INVESTIGATORY POWERS BILL

HOW TO MAKE IT FIT-FOR-PURPOSE

A BRIEFING FOR THE HOUSE OF LORDS
BY THE DON'T SPY ON US COALITION

CONTENTS

1. INTRODUCTION

The Don't Spy on Us (DSOU) coalition agrees with the Government, law enforcement agencies and secret services that a major reform of the UK's surveillance laws is required. In 2014, The Government's Reviewer of Terrorism Legislation described the current system as "undemocratic, unnecessary and – in the long run – intolerable." [1] The Investigatory Powers Bill (IP Bill) brings together many of the powers that law enforcement and the intelligence agencies can use to obtain communications and communications data into one piece of legislation. However, as drafted, it perpetuates rather than remedies these flaws.

The draft Bill was scrutinised by a Joint Committee, the Intelligence and Security Committee (ISC) and the Science and Technology Committee, who between them heard evidence from a range of experts, including representatives from the technology industry, civil liberties organisations, charities, the police, the Home Office and the security services. In total, these three reports made 123 recommendations.

During the House of Commons Committee stage, the Bill was amended. But many of the recommendations raised by the committees and by MPs have not been addressed. This is of grave concern; the IP Bill is a comprehensive law with far reaching consequences for UK citizens and individuals across the world. It needs full and proper scrutiny.

Despite the Government's claims to the contrary, the IP Bill does extend surveillance powers. Over 30 submissions to the Joint Committee make the case that the Bill expands the powers of the agencies in important ways, including proposals that would record the Internet browsing activity of UK citizens.

This report aims to give Peers a clear summary of the risks and threats posed by the IP Bill, based on the committees' reports and the evidence submitted to them. We also identify where the Bill should be amended further to make sure the UK has a surveillance law fit for a democracy, not an authoritarian state. If you would like to discuss specific amendments with a representative of the Don't Spy on Us coalition, please contact Pam Cowburn at, pam@dontspyonus.org.uk, 07749 785 932.

2. ABOUT DON'T SPY ON US

Don't Spy on Us is a coalition of the most influential organisations that defend privacy, free expression and digital rights in the UK and in Europe. Visit dontspyonus.org.uk to find out more. You can also contact Pam Cowburn at pam@dontspyonus.org.uk, 07749 785 932, if you would like to meet with members of the DSOU coalition to discuss how the Bill can be improved.

3. THE BILL FAILS TO INTRODUCE INDEPENDENT JUDICIAL AUTHORISATION

When presenting the draft Bill to Parliament, Theresa May said it would give the UK, "one of the strongest authorisation regimes anywhere in the world."[2] The so-called "double lock" of warrants being authorised by both the Secretary of State and a Judicial Commissioner is one of the most misleading aspects of the Bill. Although amendments were made by the House of Commons to improve the authorisation process, further work is needed to ensure that judicial commissioners authorise rather than merely review Ministers' decisions. If the UK wants to be able to claim its surveillance legislation is world-leading, it must at the very least adopt a real double lock of ministerial and independent judicial authorisation.

3.1 WHAT PEERS NEED TO KNOW

- The UK is alone among its democratic allies in permitting political authorisation for surveillance. In America, Australia, Canada and New Zealand, judicial authorisation is required for the use of intrusive surveillance methods.
- The authorisation system laid out in the Bill is wholly inadequate for the UK to fulfill its human rights obligations and to provide a world leading oversight regime.
- Judicial Commissioners would not be able to challenge surveillance decisions and come to their own conclusion as to whether a warrant should be granted Judicial Commissioners lack the opportunity to question the requesting agency; to probe as to whether less intrusive methods could be deployed; or to ask for further material to justify the request.
- Independent judicial authorisation could mean better cooperation from US tech firms, who have expressed unease with our political authorisation process.

