INVESTIGATORY POWERS BILL

HOW TO MAKE IT FIT-FOR-PURPOSE

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 are required. The draft Investigatory Powers Bill (IPB), published on November 5, 2015, purported to bring together all of the powers that law enforcement and the intelligence agencies can use to obtain communications and communications data into one piece of legislation.

To date, it has been scrutinised by a Joint Committee, the Intelligence and Security Committee (ISC) and the Science and Technology Committee, who between them have heard evidence from a range of experts, including representatives from the tech industry, civil liberties organisations, charities, the police, the Home Office and the security services.

In total, the three reports made 123 recommendations. The overall message is clear: the draft IPB needs to be completely rewritten if it is to become the comprehensive and clear legislation we need to regulate and oversee surveillance in the UK. We understand that a revised draft of the Bill will be published in the first week of March – less than three weeks after the Joint Committee reported its findings.

We are gravely concerned that the significant flaws within the Bill will not have been addressed.

This report aims to give MPs and Peers a clear summary of the risks and threats posed by the draft IPB, based on the committees' reports and the evidence submitted to them. We hope that it will help Parliamentarians judge whether these issues have been satisfactorily resolved in the revised Bill. DSOU invites MPs and Peers to contact us if they would like face-to-face or more detailed written briefings after the revised Bill has been published.

1.1 WHY THE RUSH?

We understand the Government's desire to pass the Investigatory Powers Bill before December 2016 when the Data Retention and Investigatory Powers Act (DRIPA) sunset clause expires. We believe that the best way to address this would be to split the Bill. The data retention powers that are affected by the imminent sunset clause could be published as a stand alone Bill and dealt with in the relevant timeframe. This would enable full consideration to be given to the committees' recommendations and scrutiny of the remaining powers.

1.2 THE NEED FOR A PUBLIC AND PARLIAMENTARY DEBATE

Whatever our personal views of Edward Snowden, his actions have ignited a long overdue public debate. Mass surveillance capabilities, built without the knowledge of Parliament, have been acknowledged, leading to three independent inquiries into the investigatory powers of the UK's law enforcement and security services. Each inquiry called for comprehensive legal reform, resulting in the draft IPB.

This chain of events explains some of the key flaws in the IPB. The law has been drafted in part to give legitimacy to programmes and practices that already exist – programmes that were built without parliamentary debate or assent.

Investigatory powers should not be passed into law simply because vast amounts of taxpayers' money has already been spent building extensive programmes. The criticisms of the IPB show that we need to go back to basics and have a proper debate about whether bulk surveillance powers are acceptable in a democracy such as the UK. As the ISC report stated, *"privacy protections should form the backbone of the draft legislation, around which the exceptional powers are then built".*[1]

2. THE DRAFT BILL FAILS IN ITS MISSION TO BE CLEAR AND COMPREHENSIVE

The draft Bill fails in its mission to be clear and to bring all investigatory powers together into one Bill. Dominic Grieve QC, Chair of the Intelligence and Security Committee said: *"the various powers and authorisations remain scattered throughout different pieces of legislation and, as a result, the draft Bill is limited in the extent to which it can provide a comprehensive legal framework. In our view this is a missed opportunity."* [2]

2.1 WHAT PARLIAMENTARIANS NEED TO KNOW

- The majority of submissions to the Joint Committee, from a broad sphere of experts, raised concerns about the lack of clarity within the Bill. This was reflected in the Committee's report which repeatedly asked for more clarity – the words "clarity" or "clear" appear 143 times. According to the ISC, the Bill is misleading in the presentation of some of its powers. Vague and obscure powers are undemocratic and should not be passed.
- The ISC report said: *"The provisions in relation to three of the key Agency capabilities – Equipment Interference, Bulk Personal Datasets and Communications Data – are too broad and lack sufficient clarity."* [3]

