Snooper's Charter 2.0: More snooping, fewer safeguards

Rights & Security International's briefing on the Investigatory Powers (Amendment) Bill

The Investigatory Powers (Amendment) Bill

Through the Investigatory Powers (Amendment) Bill, the government plans to water down the already weak safeguards meant to protect us against the security services when they could abuse our personal information. With the government seemingly intent on rushing this harmful legislation through Parliament, Rights & Security International (RSI) provides a brief overview of the (il)legality of these proposals below.

The Bill would relax the Investigatory Powers Act 2016 (IPA) – a law that already gives such broad powers to the government that many call it the 'Snooper's Charter'. Among other things, the government seeks to:

- Remove safeguards when the intelligence services want to access a 'bulk personal dataset' (BPD) – a large collection of data defined by the fact that the majority of the people included are not, and never will be, subject to a security services investigation[1] -– when it thinks they have 'low or no reasonable expectation of privacy' **(Clause 2)**;
- Double the length of time that BPD warrants can authorise the intelligence services to use the data **(Clause 3)**;
- Allow the intelligence services to intercept our communications under the theory that they are not truly private **(Clause 11(3))**; and
- Allow the security services to carry out speculative surveillance by snooping on our internet connection records – data that tells the security services who connected to the internet, where, and when – in ways that far exceed the authorisation Parliament originally gave when passing the IPA **(Clause 14)**.[2]

While RSI holds specific concerns about each of these clauses, they all suffer from three fundamental flaws that mean they may violate the European Convention on Human Rights (ECHR):

1. The government has ignored well documented failures in the way the security services hold surveillance data, instead deciding to reduce the already weak safeguards that prevent them from using our data unlawfully;
2. The government's legal analysis relies on some people losing their privacy because they do not have a 'reasonable expectation of privacy' – a legal concept that the European Court of Human Rights has rejected; and
3. The government has not explained why these interferences with our privacy are necessary, as opposed to merely 'convenient'.

In a democracy, privacy is essential: if the government can spy on people any time it likes, then it will be far too powerful and dissent will become impossible. Surveillance causes clear risks for rights, yet the government has decided not to conduct a Privacy Impact Assessment of its proposed reforms.[3] Instead of considering the risks to our privacy and therefore to democracy in the UK, it is trying to rush through

[1] As defined in the Investigatory Powers Act 2016, s199.
[2] UK Government, 'Operational Case for the Retention of Internet Connection Records' (2016), p. 13.
[3] Home Office, 'Impact Assessment: Investigatory Powers (Amendment) Bill 2023', IA No. HO0476 (7 November 2023, p. 28

legislation that could lead to significant harms. This sets the UK up for another lengthy court battle over its surveillance regime.

Rather than rushing its reforms through Parliament with little scrutiny, the government should drop the Bill. It should then reform the IPA as a whole and otherwise ensure that all surveillance respects our rights.

Watering down already weak safeguards

Currently, security services that want to request surveillance warrants must first go to the Home Secretary for a decision. This decision is reviewed by a Judicial Commissioner.[4]

This system of review is already weak and may violate the European Convention, since the Home Secretary is not independent from the security services and since the Judicial Commissioner cannot assess the warrant on its merits. It also does not stop the security services from holding our data illegally, as the Investigatory Powers Commissioner concluded in relation to the Secret Intelligence Service.[5] Yet, the security services have been applying for more warrants every year.[6] The removal of some of the few safeguards that exist in the IPA would create a real risk of 'data hoarding', allowing the security services to create secret files on anyone and everyone.

Rather than addressing the IPA's shortcomings, the government has decided to water down what few safeguards there are.

'Reasonable expectation of privacy'

By introducing clause 2, the government seeks to introduce a new category of data in which they say people have 'low or no reasonable expectation of privacy'. If the security services want access to such data through bulk personal datasets, they will be able to avoid even the existing flawed system for warrant authorisation. Further, in clause 11(3), the government also seeks to grant the security services the power to access what it calls public or semi-public communications, such as people's direct messages on social media or communications on virtual message boards.[7] Both these proposals are based on the idea that people do not have a 'reasonable expectation of privacy' when they make some aspects of their lives public. In the US, 'reasonable expectation of privacy' has led to massive surveillance and enabled race-based targeting, among other problems.

Clauses 2 and 11(3) are based on the legal misunderstanding that people lose their right to respect for private life when they happen to share certain information with someone else. The European Court has rejected those legal ideas, and has held that we can still have privacy rights even if we do not keep something in total secrecy.[8]

[4] Investigatory Powers Act 2016, ss15-43.
[5] Investigatory Powers Commissioner's Office and Office for Communications Data Authorisations, 'Annual Report of the Investigatory Powers Commissioner 2021', HC 910, 20 March 2023, paras. 9.2-9.4.
[6] Home Office, 'Post Implementation Review: Investigatory Powers Act 2016 (IPA 2016)', PIR No. HO PIR0004 (28 April 2023), pp. 6-8
[7] See the definition of 'publish' in s11(3B), as proposed in clause 11(3).
[8] 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

To the contrary, the Court has repeatedly said that privacy includes 'the right to establish and develop relationships with other human beings'.[9]

These interferences with our privacy are not necessary

Under the European Convention on Human Rights, the UK government must ensure that everything it does, including in the name of national security, complies with human rights laws. This means it must make sure that any time it interferes with the privacy of people in the UK, it obeys the law, has a legitimate goal and only does what is truly necessary to achieving that goal.

The European Court has said clearly that efficiency and convenience are not the same as necessity.[10] But the government's justification for this Bill – and for its individual provisions – is efficiency. For instance, it has argued that the security services will encounter 'inefficiencies' when using machine learning and artificial intelligence without this new law.[11] In other words, the current system does not prevent the security services from accessing the data they need to do their jobs.

The government must explain why the security services need these powers with reduced safeguards in order to protect national security. Without an explanation, Parliament must stop the Bill.

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.

[9] E.g. *Oy and Oy v Finland*, *supra*, para. 133.

[10] See, 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. For a summary, see European Court of Human Rights, 'Guide on Article 8 of the European Convention on Human Rights: Right to respect for private and family life, home and correspondence' (31 August 2022), paras. 612-631.

[11] Home Office, 'Post Implementation Review: Investigatory Powers Act 2016 (IPA 2016)', PIR No. HO PIR0004 (28 April 2023), pp. 14-15