attempt to expand surveillance powers in highly intrusive directions and at a massive scale by removing clauses 2 and 5.

Clause 2: 'Low or no reasonable expectation of privacy'

In the US, police and intelligence agencies can obtain personal data when – under a problematic strand of case law originally concerning technology that is now badly outdated – they believe an individual has 'no reasonable expectation' of privacy (REP) in it. The concept of REP has led to intrusive and at times massive surveillance, and has evolved in an environment of heavily racialised policing and prosecutions as well as a willingness to engage in mass incarceration. By borrowing the REP standard and introducing an unprecedented category of 'low expectation of privacy', clause 2 of the IPAB would give UK security services even broader powers to justify gathering and analysing information about people a massive scale. The US example provides no reason to think that such practices would lead to greater justice or less violence.

Clause 2 of the Bill would introduce the idea that people could have 'low or no reasonable expectation of privacy' in information if they have not literally kept it secret, no matter how sensitive that information is or how easily it could lead to abuse. In essence, the concept shifts blame onto people for disclosing their thoughts, opinions, religious or other beliefs, sexual orientation or tastes, gender identity, race, trade union status, family relationships, health conditions, speculations or points of curiosity to some other person or a tech platform – rather than asking how governments should treat sensitive information in order to protect democracy and equality for everyone, and how prone the information could be to abuse. Under this Bill, if police or security agencies want to access BPD containing data they believe has 'low or no reasonable expectation of privacy', they will be able to avoid the current system for warrant authorisation.

The REP is a concept alien to UK law, as a departure from the Data Protection Act 2018, and also runs contrary to the European Convention on Human Rights.[3]

In the US, courts use the REP standard retrospectively to determine whether a warrantless search by police or intelligence agencies constituted an 'unreasonable search' under the Fourth Amendment to the Constitution. Where a search infringes on an individual's 'reasonable expectation of privacy', this would violate the Fourth Amendment and could lead to the exclusion of evidence from criminal prosecutions; in some circumstances, it could also lead to a lawsuit for damages against the authorities who carried out the search.[4]

The 'reasonable expectation of privacy' standard is highly controversial in the US, having led to massive surveillance and enabled race-based targeting, among other problems.[5] For example, the REP standard was

[3] See App. No. 62357/14, *Benedik v. Slovenia*, Judgment, 24 April 2018, para. 101; App. No. 931/13, *Oy and Oy v. Finland*, Judgment, 27 June 2017, paras. 133-138.

[4] See *Katz v. United States*, 289 U.S. 347 (1967), *Oliver v. United States*, 466 U.S. 170 (1984), *Terry v. Ohio*, 392 U.S. 1 (1968).

[5] See 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; Kami Chavis Simmons, 'Future of the Fourth Amendment: The Problem with Privacy, Poverty and Policing' (2015) 14(2) University of Maryland Law Journal of Race, Religion, Gender and Class 240.

used by the US government to justify some of the mass surveillance programmes originally exposed by Edward Snowden, such as the massive gathering and mining of people's telephone call records.

The REP doctrine does not ask how sensitive the data it is and what the consequences could be of either individual police/intelligence officers or agencies as a whole having access to it. Instead, it asks how the person whom the information concerns handled that information. Such an approach cuts against the Data Protection Act, the European Convention on Human Rights and the EU's GDPR; respect for the latter remains crucial for data flows between the UK and Europe.

Critically, the US Supreme Court decided in 1979 that people did not have a reasonable expectation of privacy in the telephone numbers they dialled because they were necessarily sharing that information with a third party: the telephone company. According to that decision, whenever we share information with a private company, we are 'assum[ing] the risk' that the company will turn over the information to police – for any reason or no reason.[6] In a world in which we use the internet, mobile phones and electronic bank accounts for nearly every aspect of everyday life, this 'third-party doctrine' has the potential to destroy privacy entirely and create a vast power gulf between the government and the governed.

The REP also rests on an assumption that expectations of privacy – for both individuals and society at large – are stable and constant. But this is not the case.[7] Privacy expectations are subjective, and change in response to personal experiences, technological advancements, and social change. For example, most people who send direct messages on WhatsApp, Facebook or X (formerly Twitter) likely do so with the expectation that those messages are private, akin to letters; they probably do not do so with the understanding that police could be grabbing, storing and viewing those messages forever, simply because the messages have passed through a tech company's server. Further, the most empowered groups in society are likely to substitute their own beliefs about what is 'reasonable' or ('private') at the expense of people from other backgrounds. Stuart McDonald MP made a statement gesturing at this problem during the Bill's second reading, asking 'How are potentially very different subjective attitudes to be accounted for?'[8]

Further, the standard of 'low or no reasonable expectation of privacy' that the Bill proposes goes well beyond the standard used in US law. Rather than the 'on-or-off' binary question of whether someone has a REP (which is the question in US law), this Bill would add a vague and undefined category of '**low** expectation of privacy'. There is little or no way to guess what the government thinks this means.

The 'reasonable expectation of privacy' standard conflicts with other legal rights, is not appropriate for the digital age and has led to abuse elsewhere. MPs should remove this clause from the Bill.