- The intelligence agencies will still use very broad statutory powers defined in the Security Service Act 1989 and the Intelligence Services Act 1994 to acquire and use data – for example bulk personal datasets. The wording of these powers is very broad: *"that there are arrangements for securing that no information is obtained by the (Service) except so far as necessary for the proper discharge of its functions or disclosed by it except so far as necessary for that purpose"*. [4]
- Despite the Government's assurances to the contrary, the draft 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 subtle but important ways, including proposals that would record the Internet browsing activity of UK citizens.
- The Bill was presented as a comprehensive reform of surveillance, yet one of the most controversial practices, covert human surveillance currently regulated by Part 2 of RIPA, is not included. The ongoing scandals about the behaviour of the police officers infiltrating political groups have led to a major Inquiry into undercover policing, chaired by Lord Justice Pitchford. While it would be difficult to provide for full reform while the Inquiry is in place, there should be at least some consideration for how all forms of surveillance will have to be brought under a common framework. Current authorisation and oversight procedures have completely failed to stop abuses such as the fathering and abandonment of children. Neither did the Bill encompass all the equipment interference or hacking methods used, which would continue under existing legislation
- The draft Bill failed to address international bulk data sharing – one of the most controversial practices uncovered by the Snowden revelations. The ISC remarked that *"the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception"*. [5]
- Any evidence that is gathered through the interception of communications cannot be used in UK courts. It has been argued that doing so would reveal the techniques being used and could therefore jeopardise future operations. Given the increase in transparency over the Government's surveillance powers, this argument no longer applies. Intercept evidence is used in many other countries – including all other Five Eyes countries – Australia, Canada, New Zealand and the U.S.
- The Bill fails to protect privileged communications. Article 19 told the Joint Committee: *"Clause 61 of the draft Bill fails adequately to protect the confidentiality of journalistic sources (including those of non-governmental organisations) and provides no protection whatsoever to a person's confidential communications with doctors and ministers of religion, or the privileged communications of MPs and lawyers."* [6]
- The Bill allows the Secretary of State to issue National Security Notices (NSNs), which are described in such general terms that could encompass asking telecommunications providers anything and everything. Similarly vague and general provisions in the Telecommunications Act 1984 have been secretly used for years by agencies to collect the phone records of the whole country in bulk. The Bill should put an end to ambiguous interpretations of the law and make sure that the revised Bill restricts NSNs to emergencies.

- Judicial authorisation should be required for any National Security Notice to support the intelligence services.
- Post-Snowden, there has been consensus that more transparency is needed about the state's surveillance powers. Despite this, there are several new criminal offences for disclosure, including for private sector employees who may be forced into complicity with state hacking or spying demands.

3. THE OPERATIONAL CASE HAS NOT BEEN MADE FOR ALL POWERS

The Home Office has provided some evidence in attempt to support the extension of powers in the draft Bill for recording Internet browsing history through the collection of Internet Connection Records (ICRs). But it has failed to provide comprehensive evidence for the operational need for many of the powers in the Bill.

3.1 WHAT PARLIAMENTARIANS NEED TO KNOW:

- 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. [7] No such case has been presented, with instead two limited anecdotes relating to serious crime presented.
- Bulk powers: 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."* [8] 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."* [9]
- Bulk personal datasets: The Joint Committee recommended that the Home Office produce a case for bulk personal datasets and that, *"the lack of that detail makes it hard for Parliament to give the power sufficient scrutiny"*. [10]

4. INTERNET CONNECTION RECORDS ARE ILL-DEFINED AND INTRUSIVE

Written submissions to the Joint Committee have raised concerns about proposals to record UK citizens' Internet history through the collection of Internet Connection Records (ICRs). These include privacy and free speech concerns about the unprecedented step of recording web histories, to the security risks of storing such personal data.