- The Joint Committee called for independent judicial appointments rather than appointment by the Prime Minister, which undermines the perception of independence. IPC and Judicial Commissioners should be appointed independently, ideally by the Judicial Appointments Commission as is the norm for judicial appointments.
- The Bill proposes that Judicial Commissioners take responsibility for both the (limited) authorisation of warrants for investigatory powers, and for the oversight of the exercise of those investigatory powers. The Joint Committee report into the IP Bill noted that this proposal has been "heavily criticised by many of our witnesses".[3] The functions should be formally distinct, with judges tasked with authorising warrants, and a new body established to unify and fulfil the oversight role.
- The introduction of the flawed judicial authorisation is not applied consistently to powers across the Bill. Judges do not need to sign off warrants for the acquisition of communications data such as call records and internet histories. The police and public bodies, such as HMRC, can sign off warrants internally without the involvement of judges.

Recommendation: The IP Bill should be amended throughout to ensure that Judicial Commissioners do not just have the powers to review Ministers' decisions but are tasked with making a substantive decision as to whether a warrant is merited. The Bill should be amended so that judicial authorisation is applied consistently across surveillance powers.

4. INTERNET CONNECTION RECORDS THREATEN OUR PRIVACY, FREE SPEECH AND SECURITY

The IP Bill will compel Internet Service Providers to retain their customers' data for 12 months. ISPs are already obliged to retain some data by the Data Retention and Investigatory Powers Act (DRIPA). The IP Bill will extend this to include Internet Connection Records (ICRs). The technology sector and civil society have criticised the vague definition of ICRs presented in the Bill, which could be open to interpretation. Despite this lack of clarity, ICRs are generally understood to mean that UK Internet users' web browsing history and app use will be recorded.

The indiscriminate generation and retention of the population's Internet Connection Records is not only an unprecedented violation of privacy, it will have a chilling effect on freedom of expression.

4.1 WHAT PEERS NEED TO KNOW:

The operational case has not been made for ICRs: David Anderson in his report A Question of Trust, which formed the basis for the current review of surveillance legislation, asked for a "compelling operational case" for the retention of third party data.[4] No such case has been presented, with instead two limited anecdotes relating to serious crime presented.

- Alistair Carmichael, MP (Liberal Democrats) told the House of Commons: "David Anderson QC described the expanded data collection by internet service providers as "overstated and misunderstood"—to the point and understated. There is no other "Five Eyes" country in which operators have been forced, or are being forced, to retain similar internet connection data. That surely tells us all that we need to know. The case has not been made. It is always open to the Government to come back on some future occasion to make a case and to put these provisions in another Bill. They have not made the case, and the provisions should not be in this Bill." [5]
- ICRs are not the same as telephone records. As the Joint Committee noted: "We do not believe that ICRs are the equivalent of an itemised telephone bill. However well-intentioned, this comparison is not a helpful one."[6]
- ICRs could damage the UK technology sector: the Science and Technology Committee stated that the lack of definition around ICRs could seriously harm British businesses and the competitiveness of the UK.

- The technology industry does not agree with the Government's estimated costs of £174.2 million over ten years for ICRs: The Internet Service Providers Association explained that the figure is one that they "do not recognise".[7] BT stated that, in their view, the costs are likely to be "significantly more than the cost estimates we have seen to date from the Government."[8] After detailed scrutiny, the Joint Committee concluded that they are "not able to make an assessment of the data retention costs provided by Government."[9] Similar proposals by the Danish Government were dropped on costs grounds. Based on their independent evaluation, ICRs could cost the UK over £1 billion to implement.[10]

Recommendation: DSOU is calling for the removal of the powers to collect Internet Connection Records from Part 4 of the Bill.

5. THE REQUEST FILTER WOULD ALLOW UNAUTHORISED INTRUSION INTO PERSONAL DATA

The IP Bill includes proposals for a "Request Filter", which will allow law enforcement agencies and government departments to access communications data including our web browsing history. The Request Filter is described by the Home Office as a safeguard designed to reduce the intrusion produced in searching for small, specific information in a large dataset.

In reality, the Request Filter would allow automated complex searches across the retained data from all telecommunications operators without any judicial authorisation at all.