Clause 5: Third-party bulk personal datasets

In the US, police can rely on the 'third-party doctrine' (TPD), or controversial notions of 'consent', to grab and store information that people transmit via tech companies. For the reasons outlined above, this doctrine is not appropriate to the digital age – potentially meaning that almost no digitised information is private – and cuts against the Data Protection Act, the European Convention on Human Rights and the EU's GDPR. Clause 5 of the IPAB would bring this reality-defying and mass-surveillance-enabling doctrine into UK law.

[6] *Smith v. Maryland*, 442 U.S. 735 (1979).
[7] See Justice Scalia's opinion in *United States v. Jones* 615 F.3d 544 (2012).
[8] Hansard, Investigatory Powers (Amendment) Bill [Lords], Monday 19 March 2024, Volume 745, Col. 533.

The Fourth Amendment to the US Constitution protects the right to be free from unreasonable searches and seizures of property. However, in its controversial decision in *Smith v Maryland*, the US Supreme Court adopted the 'third-party doctrine', allowing police to gain access without a warrant to nearly any information that someone has (supposedly voluntarily) shared with a private company.[9] In the digital age, this doctrine creates a mess, leaving courts to grapple with – for example – we are voluntarily sharing our location whenever we carry a mobile phone.[10] (The US Supreme Court has found that the third-party doctrine does not apply to certain kinds of mobile phone location data, but questions remain about other location data generated by our phones or apps.) Potentially, any data a person generates when they sign up for a dating app, unlock a phone or using facial recognition, carry out a Google search, use a video doorbell, or even use a credit or debit card at a shop, would be fair game for warrantless police access under this doctrine.[11] The US notion of 'consent' could also make any facial recognition data gathered in public fair game.

The problems are not hypothetical: for example, the US National Security Agency initially justified its bulk collection of Americans' telephone records – revealed by Edward Snowden – by pointing to the TPD.[12] The US Drug Enforcement Administration have used the doctrine to argue in favour of warrantless bulk access to information about the medications doctors prescribe.

The UK government, in proposing clause 5, apparently aims to create similar powers here. It wants to allow police and security services to demand access to massive amounts of data held by a third party such as a tech company. The clause specifically covers health data, other sensitive personal data, and what it describes as 'contentious' data use – but it does not provide any additional safeguards to prevent misuse of this data.[13] The government's recognition that it intends to engage in the potentially 'contentious' or controversial collection and processing of our data is particularly troubling.

The government may claim that there is one key distinction between the US approach and the one proposed in clause 5 of the Bill: the UK would require the formality of the government's issuance of a warrant and the brief review of a judicial commissioner. However, such a claim would be misguided – the toothless nature of the proposed safeguards would do little to kerb potential harms under clause 5.[14] Additionally, since few people (or potentially no one) would ever find out that the government had gathered their data this way,

---

[9] Generally, see *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979); *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

[10] Among others, see *United States v. Graham*, 824 F.3d 421, pp. 437-438 (4th Cir. 2016); *United States v. Wheelock*, 772 F.3d 825, p. 829 (8th Cir. 2014); *New York v. Thompson*, 28 N.Y.S.3d 237, pp. 250-251 (N.Y. 2016); *Apodaca v. N.M. Adult Prob. And Parole*, 998 F. Supp. 2d 1160, p. 1180 (D.N.M. 2014); *United States v. Jones*, 565 U.S. 400, p. 417 (2012).

[11] On online services generally, see *United States v. Davis*, 785 F.3d 498, pp. 535-536 (11th Cir. 2015); on online dating services and social media profiles, see *R.S. ex rel S.S. v. Minnewaska Area School District No. 2149*, 894 F. Supp. 2d. 1228 (D. Minn. 2012); on location data, see *Carpenter v. United States*, 138 S. Ct. 2206 (2018); on 'smart home' technology, see Brandon Pieratt, 'Alexa, Give My Personal Information to the Government: The Application of the Third-Party Doctrine to Smart Devices' (2018) 21 SMU Science & Technology Law Review 291, pp. 291-292; and on card payments, see *United States v. De L'Isle*, 825 F.3d 426 (8th Cir. 2016).

[12] *In Re Application of the Federal Bureau of Investigation for an order requiring the production of tangible things from [redacted]*, Foreign Intelligence Service Court, Docket Number: BR 13-109.

[13] Clause 5 proposes a new s226G for the Investigatory Powers Act 2016. See s226G(7) for these examples; s226G(3) only requires the requesting body to flag this fact to the Secretary of State.

[14] Rights & Security International, 'Snooper's Charter 2.0: More snooping, fewer safeguards – Rights & Security International's briefing on the Investigatory Powers (Reform) Bill' (December 2023): https://www.rightsandsecurity.org/assets/downloads/RSI_IPA_reform_brief.pdf.

the government-issued warrant would seldom or never be subject to the safeguard of a human rights challenge in court.

Clause 5 is an invitation for the government to purchase or demand vast quantities of sensitive information about people in the UK. This would be an abuse in itself and could easily facilitate other abuses, as the US experience demonstrates. Parliament should demand the removal of the clause.

About 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.