4.1 WHAT PARLIAMENTARIANS NEED TO KNOW:

- 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."* [11]
- ICRs are not clearly or consistently defined in the draft Bill: When asked to rate the clarity of definitions contained in the Bill, on a scale of one to ten, Adam Kinsley of Sky told the Joint Committee that the definition of ICRs was, *"pretty close to zero"*. [12] Many ISPs agreed. The Joint Committee recommended: *"that the definition of Internet Connection Records should be made consistent throughout the Bill and that the Government should give consideration to defining terms such as 'internet service' and 'internet communications service'. We recommend that more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level."* [13]
- ICRs could damage the UK the sector: The Science and Technology Committee stated that this lack of definition could seriously harm British businesses and the competitiveness of the UK.
- If the UK begins collecting Internet Connection Records, it will be the only country in the world to have a policy of capturing and recording every citizen's Internet use.
- The tech industry does not agree with the Government's estimated costs of £174.2 million over 10 years for ICRs. The Internet Service Providers Association explained that the figure is one that they *"do not recognise"*. [14] 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."* [15] After detailed scrutiny, the Joint Committee concluded that they are *"not able to make an assessment of the data retention costs provided by Government."* [16]
- The indiscriminate generation and retention of the population's Internet Connection Records is not only an unprecedented mass violation of privacy, it would have a chilling effect on freedom of expression.

5. BULK PERSONAL DATASETS (BPDS) ARE INTRUSIVE AND LACK SUFFICIENT SAFEGUARDS

Former Director of GCHQ Iain Lobban told the Telegraph, *"Who has the info on you? It's the commercial companies, not us, who know everything."* [17] With Bulk Personal Datasets, intelligence agencies are forcing numerous commercial companies to hand over everything they know, in bulk, to allow the agencies to combining the knowledge of multiple commercial companies in a single place.

Under the draft Bill, the intelligence agencies would be able to get copies of entire 'bulk personal datasets' held by private and public organisations. The examples given in evidence were the electoral roll or the telephone directory but the contents and scope of bulk personal databases are unlimited in the draft Bill.

5.1 WHAT PARLIAMENTARIANS NEED TO KNOW

- The Joint Committee said that the operational case for BPDs had not been made: *"the lack of that detail makes it hard for Parliament to give the power sufficient scrutiny."* [18]
- The majority of individuals whose data will be in a BPD are not under suspicion or of interest to the agencies, but the data is routinely analysed regardless.
- The draft Bill would allow the agencies to use class BPD warrants to get multiple datasets that fall into a category, such as 'travel'. In their reports, both the Intelligence and Security Committee and the Joint Committee called for the removal of these class warrants from the Bill.
- The ISC noted that a loophole in the Bill means that theoretically: *"an Agency could hold a BPD without authorisation indefinitely."* [19]
- There has been no clarification about whether sensitive data, such as health records, can be accessed.
- The Joint Committee has also raised concerns that: *"The safeguards for BPDs are not sufficiently explained in the Bill."* [20]

6. THE DRAFT BILL WOULD PUT UK INDUSTRY AT RISK

This draft Bill is bad for business, and in the words of Gigaclear, *"a massive own goal"*.[21] By putting in place high compliance costs, a proposed legal framework that lacks clarity, and forcing companies to spy on their users, this draft Bill will damage industry. The Science and Technology Committee concluded that in its present form, the Bill could undermine the UK tech sector.