5.1 WHAT PEERS NEED TO KNOW:

- The Request Filter brings huge privacy risks. Even the Food Standards Agency will be able to self-authorise itself to cross reference UK citizens' Internet history with mobile phone location and landline phone calls — and search and compare millions of other people's records too.

Recommendation: The Request Filter should be removed from Part 3 of the Bill.

6. HACKING POWERS WILL THREATEN THE SECURITY OF THE INTERNET

The IP Bill will allow law enforcement and intelligence agencies to carry out targeted equipment interference (EI). More commonly understood as hacking, this would allow devices such as mobile phones or computers to be accessed in order to acquire the data they hold. This includes the devices of people who are not under suspicion. The intelligence agencies will also be given powers to carry out non-targeted mass hacking of networks and devices.

6.1 WHAT PEERS NEED TO KNOW

- Internet security could be undermined by hacking, with serious security implications for individuals and companies who may not be suspected of any crimes. Internet companies could be forced to hack their customers. There are widespread concerns over requirements for companies to collaborate with intelligence agencies or police in the hacking of their targets. For example they could be forced to send out software updates that contain 'malware', which will infect phones or laptops to allow them to be accessed.
- Companies are worried about the damage to their customers' trust. The Bill undermines consumer trust by forcing companies to spy on their users instead.
- As Vodafone put it, "turning network operator employees into spies and hackers is manifestly inappropriate."[11] Silicon Valley tech companies felt the requirements that could be imposed in the Bill "represent a step in the wrong direction" and that aspects of the Bill which would force companies to make their systems more vulnerable would damage that trust and is "a very dangerous precedent to set."[12]

Recommendation: Part 5 should be amended so that companies are not forced to hack their customers or change the way they operate. Equipment interference should be limited to what is strictly necessary and authorised by a proper "double lock".

7. BULK POWERS HAVE NOT BEEN JUSTIFIED

The Bill enshrines in legislation for the first time the use of many bulk surveillance powers, which constitute an unnecessary and disproportionate human rights violation. The Joint Committee pointed out the lack of justification for bulk powers: "Although the majority of witnesses queried the justification for bulk powers, they, like the Committee, were inevitably commenting on the basis of incomplete information."[13] The Government has produced no evidence to show that the powers keep us any safer, and in fact evidence is increasingly suggesting that they make it harder for the security and intelligence agencies to do their jobs properly.[14]

The Committee recommended that the Government, "should publish a fuller justification for each of the bulk powers alongside the Bill. We further recommend that the examples of the value of the bulk powers provided should be assessed by an independent body, such as the Intelligence and Security Committee or the Interception of Communications Commissioner."[15]

At the request of the Opposition in the House of Commons, David Anderson QC is leading a review into bulk powers, which will report in September. The House of Lords will have the opportunity to debate and amend the bulk powers outlined in the IP Bill.

ENDNOTES

1 Independent Reviewer of Terrorism Legislation, A Question of Trust – Report of the Investigatory Powers Review, June 2015 para 35 bit.ly/1WLue5n

2 https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill

3 Joint Committee on the Draft Investigatory Powers Bill Report p149 bit.ly/1QAgdmo

4 A Question of Trust p5

5 HC Hansard, 7 June 2016, col 1135.

6 Joint Committee report p8

7 Science and Technology Committee, Investigatory Powers Bill: technology issues bit.ly/1TB5EEK p24

8 Written evidence submitted to the Joint Committee on the Draft Investigatory Powers Bill p204 bit.ly/1QHKlm2

9 Joint Committee report p10

10 https://www.dontspyonus.org.uk/blog/2016/03/30/'snoopers'-charter'-could-hit-police-forces-with-£1-billion-bill/

11 Written evidence submitted to the Joint Committee on the Draft Investigatory Powers Bill p1138 bit.ly/1QHKlm2

12 Written evidence submitted to the Joint Committee p391

13 Joint Committee report p88

14 https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/

15 Joint Committee report p9

DONTSPYONUS.ORG.UK