6.1 WHAT PARLIAMENTARIANS NEED TO KNOW

- Companies could be forced to change their business models: TechUK explained to the Science & Technology Committee that *"the Government reserves the right to compel companies to change their business models in order to facilitate access to data that they would not have kept under standard business operations"*.[22] These provisions are broad in scope, and can be imposed at any time, placing companies in a position of significant uncertainty and affecting how well they are able to protect their customers.
- The draft Bill could undermine innovation: New powers in the draft Bill could prevent companies from building technologies in the way they want, harming their independence and innovation. Vodafone stated that the Equipment Interference power in the draft Bill amounts to a *"major imposition on the freedom of an operator to design and operate its services in the way it sees fit"*.[23]
- Internet security could be undermined: Strong encryption is the cornerstone of British cyber-security. Encryption protects billions of people every day against threats that include criminals trying to steal our phones and laptops, cyber criminals trying to defraud us and foreign intelligence agencies targeting companies' valuable trade secrets. Several submissions to the Joint Committee pointed out that the draft Bill could be open to interpretation when it comes to encryption. The Committee recommended: *"The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide decrypted copies of those communications if it is not practicable for them to do so."* [24]
- Companies are worried about the damage to their customers' trust: The draft Bill undermines consumer trust by forcing companies to instead spy on their users. As Vodafone put it, *"turning network operator employees into spies and hackers is manifestly inappropriate."*[25] Silicon Valley tech companies felt the requirements that could be imposed in the draft 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."* [26]
- There are widespread concerns over requirements for companies to collaborate with intelligence agencies or police in the hacking of their targets.

7. THE BILL'S IMPACT WILL BE FELT AROUND THE WORLD

Touted as a gold standard for surveillance legislation when introduced, this Bill contains some of the most intrusive surveillance powers anywhere in the world. It will damage civil liberties globally as other countries follow suit, and cause chaos for companies as claims of extraterritorial jurisdiction create conflicts of law. Britain should be leading the world; but leading in the promotion of democratic values and human rights, not in surveillance that is the envy of the world's despots.

7.1 WHAT PARLIAMENTARIANS NEED TO KNOW:

- The Bill will be copied by authoritarian regimes: TechUK say that *"many governments – often in countries with immature democratic and human rights standards – are eagerly awaiting the Investigatory Powers Bill and have plans to propose similar laws."* [27] China has already said it took inspiration for its surveillance measures from the the US and UK. Its recently passed anti-terror law, which was heavily criticised by the international community, bears marked similarities to the draft Investigatory Powers Bill.
- No other country has legislated for bulk equipment interference: Some powers in the draft Bill, such as Bulk Equipment Interference, are so dangerous they *"threaten the security of the Internet"* according to TechUK. [28]
- Vodafone believes that if passed, the Bill *"will have material repercussions in the global marketplace for communications services, making a UK-based provider a less attractive option than a provider domiciled in a country which does not have such a framework."* [29]
- Extraterritorial powers: The draft Bill is littered with unilateral assertions of extraterritorial jurisdiction. A patchwork of overlapping and conflicting laws around the world, enforced by the domestic legislation of multiple countries all claiming extraterritorial powers could cause havoc. Companies have warned that if passed, other countries will follow suit, placing them in impossible positions.
- The London Internet Exchange (LINX) said that this position *"will rob the United Kingdom of a principled basis for dissuading or criticising foreign governments from following this precedent, and will indeed encourage such behaviour. This will diminish British sovereignty, and place the interests of British businesses and the liberty of their personnel in jeopardy, as countries with legal standards and traditions very different to our own seek to assert their own laws."*[30]
- The Joint Committee recommended that the *"Government should give more careful consideration to the consequences of enforcing extraterritoriality."*[31] The Intelligence and Security Committee concluded that it is *"disappointed that the Government has not done more to make progress on this crucial issue."*[32]

- Loopholes in the draft Bill would permit the warrantless interception of UK citizens. The Bill fails to address the necessary arrangements and constraints for highly controversial international data sharing – a method by which a significant amount of intelligence is acquired. As the ISC report emphasised, *"the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception"*.[33] The Joint Committee also noted this significant omission and called for *"more safeguards for the sharing of intelligence with overseas agencies on the face of the Bill"*, which should necessarily *"address concerns about potential human rights violations in other countries that information can be shared with"*.[34]

8. 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."*[35] The so-called 'double lock' of warrants being authorised by both a Secretary of State and a Judicial Commissioner is one of the most misleading aspects of the draft Bill. It is in reality a single lock, and it is the Secretary of State who has the key. In practice, judicial commissioners would be unable to challenge decisions. If the UK wants to be able to claim its surveillance legislation is world-leading, it must at the very least adopt independent judicial authorisation.

8.1 WHAT PARLIAMENTARIANS NEED TO KNOW:

- Judicial authorisation is an international norm: The UK is alone among democratic allies in permitting political authorisation. 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 fulfil its human rights obligations and to provide a world leading oversight regime.
- Judicial Commissioners would not be able to challenge surveillance decisions: Judicial Commissioners (JCs) would sign off on whether ministers had followed proper processes, in secret. 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 draft 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 noted that this proposal has been *"heavily criticised by many of our witnesses"*.[36] The functions should be formally distinct, with judges tasked with authorising warrants, and a new body established to unify and fulfill the oversight role.
- The introduction of the flawed judicial authorisation is not applied consistently to powers across the draft 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.

9. WHAT NEXT?

Don't Spy on Us is a coalition of the most influential organisations who defend privacy, free expression and digital rights in the UK and in Europe. We would like to invite MPs and Peers to meet with us to discuss the revised Investigatory Powers Bill so that we can work to get surveillance legislation that is fit-for-purpose.

PLEASE CONTACT:

Eric King, Director, Don't Spy on Us: eric@ericking.co.uk

Pam Cowburn, Communications Director, Open Rights Group: pam@openrightsgroup.org

Mike Harris, Consultant, Don't Spy on Us: mike@89up.org

REFERENCES

1 Report on the draft Investigatory Powers Bill, Intelligence and Security Committee of Parliament, February 2016, p3 bit.ly/1T9AENO

2 Intelligence and Security Committee press release announcing publication of their report into the Investigatory Powers Bill bit.ly/1S3uxZU

3 ISC report p2 bit.ly/1T9AENO

4 Intelligence Services Act 1994, p2 bit.ly/1QAen4V

5 ISC Report p12

6 Written evidence submitted to the Joint Committee on the Draft Investigatory Powers Bill p83 bit.ly/1QHKlm2

7 Independent Reviewer of Terrorism Legislation, A Question of Trust – Report of the Investigatory Powers Review, June 2015 p5 bit.ly/1WLue5n

8 Joint Committee on the Draft Investigatory Powers Bill Report p88 bit.ly/1QAgdmo

9 Joint Committee report p9

10 Joint Committee report p104

11 Joint Committee report p8

12 Oral evidence to the Joint Committee on the Draft Investigatory Powers Bill bit.ly/1OxpESk

13 Joint Committee report p8

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

15 Written evidence submitted to the Joint Committee p204

16 Joint Committee report p10

17 http://www.telegraph.co.uk/news/11155337/Big-companies-snoop-on-public-more-than-GCHQ-says-spy-chief.html

18 Joint Committee report p104

19 ISC report p7

20 Joint Committee report p14

21 Science & Technology Committee report p22

22 Science & Technology Committee report p23

23 Written evidence submitted to the Joint Committee p1337

24 Joint Committee report p11

25 Written evidence submitted to the Joint Committee p1338

26 Written evidence submitted to the Joint Committee p391

27 Written evidence submitted to the Joint Committee p1269

28 Written evidence submitted to the Joint Committee p1270

29 Written evidence submitted to the Joint Committee p1337

30 Written evidence submitted to the Joint Committee p909

31 Joint Committee report p8

32 ISC report p12

33 ISC report p12

34 Joint Committee report p17

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

36 Joint Committee Report p149

DON'T SPY ON US

Don't Spy On Us is a coalition of the most influential organisations who defend privacy, free expression and digital rights.

dontspyonus.org.uk

OPEN RIGHTS GROUP

ARTICLE 19

ENGLISH PEN

PRIVACY INTERNATIONAL

BIG BROTHER WATCH
DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

LIBERTY
PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS