PRIVACY INTERNATIONAL

Submitted to the Honourable Members of the Joint Committee on the Draft Investigatory Powers Bill

Submission to the Joint Committee on the Draft Investigatory Powers Bill

Submitted by Privacy International

21 December 2015

PRIVACY INTERNATIONAL'S SUBMISSION TO THE JOINT COMMITTEE ON THE DRAFT INVESTIGATORY POWERS BILL IN RESPONSE TO THE CALL FOR EVIDENCE ON THE DRAFT INVESTIGATORY POWERS BILL

21 December 2015

Submitted to the Honourable Members of the Joint Committee on the Draft Investigatory Powers Bill

Summary

1. Thank you for the opportunity to provide comments on the draft Investigatory Powers Bill (IP Bill).

2. Privacy International was founded in 1990. It is a leading charity promoting the right to privacy across the world. It is based in London and, within its range of activities, focuses on tackling the unlawful use of surveillance. It is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised, and reported to, among others, the Council of Europe, the European Parliament, the Organisation for Economic Co-operation and Development, and the United Nations.

3. The IP Bill aims to overhaul existing surveillance legislation and act as an example of the "gold standard" for governments around the world. Unfortunately, the current draft falls significantly short of this goal.

4. In doing so, the IP Bill, as currently drafted, violates the right to privacy (under UK and international human rights law); undermines the security of digital data; imposes burdensome and unreasonable requirements on companies; and erodes the trust of individuals in communication technologies. It does all this while, at the same time, failing to provide an accessible, foreseeable legal framework that would make intelligence agencies and the police accountable for their surveillance activities; or providing for an oversight framework which - while in some ways improves upon the current regime - still does not have the necessary powers to check and prevent abuse.

5. The following are some highlights of our concerns and recommendations, which are more fully described throughout this submission:

6. Bulk warrants – Parts 6 and 7 of the draft IP Bill address a range of bulk warrants: bulk interception warrants; bulk acquisition warrants; bulk equipment interference warrants; and bulk personal dataset warrants. We have expressed our concern that such warrants would codify a practice of mass, untargeted surveillance.[1] This practice subverts the traditional investigative

1 *See* Privacy International & Open Rights Group, Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, 7 Dec. 2015, para. 9 [hereinafter "Joint Committee on Human Rights Submission"], available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf; *see also* Anderson

process, by which the Government has reason to suspect someone and applies for a warrant to surveil that person.[2] Bulk warrants, by contrast, permit the intelligence agencies to surveil everyone. They are neither lawful, nor necessary or proportionate. Nor have they proven to be effective. Privacy International calls for their removal from the IP Bill.

7. Thematic warrants – While disguised as targeted surveillance, the IP Bill seeks to introduce in law "thematic warrants" (both for interception and equipment interference.) Thematic warrants delegate the choice as to whose privacy will be interfered with to the police or intelligence agencies, increasing the risk of arbitrary action and undermining the implementation of effective judicial authorisation. Communications or equipment *within* the United Kingdom may be intercepted or interfered with under a thematic warrant. These are bulk powers being used against people within the UK. Privacy International calls for their removal from the IP Bill.

8. Communications data and data retention – Even the Home Office admits that these parts of the IP Bill contain new powers. In fact, they significantly expand the capacity of a range of public authorities (not only the intelligence services and the police) to obtain highly sensitive information about individuals without judicial authorisation. Internet Connection Records (ICRs), while far from clear in scope, have the potential to intrude significantly into people's private lives. This is combined with a regime of blanket, untargeted data retention that, if adopted, will lead to the collection and storage, for up to a year, of highly revealing information pertaining to virtually all communications sent, received or otherwise created by us all. Privacy International opposes blanket data retention and suggests the introduction of targeted preservation orders instead.

9. Equipment interference – The IP Bill seeks to introduce "equipment interference" powers, including in bulk. Hacking is an incredibly intrusive form of surveillance, permitting both real-time surveillance as well as access to the breadth of private information we increasingly store on our digital devices, from text messages and emails to photos, videos, address books and calendars. Moreover, hacking, as undertaken by any actor, including the state, fundamentally impacts on the security of computers and the internet. For these reasons, we question whether hacking can ever be a legitimate aspect of state surveillance.

10. Privacy International submitted oral evidence to the Joint Committee on 9 December 2015. In this submission, Privacy International builds on the information provided during that hearing and provides responses to all the questions posed by the Joint Committee in its call for written evidence.[3]

Report, para. 2.31 ("Bulk collection of electronic messages, as the Snowden Documents brought home, can be achieved with far less effort and so brings the potential (if not properly regulated) for spying on a truly industrial scale.").

2 Bruce Schneier, Data and Goliath (2015), page 179.

3 Privacy International also submitted written evidence on the IP Bill to the Science and Technology Committee of the House of Commons (available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html) and the Joint Committee on Human Rights (available at:

Overarching/thematic questions

Are the powers sought necessary?

11. This question has two dimensions – efficacy and legality. Privacy International submits that for certain of the parts of the IP Bill, particularly the bulk powers and data retention, necessity has not been demonstrated on either dimension.

Has the case been made, both for the new powers and for the restated and clarified existing powers?

12. We dispute the UK Government's characterisation of particular powers as "existing" rather than "new". The foreword to the draft IP Bill by the Home Secretary states, for example, that "[t]he draft Bill only proposes to enhance powers in one area – that of communications data retention".[4] The distinction between "new" and "existing" powers is important because "new" powers are often subjected to a higher level of scrutiny. By erroneously describing "new" powers as "existing", the Government seems to be seeking easier acceptance of new and/or enhanced powers that should be subject to especially critical analysis and robust debate.

13. One particularly glaring example of this mischaracterisation concerns the "equipment interference" power. Privacy International's current complaint before the Investigatory Powers Tribunal (IPT), which asserts that GCHQ has violated the Computer Misuse Act (CMA) 1990 and the European Convention on Human Rights (ECHR) by hacking computers, is instructive on this point.[5] Until we brought our claim, GCHQ had never publicly acknowledged engaging in equipment interference.[6] After we filed our complaint, the Home Office published a draft Equipment Interference Code of Practice[7] in an apparent attempt to provide the legal specificity necessary to address our assertion any hacking the intelligence services were conducting was not "in accordance with law." Yet the draft Code is not primary legislation.

14. The draft IP Bill places the power to hack on statutory footing for the first

---

http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf).

4 Foreword, Investigatory Powers Bill.

5 The Snowden documents indicate that GCHQ had, at least internally, arrived at a similar conclusion. A September 2010 document prepared by a GCHQ representative reports a "concern" that a certain hacking technique "may be illegal" because

> The Computer Misuse Act 1990 provides legislative protection against unauthorised access to and modification of computer material. The act makes specific provisions for law enforcement agencies to access computer material under powers of inspection, search or seizure. However, the act makes no such provision for modification of computer material.

Privacy International et al. v. Secretary of State for Foreign and Commonwealth Affairs, Skeleton Argument Served on behalf of the Claimants, para. 23, 7 Oct. 2015 [hereinafter "Skeleton Argument"].

6 *See* Anderson Report, paras. 7.64-5, 14.13.

7 The draft Equipment Interference Code of Practice is available at: https://www.gov.uk/government/publications/interception-of-communications-and-equipment-interference-codes-of-practice

time.[8] In such circumstances, we submit that this power cannot be characterised as "existing".

15. *New Powers* - Below, we detail how the operational case for the following new powers has not been made: bulk warrants; communications data, with respect to (a) ICRs and (b) data retention; and equipment interference.

16. Bulk Warrants - Efficacy: The primary operational justification for bulk warrants is to improve knowledge of threats to national security through the detection of patterns and links in communications data.[9] The Government has represented that it needs "to sift through 'haystack' sources – without looking at the vast majority of material that has been collected – in order to identify and combine the 'needles', which allow them to build an intelligence picture."[10]

17. This operational argument is subject to critical fallacies that we encourage the Committee to seriously consider. The success of data mining relies on a set of particular factors, including "a well-defined profile", "a reasonable number of events per year", and a low "cost of false alarms".[11] For this reason, credit card fraud detection, for example, has become a relatively effective form of data mining: fraudulent purchases are easy to identify, credit card transactions number in the billions and the cost of a false alarm is a phone call to the cardholder.

18. By contrast, terrorist plots are rare and each has unique facets, meaning "false positives completely overwhelm the system."[12] And the cost of a false alarm is high, leading to time and money wasted following false leads when our intelligence agencies could be doing more productive work. We see this in the

---

8 *See* Anderson Report, para 12.8 (noting that "the use of [equipment interference], only recently acknowledged by the Government through the publication of the Draft Equipment Interference Code" was one of several "intrusive practices" that "do not find clear and explicit basis in legislation"). The pre-existing legislation that the Home Office cites as authorizing hacking – the Intelligence Service Act 1994 and the Police Act 1997 – both do not mention equipment interference. Instead, they provide broad powers under which, as Anderson declares, it is not at all clear hacking would be carried out.

9 See the Home Office Factsheets on "Bulk Interception", "Bulk Communications Data", "Bulk Equipment Interference", and "Bulk Personal Databases", all available at https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents. *See also* ISC Report, para. 90 ("GCHQ's bulk interception capability is used primarily to find patterns in, or characteristics of, online communications which indicate involvement in threats to national security.").

10 *See* ISC Report, para. 51 (quoting written evidence submitted by the Government); *see also* Anderson Report, para. 10.22(a).

11 *Id*.

12 *Id*. at page 137 (citing, *inter alia*, John Mueller and Mark G. Stewart, Terror, Security, and Money: Balancing the Risks, Benefit, and Costs of Homeland Security, Oxford University Press (2011), chap. 2; G. Stuart Mendenhall & Mark Schmidhofer, "Screening Tests for Terrorism", *Regulation*, Winter 2012-13, http://object.cato.org/sites/cato.org/files/serials/files/regulation/2013/1/v35n4-4.pdf; Fred H. Cate, "Government data mining: The need for a legal framework", Harvard Civil Rights-Civil Liberties Law Review 43, Summer 2008, http://www.law.harvard.edu/students/orgs/crcl/vol43_2/435-490_Cate.pdf; Jeff Jonas & Jim Harper, "Effective counterterrorism and the limited role of predictive data mining", Cato Institute, 11 Dec. 2006, http://www.cato.org/publications/policy-analysis/effective-counterterrorism-limited-role-predictive-data-mining); *see also* ISC Report, para. 56 ("Amongst the everyday internet usage of billions of people . . . a very small proportion will relate to threats to the national security of the UK and our allies.").

American context: reviews of the NSA's mass surveillance programs have concluded that they were "not essential to preventing attacks" or had "no discernible impact".[13] A recent Council of Europe report came to the same conclusion this year, finding that "mass surveillance is not . . . effective as a tool in the fight against terrorism and organised crime, in comparison with traditional targeted surveillance."[14]

19. As security expert Bruce Schneier puts it:

> When you're looking for the needle, the last thing you want to do is pile lots more hay on it. More specifically, there is no scientific rationale for believing that adding irrelevant data about innocent people makes it easier to find a terrorist attack, and lots of evidence that it does not. You might be adding slightly more signal, but you're also adding much more noise.[15]

20. Mass surveillance is the wrong tool for ferreting out criminals and terrorists. Pouring more resources into these programs results in less security for us all.[16] We are awash with examples of how terrorist plots have been or could have been detected using time-honoured investigative techniques.[17] The RUSI report indicates that "lack of detailed intelligence available on a small number of high-priority targets . . . is the prime concern, rather than broader intelligence available on a large number of low-priority targets.[18]

21. Both the Anderson and ISC Reports cite case studies provided by GCHQ, which supposedly demonstrate the efficacy of bulk capabilities.[19] These case studies cannot be published, even in redacted form, which makes it difficult for the public to independently evaluate the efficacy argument.[20] Anderson himself

---

13 Peter Bergen, "Do NSA's Bulk Surveillance Programs Stop Terrorists?", New America Foundation, Jan. 2014, https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/; The President's Review Group on Intelligence and Communications Technologies, Liberty and Security in a Changing World, Dec. 2013, page 104; *see also* Yochai Benkler, "Fact: The NSA Gets Negligible Intel from Americans' metadata. So end collection", Guardian, 8 Oct. 2013, http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

14 PACE Committee on Legal Affairs and Human Rights, *Mass Surveillance* (Jan. 2015), at para. 126, available at http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf.

15 Schneier, Data and Goliath, page 138 (citing Mike Masnick, "Latest Revelations Show How Collecting All the Haystacks to Find the Needle Makes the NSA's Job Harder", Tech Dirt, 15 Oct. 2013, https://www.techdirt.com/articles/20131014/17303424880/latest-revelations-show-how-collecting-all-haystacks-to-find-data-makes-nsas-job-harder.shtml; Chris Young, "Military intelligence redefined: Big Data in the battlefield", Forbes, 12 Mar. 2012, http://www.forbes.com/sites/techonomy/2012/03/12/military-intelligence-redefined-big-data-in-the-battlefield/).

16 *See* Jeffrey W. Seifert, "Data Mining and Homeland Security: An Overview", Congressional Research Service, 3 Apr. 2008, https://fas.org/sgp/crs/homesec/RL31798.pdf.

17 National Commission on Terrorist Attacks, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Activities upon the United States, https://www.gpo.gov/fdsys/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf. Simon Shuster, "The Brothers Tsarnaev: Clues to the Motives of the Alleged Boston Bombers", Time, 19 Apr. 2013, http://world.time.com/2013/04/19/the-brothers-tsarnaevs-motives/.

18 RUSI Report, para. 3.53.

19 Anderson Report, para. 7.26; ISC Report, para. 81.

20 Anderson Report, para. 7.26; ISC Report, para. 81. Anderson annexed six outline examples of these case studies to his report, but describes this effort as only "go[ing] a little way towards remedying th[e] defect" of lack of public transparency. Anderson Report, para. 7.27.

notes that "[t]here are limits to what the public will (or should) take on trust" and that "the justification to a public audience of such a potentially intrusive power deserves and arguably needs more".[21] The Government has thus far failed to provide more. We therefore encourage the Committee to closely scrutinise arguments that these tactics are operationally necessary, including by considering the actual value of information produced by mass surveillance and how much of this information could have been obtained by less intrusive means.

22. Internet Connection Records (ICRs) – Efficacy: The "great majority of communications data use is for the prevention or detection of crime, or the prevention of disorder", followed by national security and emergency prevention of death or injury.[22] The Government represents that ICRs "are records of the internet services that have been accessed by a device" and the power to collect them is necessary "to attribute a particular action on the internet to an individual person."[23] It provides, as an example of an ICR, "a record of the fact that a smartphone had accessed a particular social media website at a particular time."[24]

23. The precise definition of an ICR remains unclear but appears to include the "web logs" addressed by Anderson.[25] In his report, Anderson noted that "web log" was also an uncertain term but quoted the Home Office's definition:

> "Weblogs are a record of the interaction that a user of the internet has with other computers connected to the internet. This will include websites visited up to the first '/' of its [url], but not a detailed record of all web pages that a user has accessed. This record will contain times of contacts and the addresses of the other computers or services with which contact occurred."[26]

24. Anderson concluded that "[u]nder this definition, a web log would reveal that a user has visited e.g. www.google.com or www.bbc.co.uk, but not the specific page."[27]

25. The equivalence between ICR and "web log" is important because Anderson expressed deep hesitation about introducing an obligation for CSPs to retain such data. He noted it had not been demonstrated that "access to weblogs is essential for a wide range of investigations" and that even within the law enforcement community, "it is widely accepted . . . that the compulsory retention of web logs would be potentially intrusive."[28] From a comparative perspective, Anderson observed that no other European or Commonwealth

---

21 Anderson Report, paras. 7.27, 10.8.
22 Anderson Report, para. 9.21.
23 Home Office, "Factsheet: Internet Connection Records", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473745/Factsheet-Internet_Connection_Records.pdf.
24 *Id*.
25 See Investigatory Powers Bill, Explanatory Notes, para. 190, which describes ICRs in language that is similar to Anderson's description of web logs. It is not clear, however, that paragraph 190 is an accurate description of everything that could be captured under the IP Bill's definition of ICRs.
26 Anderson Report, para. 9.53.
27 *Id*. at para. 9.54.
28 *Id*. at para. 9.60.

country appears to compel their CSPs to retain such data and that Canadian and American law enforcement represented "that there would be constitutional difficulties in such a proposal."[29] He concluded that while "retained records of user interaction with the internet (whether or not via web logs) would be useful . . . that is not enough on its own to justify the introduction of a new obligation on CSPs, particularly one which could be portrayed as potentially very intrusive on their customers' activities."[30]

26. Anderson emphasised that any proposal progressing this issue would "need to be carefully thought through and road-tested with law enforcement, legal advisers and CSPs" with robust consultations with "[o]utside technical experts, NGOs and the public".[31] He suggested a detailed list of issues that should be addressed, including, *inter alia*:

    1. the precise definition of the purposes for which such records should be accessible, and the relative importance of those purposes;

    2. the extent to which those purposes can in practice be achieved under existing powers (e.g. the inspection of a seized device), by less intrusive measures than that proposed or by data preservation, i.e. an instruction to CSPs to retain the web logs or equivalent of a given user who was already of interest to law enforcement;

    3. the precise records that would need to be retained for the above purposes, and how those records should be defined;

    4. the steps that would be needed to ensure the security of the data in the hands of the CSPs;

    5. the implications for privacy; or

    6. the cost and feasibility of implementing the proposals.[32]

27. Privacy International notes that while the Home Office has produced a stand-alone document purporting to lay out the operational case for ICRs, it fails to address many of the questions outlined above.[33] We accordingly encourage the Committee to press the Home Office on these points.

28. Data Retention- Efficacy: The primary operational justification for compulsory data retention comes from law enforcement agencies, who insist they need this power to preserve evidence of historic criminality.[34] Privacy International does not dispute that older data can be important to criminal investigations; we simply submit that there are alternatives that may be just as effective but do not pose the same privacy intrusions or security risks as bulk retention. The serious security risks posed by the data retention requirements in the draft IP

29 *Id*. at para. 9.55.
30 *Id*. at para. 14.33.
31 *Id*. at para. 14.35.
32 *Id*. at para. 14.33.
33 Home Office, "Operational Case for the Retention of Internet Connection Records", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf.
34 *See* Anderson Report, para. 9.45.

Bill are particularly acute.[35] Precisely because of the revealing nature of such data, the database(s) where this retained data is stored are also likely to be targeted by cyber criminals and foreign intelligence services. By compelling retention, the Government "unnecessarily endangers the security of communications service providers who could be subject to increased attacks."[36] In the past year, we have witnessed the ramifications of several such attacks on businesses such as TalkTalk, Vodafone and British Gas.[37] In a study commissioned by the Department of Business, Innovation and Skills, 90% of large businesses and 74% of small businesses had detected at least one breach in the previous twelve months.[38]

29. We urge the Committee to press the Home Office on alternatives such as Data Preservation Orders for specific individuals based on an investigation or proceeding. The Home Office's answers should be concrete, focusing on issues such as relative efficacy, cost and intrusion on privacy. Finally, we remind the Committee that CSPs tend to keep customer data for their own business purposes so foregoing mandatory bulk retention will not mean that it will all disappear.

30. Equipment Interference - Efficacy: With respect to law enforcement, the Government has failed to make any operational case for the power to hack. The Government's factsheet on "Targeted Equipment Interference" is limited to sweeping statements – e.g., "helps law enforcement agencies to protect the most vulnerable members of society" – but makes no concrete arguments as to why such an intrusive surveillance technique is needed.[39] For example, while the Government argues that hacking could assist in obtaining "a key piece of information encrypted in transmission", it has provided no evidence as to the number of times encryption has actually impeded a criminal investigation.[40] As a point of comparison, the US government has reported that in 2013, encryption stymied the police just nine times, up from four in 2012.[41]

31. The operational case for why the security and intelligence agencies require the power to hack is similarly weak. The only operational statement described by Anderson in terms of this capability is that the agencies "need to develop new methods of accessing data, for example through increased use of CNE."[42] But there is no further elaboration on how necessary CNE is to the acquisition of operationally important data. The Government's factsheet points to the two

35 Science & Tech Committee Submission, paras. 26-30.
36 *Id*. at para. 29.
37 *Id*. at para. 29 n. 17.
38 Department of Business, Innovation and Skills, "2015 Information Security Breaches Survey", https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf.
39 Home Office, "Factsheet: Targeted Equipment Interference", https://www.gov.uk/government/publications/draft-investigatory-powers-bill-overarching-documents. Anderson records an equally vague statement from law enforcement agencies regarding their need for this power. *See* Anderson Report, para. 9.75.
40 Home Office, "Factsheet: Targeted Equipment Interference".
41 *See* Andy Greenberg, "Rising use of encryption foiled cops a record 9 times in 2013," *Wired*, 2 July 2014, http://www.wired.com/2014/07/rising-use-of-encryption-foiled-the-cops-a-record-9-times-in-2013/.
42 Anderson Report, para. 10.21. The ISC Report is limited to describing the scope of current hacking operations. *See* ISC Report, paras. 173-78.

following facts as support for the power to hack:[43]

1. During 2013 around 20% of GCHQ's intelligence reports contained information that derived from EI operations;

2. MI5 has relied on EI in the overwhelming majority of high priority investigations over the past 12 months.

32. These two assertions fail to demonstrate that the potential intelligence benefits of hacking outweigh the critical security risks posed by this practice. The Government does not, for example, elaborate on the quality of "information that derived from EI operations" and whether that information could have been obtained by any other means. Similarly, it is unclear the extent to which EI was critical to the "high priority investigations" in which it played a role and again, the extent to which MI5 might rely on other techniques that expose the public to less of a security risk.

33. Existing Powers - Even if the Government were to insist that the powers we characterise as "new" are "existing", Privacy International submits that the efficacy and legality concerns outlined above remain relevant and are reason enough to seriously question the inclusion of such powers in the draft IP Bill.

34. We also submit that with respect to existing powers, the draft IP Bill proposes expanding some of them. Below, we describe how the case has not been made for one such expansion: the use of "thematic warrants" under targeted interception as reflected in the expansion of the subject matter of warrants in IP Bill clause 13.

35. The ISC Report revealed for the first time that the Home Secretary has been interpreting "person" in the Regulation of Investigatory Powers Act 2000 (RIPA) section 8(1)(a) as "any organisation or any association or combination of persons".[44] MI5 has been, in practice, obtaining "thematic warrants" in reliance on this definition.[45] We address the legal concerns surrounding thematic warrants in more detail in paragraphs 67 to 77 below. Given the very recent avowal of thematic warrants and the shaky interpretation of RIPA upon which they rest, we submit that thematic warrants should be considered an expansion of the targeted interception authorised under RIPA.[46]

36. Efficacy: The operational case for such an expansion is not clear. The ISC indicates that "the very significant majority of 8(1) warrants relate to one individual" while "in some limited circumstances an 8(1) warrant may be

43 Home Office, "Factsheet: Targeted Equipment Interference". The Home Office's Factsheet on "Bulk Equipment Interference" is even less helpful. Aside from reiterating the first statistic, it provides no additional substantive arguments in support of the hacking power. As we explained in our prior submission to the Science & Technology Committee, the bulk equipment interference powers compound the security concerns presented by targeted hacking by giving "almost unfettered powers to the intelligence services to decide who and when to hack." Science & Tech Committee Submission, para. 18.

44 ISC Report, para. 42.

45 *Id*. at para. 43; Anderson Report, para. 6.42.

46 Anderson Report, para. 14.62 (noting that there is "no very clear backing for [thematic warrants] on the face of RIPA s8(1)).

thematic."[47] MI5 explained to the ISC that it applies for a thematic warrant "where we need to use the same capability on multiple occasions against a defined group or network on the basis of a consistent necessity and proportionality case . . . rather than [applying for] individual warrants against each member of the group."[48] This explanation suggests a thematic warrant is a matter of convenience – resulting in certain efficiency gains – rather than of operational necessity. This reading is borne out by law enforcement's representation to Anderson that thematic warrants would help to deal with the proliferation of documents required by the current warrant regime.[49] It is worth underlining that the Interception of Communications Commissioner's Office represented to the ISC that, in some instances, thematic warrants have been abused.[50] The ISC itself expressed, in its conclusion, reservations about "the extent that this capability is used and the associated safeguards."[51]

37. Recommendations

    1. Remove bulk powers from the draft IP Bill.

    2. Remove ICRs as a category of communications data that can be collected or ordered retained from the draft IP Bill.

    3. Remove the obligation to retain communications data in the draft IP Bill, replacing it with the ability to issue targeted preservation orders based on individualized suspicion.

    4. Carefully assess whether the operational case for including equipment interference in the draft IP Bill outweighs the security concerns raised by government use of equipment interference.

    5. Remove Clause 13(2), which permits the Government to apply for "thematic warrants" under the targeted interception power, from the draft IP Bill.

Are the powers sought legal? Are the powers compatible with the Human Rights Act and the ECHR?

38. The fact that the IP Bill seeks to put on a statutory footing the surveillance powers exercised by the intelligence services and law enforcement does not, in itself, fulfil the requirements of legality under international human rights law.

39. Article 8 of the ECHR requires certain minimum safeguards in the legal framework regulating surveillance activities to protect against arbitrary interference with privacy and abuse. In particular, the law must include the nature of the offences which may give rise to an order to interfere with someone's privacy; a definition of the categories of people liable to have their communications (including communications data) monitored; a limit on the

47 ISC Report, para. 43.

48 *Id*. at para. 43 (quoting written evidence submitted by MI5).

49 Anderson Report, para. 9.33 (quoting the law enforcement agencies' complaint of "so many pieces of paper on the same target: different routes, different authorisation levels, not much flexibility of timescale").

50 ISC Report, para. 45.

51 *Id*. at ISC, page 24, para. D; *see also* Anderson Report, para. 7.16(a) (describing the ISC as viewing thematic warrants "warily").

duration of such monitoring; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when sharing the data with other parties; and the circumstances in which the data obtained must be erased or destroyed.[52]

40. That the data sought may be of value is not sufficient to make its collection or retention lawful. For instance, in S and Marper v United Kingdom, the UK government submitted that the retention of DNA samples from people who had not been charged or convicted of a criminal offence was of "inestimable value" and produced "enormous" benefits in the fight against crime and terrorism (§92). The Grand Chamber of the ECtHR nonetheless held that the retention was a "disproportionate interference" with those individuals' private lives (§135). Central to the reasoning was the absence of any assessment of suspicion by the authorities that was sufficient to justify the retention of each individual's DNA data.[53]

41. Furthermore, in October 2015, the Grand Chamber of the Court of Justice of the European Union (CJEU) ruled that "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life."[54]

42. Given this, Privacy International believes the bulk warrants in the draft IP Bill are unlawful (Parts 6 and 7 of the IP Bill). Similar concerns apply to the proposed regime for retention of communications data (Part 4 of the IP Bill). We have expressed certain of our concerns regarding legality in our joint submission with Open Rights Group to the Joint Committee on Human Rights.[55] We expand upon that submission here.

Bulk Warrants

43. Targeting - Bulk warrants do not require any suspicion whatsoever on the part of the authorities that a person has committed a criminal offence or is a threat to the interests of national security (or other relevant grounds.) Similarly these warrants do not have to define the categories of persons who are liable to have their communications monitored. Instead bulk warrants need only state the operational purposes for which data is to be obtained, and the IP Bill expressly notes that these can be "general purposes", thereby potentially being as broad as "countering terrorism" (see in particular Clauses 111(4), 125(4) and 140(5)).

44. In this respect, the IP Bill does not address the concerns raised by the current "bulk" warrant regime under RIPA, which this bill aims to reform. As noted by the ISC in relation to the RIPA regime: "[T]he categories are expressed in very general terms. For example: 'Material providing intelligence on terrorism (as

52 See Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, confirming earlier jurisprudence of the Court.

53 See S and Marper v United Kingdom, [GC] No. 30562/04, 4 December 2008.

54 Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner, 6 October 2015.

55 See Privacy International and Open Rights Group's Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, submitted 7 December 2015, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf

defined by the Terrorism Act 2000 (as amended)), including, but not limited to, terrorist organisations, terrorists, active sympathisers, attack planning, fund-raising.'"[56]

45. Further, nowhere in the IP Bill is there a definition of "national security" or "economic well-being" of the United Kingdom (grounds under which bulk warrants can be issued), nor any indication of the circumstances under which communications can be surveilled on the basis of such grounds. It leaves authorities an almost unlimited degree of discretion in determining which events are relevant to national security and does not require any assessment of the level of threat to justify secret surveillance.

46. As we discuss in our response to the question, "Is the authorisation process appropriate?", the broad scope of the "bulk" warrants means the authorisation process falls short of what is required under international human rights law. In particular it leaves the authorities (including the Judicial Commissioners) unable to verify, as recently reiterated by the European Court of Human Rights in Zakharov, "the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security." [57] Nor it will allow them to "ascertain whether the requested interception meets the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the [ECHR], including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means."[58]

47. Renewal - "Bulk" warrants can be renewed an indefinite number of times (see Clauses 113, 127, 142, 161) and as there is no requirement to target a particular individual or premises, there is no restriction on the possibility that a person's communications may be routinely intercepted, again and again, for an indefinite period under successive "bulk" warrants.

48. Safeguards - The procedure to be followed for examining, sharing, retaining and deleting material or data obtained through "bulk" warrants are too broad and vague to provide sufficient guidance and prevent abuse.[59]

49. In particular, the disclosure and copying of information obtained under a "bulk" warrant is broadly permitted so long as the information is or *is likely* to become necessary in the interests of national security or other relevant grounds. Similarly provisions regulating the destruction of material or data obtained through "bulk" warrants would allow the retention of such data indefinitely. Notably, these provisions do not limit copying, sharing or retaining data as necessary for the ground for which the specific warrant was originally issued, but for any grounds under which the "bulk" warrants can be issued.

50. There are no details on the safeguards required for the storage of data collected,

56 Intelligence and Security Committee of Parliament, report: Privacy and Security: A modern and transparent legal framework, 12 March 2015 para 101.
57 Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 260.
58 Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 261.
59 See"general safeguards" under Clauses 117, 131, and 146.

with relevant Clauses of the IP Bill simply stating that such storage is done in "a secure manner".

51. The "safeguards" for examination of intercepted materials under "bulk" interception warrants confirm the discriminatory distinction already contained in the Regulation of Investigatory Powers Act (RIPA) between materials referable to an individual in the British Islands or not. For materials not related to individuals in the UK, there is no requirement of a targeted examination warrant. Instead, the intercepted materials can be examined without limitation, in so far as it is necessary for the purpose specified in the bulk warrant, which can be very general (Clause 119). A similar provision applies for bulk equipment interference warrants (Clause 147).

52. This distinction between external and internal communications is discriminatory on grounds of nationality and national origin.[60] Further, as noted by David Anderson in his report A Question of Trust, the distinction between internal and external communications is arbitrary and rendered meaningless in the context of the technical architecture of modern digital communications, with messages such as e-mails routed through different countries even if both the sender and the intended recipient are resident in the UK.[61]

53. Transferring data overseas - The "safeguards" that apply to transferring data to parties overseas are even weaker than those applicable for "domestic" sharing and leave wide discretion, only requiring the Secretary of State or another relevant authority to apply the already vague standards applicable to domestic sharing "to the extent (if any) as the Secretary of State consider appropriate".[62] As such, any restrictions on the sharing of the collected data with foreign authorities are entirely at the discretion of the Secretary of State.

54. Privacy International is also concerned that the IP Bill fails to specify the circumstances in which such overseas transfer can be authorised. Except for the provisions regulating Mutual Assistance Warrants (that apply only to interception of communications) there is no mention in the IP Bill of the grounds, limits and authorisations required for sharing data obtained through surveillance. In this respect the IP Bill fails to resolve one of the most controversial and concerning practices of UK intelligence agencies, namely receiving and sharing acquired data in ways that are unregulated and may have the effect of circumventing applicable safeguards (notably under the Five Eyes arrangements). If confirmed, this would leave a significant loophole in the new regime regulating the use and oversight of investigatory powers, resulting

60 The UN High Commissioner for Human Rights and the UN Special Rapporteur on counter-terrorism and human rights have noted how several legal regimes on interception of personal communications, like the UK, distinguish between obligations owed to nationals and non-nationals and residents and non-residents, providing external communications with lower or non-existent protection, in ways that are discriminatory and incompatible with Article 26 of the ICCPR. See report of the UN High Commissioner on Human Rights on the right to privacy in the digital age, UN doc. A/HRC/27/37, 30 June 2014; and report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014.

61 David Anderson QC, A Question of Trust, June 2015.

62 See Clauses 118(2); 131(9); 146(9).

in significant risks of abuse.[63]

Data Retention

55. In our submission to the Joint Committee on Human Rights, we explained the extensive legal concerns raised by the communications data provisions in the draft IP Bill, including those on ICRs.[64] We noted that the CJEU, ECtHR, and numerous UN human rights experts have recognised that the interception, collection and use of communications data interferes with the right to privacy.[65] We also criticised provisions of the draft IP Bill that permit public authorities, with few exceptions, to obtain communications data without prior judicial authorisation.[66] We further point the Committee to Open Rights Group's submission to the Science and Technology Committee, which explains why the operational case made by the Government falls short of demonstrating the necessity and proportionality of the communications data provisions.[67] Finally, we highlight that, with respect to ICRs, Anderson observed that their legality remains in serious question.[68]

56. In our submission to the Joint Committee on Human Rights, we highlighted that the draft IP Bill's communications data retention regime violates existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC.[69] We also noted that the regime appears to run afoul of the CJEU's ruling in *Digital Rights Ireland*, which struck down the 2006 Data Retention Directive.[70] We emphasised that the draft IP Bill's provisions go much further than the invalidated EU Directive in several respects. We also highlighted that the lack of judicial authorisation required for data retention notices seems to flout language in *Digital Rights Ireland* describing the necessary review prior to government access to retained data.[71] Finally, we described how these provisions are in breach of Article 8 of the ECHR as they exceed what could reasonably be regarded as "necessary in a democratic society".[72] In short, the draft IP Bill's data retention requirements are likely to be subject to legal challenge based on recent judgments.

57. Recommendations

    1. Delete Parts 6 & 7 of the IP Bill related to "bulk warrants" and amend other Clauses accordingly.

---

63 See in this respect David Anderson's report, A question of trust, in particular recommendations 76 to 78.

64 Joint Committee on Human Rights Submission, paras. 23-31.

65 *Id*. at para. 29.

66 *Id*. at para. 52.

67 Written evidence submitted by Open Rights Group (IPB0034), http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology- committee/investigatory-powers-bill-technology-issues/written/25147.html.

68 Anderson Report, paras. 9.56, 9.60 ("[I]t is widely accepted within the law enforcement community that . . . the legal environment: *Digital Rights Ireland* may not be conducive to the imposition of such an extensive obligation").

69 Joint Committee on Human Rights Submission, para. 34.

70 *Id*. at para. 35.

71 *Id*. at paras. 53-54.

72 *Id*. at paras. 40-41.

2. Remove the obligation to retain communications data in the draft IP Bill, replacing it with the ability to issue targeted preservation orders based on individualized suspicion.

58. Questions

1. Ask the Home Office to clarify whether the IP Bill seeks to regulate intelligence sharing; if so how; and if not, why not?

Is the requirement that they be exercised only when necessary and proportionate fully addressed?

59. The fact that warrants and authorisations under the IP Bill can only be issued upon consideration that the measures are necessary and proportionate is not sufficient to ensure that such measures are indeed necessary to the pursuance of a legitimate aim.

60. Firstly, the warrant regime proposes a weak necessity test. The IP Bill specifies that the relevant authority, when assessing the necessity and proportionality of a proposed measure that will interfere with the right to privacy, should take into account "whether the information which it is considered necessary to obtain under the warrant could reasonably be obtained by other means."[73]

61. This test falls short of requiring consideration of whether other less invasive techniques have been exhausted or would be futile, such that the techniques used is the least invasive option. It is a well-established principle under international human rights law that when contemplating a limitation to someone's right, the least invasive measure should be applied.[74]

62. Secondly, the requirements of some of the warrants are so vaguely formulated that they will make it next to impossible to assess the necessity and proportionality of the envisaged measure. As noted above, the IP Bill allows the purposes of "bulk" warrants to be described in "general terms".

63. Even those supposedly "targeted" warrants (such as "targeted interception warrants" in Part 2 and "equipment interference warrants" in Part 5 of the IP Bill) would permit the intelligence services or law enforcement to conduct surveillance without needing to specify in the warrant the person or equipment that is to be the subject of the surveillance. As discussed in more detail below, in paragraphs 67 to 77, such "thematic" warrants could be broadly framed as targeting "a group of persons who share a common purpose or who carry on, or may carry on, a particular activity" (Clause 13); or "equipment belonging to, used by or in possession of persons who form a group that shares a common purpose or who carry on, or may be carrying on, a particular activity" (Clause 83).

64. This leaves almost unfettered discretion to the implementing authorities to decide who to put under surveillance and when. Notably, it makes it almost

73 See Clauses 14.6; 107.5; 122.4; and 137.4.

74 See Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paragraph 260; Human Rights Committee, in CCPR/C/21/Rev.1/Add.9 and report of the UN Special Rapporteur on counter-terrorism and human rights in A/HRC/13/37, para. 60.

impossible for the Judicial Commissioner to assess whether the measures are necessary, in the absence of any requirement of reasonable suspicion.

Are [the powers sought] sufficiently clear and accessible on the face of the draft Bill?

65. It is difficult to address the almost two hundred pages of the IP Bill in this submission. As a general matter, however, while the IP Bill advances the conversation by setting out a number of powers in more detail than has previously been provided, it falls short of being clear and accessible. This is in part due to the collision of law and technology, which we address in more detail below in response to the question "Are the technological definitions accurate and meaningful (e.g. content vs communications data, ICRs etc.)?"

66. Yet there are several provisions to which technology is not central, but that nevertheless remain opaque.[75]

67. "Targeted" Interception and Equipment Interference - Part 2 and Part 5 purport to permit "targeted" interception and equipment interference, respectively, in contrast to the "bulk" provisions of Part 6.

68. Describing Parts 2 and 5 as targeted is misleading. Both contain significant expansions of the subject matter of "targeted" warrants. This becomes apparent when we compare the new subject matter provisions (Clause 13 for interception and Clause 83 for equipment interference) with their immediate predecessors.

69. In RIPA, targeted interception is permitted under section 8(1) against "one person as the interception subject" or "a single set of premises." These provisions are broader than they appear on their face, as "person" is defined as "any organisation and any association or combination of persons" (RIPA section 81(1)).[76] Nonetheless, there is an attempt at defining a specific target of the interception, especially with regard to premises.

70. The claimed predecessor to Part 5 is section 5 of the Intelligence Services Act 1994 (ISA). Section 5 permits a warrant to issue against "any property so specified" (ISA section 5(2)). Again, specificity is required.

71. Clauses 13 and 83, in contrast, allow interception and equipment interference warrants to relate to, among others:

    1. people or equipment "who share a common purpose or who carry on, or may carry on, a particular activity" (Clauses 13(2)(a) and 83(b));

    2. "more than one person or organization, or more than one set of premises, where the conduct authorized or required by the warrant is for the purposes of the same investigation or operation" (Clauses 13(2)(b) and 83(c)&(e));

75 We note these provisions by way of example only.

76 This definition came to prominence when it was revealed in the Intelligence & Security Committee's report as the basis for issuing "thematic warrants," which are described in paragraphs 42 to 45 of that report. Intelligence and Security Committee of Parliament, *Privacy and Security: A modern and transparent legal framework* (12 March 2015), available at http://isc.independent.gov.uk/news-archive/12march2015 (hereinafter "ISC Report").

3. "equipment that is being, or may be used, for the purposes of a particular activity or activities of a particular description" (Clause 83(f)); or

4. the "testing, maintenance or development" of capabilities relating to interception or equipment interference (Clauses 13(2)(c) and 83 (g)).

72. These subject matter expansions are apparently intended to encompass "thematic" warrants.[77]

73. Under a thematic warrant, the Secretary of State and a Judicial Commissioner will not approve each individual target of the surveillance. Instead, the police and intelligence agencies can choose their targets without additional sign off. For instance, a thematic warrant might authorise the hacking of "all mobile phones in Birmingham" (Clause 83(e)) or the interception of the communications of "anyone suspected of having travelled to Turkey" (Clause 13(2)(a)).

74. Both the Interception of Communications Commissioner[78] and the Intelligence Services Commissioner[79] have expressed concerns about the use of such thematic warrants, especially when they become too broad. Such concern is understandable, given that thematic warrants delegate the choice as to whose privacy will be interfered with to the police or intelligence agents, increasing the risk of arbitrary action and undermining the implementation of effective judicial authorisation. As the Intelligence Services Commissioner points out, "the critical thing . . . is that the submission and the warrant must be set out in a way which allows the Secretary of State to make the decision on necessity and proportionality" (emphasis in original).[80] As discussed above, thematic warrants make this very difficult, especially where the subject matter may be drawn as broadly as Clauses 13 and 83 would permit.[81]

75. Thematic warrants also cut against deeply entrenched principles of the common law. A series of eighteenth century cases established the unconstitutionality of "general warrants", which permitted the Government to search and seize or arrest on the basis of classes of individuals. In Money v. Leach (1765) 97 ER 1075, Lord Mansfield attacked the discretion that a general warrant devolved to those executing it, stating: "It is not fit, that the receiving or judging of the information should be left to the discretion of the officer. The magistrate ought to judge." A resulting bedrock principle of the warrant system is the need to identify a specific individual or property. The draft IP Bill overturns that

---

77 Investigatory Powers Bill, Explanatory Notes, para. 212.

78 ISC Report, para. 45.

79 The Rt Hon Sir Mark Waller, *Report of the Intelligence Services Commissioner for 2014* (25 June 2015), at pages 18-19, available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/437995/50100_HC_225_Intel_Services_Commissioner_accessible.pdf.

80 Ibid. at page 18.

81 As Privacy International argued in our submission to the Joint Committee on Human Rights, such warrants are the equivalent of the long prohibited general warrants, and as such should not be allowed. See Privacy International and Open Rights Group's Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, submitted 7 December 2015, at para. 46, available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/human-rights-committee/legislative-scrutiny-draft-investigatory-powers-bill/written/25654.pdf

principle.

76. Thematic warrants also appear to violate the ECHR. In Zakharov v Russia, the Grand Chamber discussed a number of factors it considers in determining whether "authorisation procedures are capable of ensuring that secret surveillance is not ordered haphazardly, irregularly or without due and proper consideration." It reiterated the principle, expressed in a line of prior cases, that the interception authorisation "must clearly identify a specific person to be placed under surveillance or a single set of premises."[82]

77. To be clear, communications or equipment *within* the United Kingdom may be intercepted or interfered with under a thematic warrant. These are bulk powers being used against people within the UK.

78. Recommendations

    1. Clause 13

        1. Subsection 13(1)(a) – delete "organisation" and replace with "persons"

        2. Delete subsection 13(2)

    2. Clause 83

        1. Subsection 83(a) – delete "organisation" and replace with "persons"

        2. Delete subsections 83(b), 83(c), 83(e), 83(f), and 83(g)

79. Questions

    1. Would clauses 13(2)(c) and 83 (g), which permit warrants relating to the "testing, maintenance or development" of capabilities for interception or equipment interference, allow security researchers or others who are not a threat to national security or suspected of a serious crime to be the subject of interception or equipment interference?

    2. How broadly is "operation" defined? Might "preventing terrorism" be an operation? Might "stopping ISIS" be an operation?

    3. If thematic warrants are to be permitted, how will they be regulated to address the concerns raised by the Interception of Communications Commissioner and the Intelligence Services Commissioner?

80. Clause 188: National Security Notices - The extent of the powers contained with clause 188 on National Security Notices is far from clear. Our understanding is that it replaces the powers previously enshrined in the overly broad section 94 of the Telecommunications Act 1984. Some of those powers have purportedly now been made explicit in Part 6, Chapter 2 on bulk acquisition. Clause 188 presumably preserves the rest of them.

81. While clause 188 is somewhat more narrowly drawn than section 94, it still allows the Secretary of State to require a telecommunications operator to take "such specified steps" as she considers "necessary in the interests of national

[82] Zakharov v Russian Federation, [GC], No. 47142/06, 4 December 2015, paras. 259-267.

security." Section 94, in contrast, allowed the Secretary of State to make "directions of a general character . . . in the interests of national security." The fact that this old language purportedly permitted the bulk acquisition of communications data from service providers (now in Part 6, Chapter 2) raises serious questions as to what new form of surveillance, that we have not yet considered, might be permitted under clause 188.

82. Further, clause 188(4) states that the "main purpose" of a national security notice cannot be to "do something for which a warrant or authorisation is required under" the IP Bill. Does that mean a national security notice could replace a warrant or authorisation if that's the notice's subsidiary purpose? If so, that would again completely undermine effective judicial authorisation, among many other safeguards.

83. The Explanatory Notes clarify that "[i]n any circumstance where a notice would involve the acquisition of communications or data a warrant or authorization from the relevant part of this Act would always be required in parallel."[83] This is a stronger statement than the language in clause 188(4). If the Explanatory Note is correct, then the language of clause 188(4) should be amended to say as much.

84. Recommendations

    1. Clause 188(4)

        1. Delete: "the main purpose of which is"

        2. Amend to read: "But a national security notice may not require the taking of any steps to do something for which a warrant or authorisation is required under this Act. In any circumstance where a notice would involve the acquisition of communications or data a warrant or authorisation from the relevant part of this Act would always be required in parallel."

85. Questions

    1. Given that the language of clause 188 (National Security Notices) remains similar to section 94 of the Telecommunications Act 1984, what would prevent a major expansion of surveillance powers under clause 188, akin to the use of section 94 to acquire bulk communications data?

86. Judicial review - A major topic of the oral evidence presented to the Committee has been the parameters of the "judicial review" standard. This substantial debate demonstrates its meaning is far from clear. For that reason, if the intent is that the Judicial Commissioners shall have the power to fully and completely assess whether a warrant is necessary and proportionate, then any reference to a "judicial review" standard should be removed from the judicial authorisation provisions of the draft IP Bill.

83 Explanatory Notes, para. 429.

87. Recommendations[84]

1. Clause 19

    1. Subsection 19(1): delete "review the person's conclusions as to the following matters" and replace with "determine"

    2. Delete subsection 19(2)

2. Clause 90

    1. Subsection 90(1): delete "review the person's conclusions as to the following matters" and replace with "determine"

    2. Delete subsection 90(2)

3. Clause 109

    1. Subsection 109(1): delete "review the Secretary of State's conclusions as to the following matters" and replace with "determine"

    2. Delete subsection 109(2)

4. Clause 123

    1. Subsection 123(1): delete "review the Secretary of State's conclusions as to the following matters" and replace with "determine"

    2. Delete subsection 123(2)

5. Clause 138

    1. Subsection 138(1): delete "review the Secretary of State's conclusions on the following matters" and replace with "determine"

    2. Delete subsection 138(2)

6. Clause 155

    1. Subsection 155(1): delete "review the Secretary of State's conclusions on the following matters" and replace with "determine"

    2. Delete subsection 155(2)

88. Lack of an "examination" warrant for Bulk Personal Datasets (BPD) (Part 7) - Another confusing inconsistency in the Bill is the lack of a "targeted examination warrant" for information obtained through the collection of bulk personal datasets (Part 7).

89. An examination warrant is necessary when material intercepted via bulk interception (Clause 119) or obtained under bulk equipment interference (Clause 147) is to be searched using criteria that is "referable to an individual known to be in the British Islands."

84 These recommendations are intended to address only the judicial review standard. Throughout this submission we make other criticisms of the judicial authorisation process and bulk powers, for instance, which may necessitate other edits to the clauses referenced here.

90. But BPDs, which will also contain content referable to individuals in the British Islands,[85] can be accessed without targeted examination warrants.[86] The only protection provided is that the original warrant authorizing the acquisition of the BPD must also specify the "operational purposes" for which the data can be examined (Clauses 153(4) & 153(5), and Clauses 154(7) & 154(8)). Those operational purposes, however, can be extremely broad and are elsewhere in the Bill permitted to be "general purposes" (see, for example, Clause 140(5)).

91. Questions

    1. Why isn't an examination warrant required when Bulk Personal Datasets are searched using criteria that is "referable to an individual known to be in the British Islands"?

Is the legal framework such that CSPs (especially those based abroad) will be persuaded to comply?

92. While the CSPs are best positioned to answer this question, we note two important considerations.

93. First, by their nature many CSPs have an international presence. As such, they potentially can be subject to conflicting legal obligations imposed by multiple states – from the US and the UK, to Russia and China. How those conflicts should be resolved is the subject of significant ongoing discussion.[87] By including extraterritorial enforcement provisions in the draft IP Bill, the UK Government is sending a message to the world that any government is justified in reaching outside its borders to impose its will on services used by that government's citizens. The UK needs to think very carefully before setting this troubling precedent.

94. Second, in his report, David Anderson noted that certain US service providers might be more likely to comply with requests from the UK if they were authorised by a judge.[88] If US service providers might be re-assured by a UK system that includes US-like judicial authorisation, they will not be re-assured by this Bill. As we explain in more detail below, the judicial authorisation regime proposed in the draft IP Bill bears little resemblance to the US system.

Are concerns around accessing journalists', legally privileged and MPs' communications sufficiently addressed?

95. In this response Privacy International focuses on protections for journalists and legal privilege. However, we also note that the IP Bill contains no protection for

85 The definition of "personal data" within the Data Protection Act 1998 includes information that will likely fall in the definition of "content" as provided in Clause 193(6) of the IP Bill.

86 As we note elsewhere in this submission, we believe providing protections only to those in the British Islands is discriminatory, but if such protections are to exist they should at least be consistently applied across the IP Bill. We also have serious concerns about the collection of bulk personal datasets in the first instance, much less their examination.

87 See, for instance, the Internet & Jurisdiction Project, available at http://www.internetjurisdiction.net/.

88 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), at para. 11.19, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf.

MPs or members of sensitive professions, such as journalists, lawyers and others, in the context of bulk warrants.

96. Journalists - Clause 61 requires that a Judicial Commissioner authorise the acquisition of communications data for the purposes of identifying or confirming a source of journalistic information. Privacy International has some concerns about this provision.

97. First, Clause 61(1) (a) excludes intelligence services. This should be removed, as protections for journalists should apply to both law enforcement and the security services. No operational case has been made for this distinction.

98. Second, where a journalistic source is to be identified, the standard is higher than the ordinary necessary and proportionate test.[89] Clause 61 does not meet this stricter standard. While there is some mention of its development in the Codes of Practice, it would be of much greater benefit for the clarity of the protections that these standards be placed into the bill proper and not into secondary legislation.

99. Third, a source is narrowly defined in Clause 61(7) as "an individual who provides material intending the recipient to use it for the purposes of journalism or knowing that it is so likely to be used." In contrast, the Recommendation No. R (2000) 7 from the Council of Europe Committee of Ministers defines a source as "any person who provides information to a journalist".[90] No intent is required in the Council of Europe definition of a source, and so should not be included in the IP Bill.

100. Finally, judicial authorisation need only be sought if communications data is being obtained for the "purpose" of identifying or confirming a source (Clause 61(1)(a)). This suggests that if source is identified incidentally, no authorisation would be needed. This appears to be a rather broad loophole that, in addition to the lack of protections for journalists and sources in the bulk context, may significantly undermine what protections there are in the IP Bill.

101. Recommendation

1. Clause 61

    1. Subsection 1(a) delete "(other than an intelligence service)".

102. Questions

1. How would a test as to whether a person had provided material with the intention for it to be used, or knowledge that information is likely to be used for the purposes of journalism work in practice?

2. How would the incidental identification of a journalistic source be treated under the IP Bill?

89 See David Anderson report, A question of Trust, paragraph 5.49.

90 Recommendation No. R (2000) 7 of the Committee of Ministers to Member States on the Right of Journalists not to disclosure their sources of information, http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec(2000)007&expmem_EN.asp

103. Legal Privilege - The IP Bill fails, as RIPA did, to expressly protect legal professional privilege. While Schedule 6 of the IP Bill notes that Codes of Practice will be issued in respect of protections for communications data relating to a member of a profession which would regularly hold legally privileged or relevant confidential information, no further explanation of those protections are included.

104. In the interests of clarity, these protections should be laid down in primary legislation. They protections should apply to both content and communications data, and all forms of surveillance including interception, hacking, or obtaining targeted data from providers. A judge must approve any request to interfere with the privilege.

105. Recommendation:

    1. Make explicit recognition of legal professional privilege in the text of the IP Bill.

106. Question

    1. Why is there no explicit recognition of legal professional privilege in the Bill?

Are the powers sought workable and carefully defined?

107. While we recognise it is a difficult task, carefully defining the powers in the IP Bill is essential to preventing arbitrary and unlawful surveillance. Unfortunately, the current draft of the Bill contains a significant number of provisions that could benefit from more clarity and careful definition, which will also assist in the determination of whether the powers are workable.

Are the technological definitions accurate and meaningful (e.g. content vs communications data, internet connection records etc.)?

108. The technological definitions in the IP Bill raise a number of concerns. In answering this question we focus on the definitions we think are most problematic, including those for: interception; communications data; related communications data; content; telecommunications system, operator, etc. We address ICRs separately in response to the specific questions asked in the "Data Retention" section.

109. Interception (Clause 3) - We are concerned that the definition of interception does not accurately reflect the technical reality of how communications can and will be intercepted and processed.

110. Recently, the Government has advanced the argument that an interference with privacy only occurs when data is examined, or "read", by a person as opposed to a machine. We disagree with this position, as ECHR case law makes clear that the interference with privacy occurs at the time of the interception regardless of whether the data is ever "read" by a person.[91]

---

[91] See e.g. Amann v Switzerland [GC] ECHR 2000-II at §69 ("The Court reiterates that the storing by a public authority of information relating to an individual's private life amounts to an interference

111. The IP Bill, however, defines an interception as an act the effect of which is to "make some or all of the content of the communication available, at a relevant time, to a person who is not the sender or intended recipient of the communication." We question this reliance on making content available to a "person."

112. Surveillance can be undertaken entirely by systems, which can both collect the data and analyse it without the participation of a person. Indeed, we can imagine a scenario in which a surveillance system could analyse the content of a communication in real-time, delete any collected content in real-time, and feed the results of the analysis into an automated profile. At no point in such a scenario would a "person" be involved. Yet the scenario should most certainly be classified as an interception. The definition of interception in the IP Bill should not be construed, therefore, as failing to encompass situations in which a person, perhaps by design, never reads the content of an intercepted communication.

113. Communications Data (Clause 193(5)) – We have long had concerns about the definitions of communications data. We would like to remind the Committee that during the RIPA parliamentary debates there were extensive and detailed discussions around metadata that led to changes. Yet since 2000 the definitions have remained relatively stable, even as communications metadata has dramatically grown in scope and volume, and parliamentary committees have repeatedly noted concerns around the increased sensitivity of metadata. Nonetheless, the only noted change in the definition in the IP Bill is the creation of a new form of metadata for capture, the ICR.

114. In the IP Bill the definition of communications data relies on the definitions of "entity data" (data about a person or thing) and "events data" (data about activities). Communications data is entity or events data that is or may be in possession by a telecommunications operator or available directly from a telecommunication system, but does not include content.

115. The definitions of entity and events data are too vague and fail to take into account the distinctions that may arise in the types of data generated by modern technology. For instance, data about a phone call over landline (e.g. two BT numbers shared a connection for 13 minutes) is vastly different than each 'event' within a chat session (e.g. two subscribers at locations X and Y interacted 97 times over a 13 minute period — sometimes with longer gaps and larger messages, other times with fast messaging indicating agreement or disagreement).

116. Accordingly, the definition of communications data in clause 193(5) is also too vague, but not only because of its reliance on the definitions of entities and events. We also do not understand how communications data may be

---

within the meaning of Article 8. The subsequent use of the stored information has no bearing on that finding.")

"comprised in" a communication, but not be content. We are concerned that this would give rise to a situation where there is interception of content in order to reveal communications data. Further, we believe the reference in clause 193(5) to data that is "for the purposes of a telecommunication system" is too broad, and that this should be limited to "for the purposes of a telecommunication system to deliver the communication".

117. Related Communications Data (Clause 3(7)): The bill creates a new version of the definition of 'related communications data' in clause 12(6). This is data collected through interception that relates to the communication, or is comprised in, included as part of, attached to or logically associated with the communication; or it is data that is separable from content that would not reveal the meaning of the communication. If content is defined based on the conveyance of meaning, it is unknown to us how 'related communications data' could be part of content in the first place. The Home Office needs to be clearer on how these definitions interact with the technical specifications of communications. For instance, intercepting at an ISP on port 25 will give access to a communication (e.g. an email) but the "content" (email body) will include the communications data of the email (email headers).

118. Content (Clause 193(6)): The definition of content hinges on the 'meaning of the communication'. We believe greater clarity is required on the constitution of a communication, as applied to all forms of modern and emerging methods of communications. In particular, it is not clear to us, whether an entire communication or just some portion of the communication involves meaning. For instance, an intercepted email does not necessarily fall entirely within "content," but rather only the portion that conveys the meaning, whereas the rest of the email could be defined as communications data or related communications data.

119. The content definition also includes two exceptions. The first, in 193(6a), excludes from content "web browsing" information. We are confused as to why a "future proofed" legislation has such a highly specific reference to web browsing. Is web browsing only meant to encompass internet connections created when "browsing" through a "browser", and not through an App on a mobile or tablet device? That is, is it non-content when someone is browsing on BBC or Al Jazeera, but it is content when someone uses the BBC or Al Jazeera News apps for Android or iOS?

120. The second exception, in 193(6b), excludes from the definition of content any 'meaning' arising from the fact of the communication. The very ways in which we communicate today reveals the content of our interactions. Even how our devices interact includes an indication of sensitive personal activity. The meaning of a communication can sometimes be discerned just from the fact that an interaction took place. For instance, the meaning of a call to an abuse help-line or browsing the website of a support group is relatively clear. Yet 6(b) explicitly excludes this from content, and thereby ensures weak protections and safeguards for its access. This exception is an admission by the government that they view communications data as sometimes quite revelatory but they nonetheless insist that authorities must be able to access this 'meaning' with

fewer safeguards.

121. Telecommunications System, Operator, Service etc (Clause 193): The definitions of telecommunications operators, services and systems lack sufficient exclusivity. The ambiguity in the terms means that a given communications provider could fit into different definitions simultaneously. An Internet Service Provider like Zen Internet or AAISP could be a telecommunication system (as they have wires and cables), telecommunication service (as they deliver services), and telecommunications operator. Equally, Facebook could be any of these because the definition of system is based on "facilitation" of the communication. This ambiguity might reflect the intention that the Bill be as technology neutral as possible. But it gives too much discretion to the Secretary of State in deciding when a service provider fits in each definition. This creates regulatory uncertainty.

Does the draft Bill adequately explain the types of activity that could be undertaken under these powers?

122. No. As noted above, the definitions at the heart of some of the powers, like interception, are unclear. Equipment interference is also not well delineated. For instance, how equipment might be interfered with – the method that could be used to obtain the communications, private information and equipment data listed in clause 81 – is never described. This leaves us guessing at what types of activities might be carried out, especially under a power as seemingly broad as equipment interference. Similarly, bulk personal datasets are so broadly defined that it is not clear what limits, if any, there are on the data that might be obtained from public or private sources.

123. Furthermore, many of the powers allow for the taking of "necessary" steps that are not explicitly authorised in the warrant. For example, clause 12(5)(a)(i) permits conduct that is necessary to carry out what is expressly authorised in the warrant, but does not specify or in any way limit that conduct.

124. The Bill also places a number of open-ended obligations on other parties to assist, facilitate or implement many of the powers (such as Clauses 29 and 31). Again, little or no detail is given regarding the assistance that may be required - or more importantly what activities are prohibited. Only clause 189 provides some examples, including the removal of electronic protection, which are more troubling than reassuring.

125. Finally, as noted in paragraphs 80 to 85 above, clause 188 appears to be a catch-all provision that if not narrowed could permit activities that we cannot even imagine at this time.

126. Questions

1. What activities fall within the definitions of interception and equipment interference? What is prohibited?

2. What types of bulk personal datasets may be collected from public and private sources?

3. What may telecommunications services and operators be asked to do in

order to assist in carrying out a warrant for any of the enumerated powers?

Is the wording of the powers sustainable in the light of rapidly evolving technologies and user behaviours?

127. As technology continues to evolve into every facet of life and individuals adapt their behaviours to engage with these changes, it is crucial that legislation keeps pace with these advances. The IP Bill in its current form offers little concrete detail of how the provisions will be implemented (as described in the previous section). The vagueness of some of the wording runs the risk that surveillance powers will be used to conduct activities not currently envisioned. The non-technical language used to describe some of the powers threatens to creep into the realm of fantasy with its lack of technological underpinning. In this regard, it is very difficult to assess how the IP Bill will apply to current technology, let alone new technologies.

128. Rather than using ambiguous terminology, it would be preferable to use more specific technology-oriented language and apply a review process to the legislation on a regular basis. This would allow for greater specificity in the language of the Bill, while also allowing amendments at reasonably regular intervals to accommodate changes in user behaviour and the technological climate.

Overall is the Bill future-proofed as it stands?

129. Technology changes rapidly. Yet technology-neutral legislation that attempts to accommodate that change can also pose serious risks to privacy and security as technological development and innovation dramatically transform the scope of prior, vaguely worded powers.

130. We are often not equipped to understand how these powers will apply today, much less to likely technologies of tomorrow. Parliamentary debates around RIPA did not anticipate popular webmail providers based in foreign jurisdictions, extensive location data collected by devices and networks, and broad-scale interception capabilities. All these technologies appeared shortly after RIPA and fuelled surveillance capabilities for at least the next ten years.

131. We would prefer surveillance legislation that errs on the side of being too specific. This way Parliament can understand how it applies and assess the costs, benefits, and implications.

132. When the Joint Committee reviewed the draft Communications Data Bill, the Committee found that the order-making powers given to the Secretary of State were too great. This was, the Home Office argued at the time, essential to future-proofing the legislation. That is, as technologies changed, the Secretary of State did not want to seek new authorisation from Parliament to apply the powers to each new technology.

133. We believe that the IP Bill repeats this mistake. It contains vague and ill-defined terms, and places obligations on telecommunication operators and others, in the UK and abroad, to provide and, when necessary, generate data, to retain data, and to enable interception and interference, in targeted and bulk manners. The concern is that these demands placed today will shape and limit

the kinds of services developed tomorrow.

134. One possible direction of innovation is the Internet of Things. Soon many more devices, ranging from refrigerators to thermostats, cars to toasters, will be recording and communicating information about us, and not necessarily to us. These devices can be interfered with, their communications intercepted and their data shared. They may even be co-opted to gather more information. We must therefore not debate the IP Bill as though it applies only to mobile phones and laptops. We may soon be surrounded by and wearing technologies that can be used by governments and others, both in the UK and abroad, to place us under surveillance.

135. As a small reminder of history, within weeks of RIPA being given Royal Assent, the Home Office was actively pursuing new powers of data retention. A year and a half later, voluntary data retention was law. Before long, mass collection and interception exercises were in place. Six years later the Home Office was developing formal policy to support mass collection of communications data of over the top services. This current draft Bill not the last piece of legislation for new powers that will be introduced by the Home Office in the foreseeable future.

136. Recommendation

    1. Parliament should debate the extent of powers it is granting to authorities, and how these powers are being used, on a regular basis.

137. Questions

    1. How will Parliamentarians be informed about the nature of changing telecommunications technologies and their impact on the law?

    2. What assessments have been made to understand how these powers are used with respect to new and emerging technologies like the Internet of Things?

Are the powers sought sufficiently supervised?

138. While some progress is made in the IP Bill through the introduction of the Judicial Commissioner, it nonetheless leaves significant powers in the hands of the Secretary of State with no, or insufficient supervision. Like the Draft Communications Data Bill, much of the IP Bill requires secondary actions, whether regulation or subsequent actions by the Secretary of State.

139. In our review of the various capabilities granted but not specifically established in the Bill, Secretary of State may, inter alia:

    1. choose to enforce a duty upon telecommunications operators through civil proceedings (clause 31(8));

    2. establish, maintain and operate a filter and related arrangements (Clause 51), though in consultation with the Investigatory Powers Commissioner (IPC) as to the principles of the basis of the arrangements; and transfer these functions to any other public authority (Clause 67);

    3. modify, by regulations, the relevant public authorities and designated senior

officers and the authorities of those departments and agencies in Schedule 4 (Clause 55), in consultation with the IPC and the public authority;

4. require, by notice, a telecommunications operator to retain relevant communications data (Clause 71(1)), by giving, or publishing, it in such manner as he or she considers appropriate (Clause 71(6)); and

5. require, by notice, a telecommunications operator to take any further steps that the Secretary of State considers necessary in the interest of national security, that may in particular require the operator to carry out any conduct to facilitate anything done by an intelligence service or dealing with an emergency, or provide services or facilities to do so (Clause 188).

140. One of the key concerns is the maintenance of technical capability provision (Clause 189). The Secretary of State can require, inter alia, the provision of facilities or services of a specified description and the removal of electronic protection applied by a relevant operator. Though the Secretary of State must consult with certain people, including the Technical Advisory Board and persons likely to be subject to the obligations, such consultation is only a weak check on the Secretary of State's authority.

141. Furthermore, we question the extent to which modifications and extensions can be made to warrants without adequate supervision or judicial authorisation (Clauses 96, 97, 114, 128, 143, 162.) For example, names or descriptions can be added to targeted interception warrants without authorisation or other involvement of Judicial Commissioners (Clause 26).

142. We are also concerned that the IPC can approve warrants that were rejected by Judicial Commissioners without any clear follow-up process of review.

143. Question:

1. What powers will the Technical Advisory Board have to demand supervision over specific capabilities and how they are deployed?

2. If the above powers mentioned in this section are to remain in the IP Bill (and we argue a number of them should not), why couldn't the powers be transferred from the Secretary of State to the Judicial Commissioners?

Is the authorisation process appropriate?

144. No. Privacy International submits that the authorisation process articulated in the draft IP Bill is not appropriate. Authorisation must entail fully independent judicial authorisation, where judges have unfettered discretion to determine if a warrant sought by the executive is necessary and proportionate. The draft Bill, by contrast, preserves the power of the Secretary of State to issue warrants. While it permits Judicial Commissioners to "approve" this decision, it places significant limitations on the scrutiny they can exercise in reviewing the warrant (see in particular Clauses 19-21, 90, 109, 123, 138, 155). And in some instances, it does not require any form of judicial approval at all (see Clauses 26, 46, 71).

145. In deciding whether to approve the issuance of a warrant, a Judicial

Commissioner is to apply the "judicial review" standard. The precise contours of this standard are subject to some debate and we recognise that multiple interpretations have been presented to the Committee. Our understanding, which is also articulated by Liberty, is that this standard constrains review to procedural propriety and prohibits examination of the merits.[92] If the intent is for Judicial Commissioners to have unrestricted authority to assess whether a warrant is necessary and proportionate, then any reference to a "judicial review" standard should be stripped from the judicial authorisation provisions of the draft IP Bill. The fix is simple – just delete sub-section (2) from each of the clauses describing "Approval of warrants by Judicial Commissioners" and slightly reword sub-section (1), as we propose above in paragraph 87.

146. Judicial authorisation, even in the weak form expressed in the draft IP Bill, is not required for the Government to acquire communications data, issue data retention notices or modify interception warrants, all of which interfere with the right to privacy. In our prior submission to the Joint Committee on Human Rights, we noted that the lack of judicial authorisation for such powers might fall short of requirements under international human rights law.[93]

147. We also have serious concerns about whether any authorisation process – judicial or not – is workable in the bulk context. The sheer breadth of a bulk warrant inherently frustrates substantive review of its necessity and proportionality. As we also submitted to the Joint Committee on Human Rights, bulk warrants need not "specify or target the communications, data or equipment of a particular person, premises or even an organisation."[94] They need only "state the operational purposes for which data need to be obtained, and the IP Bill expressly notes that these can be 'general purposes'" (see Clauses 111(4), 125(4), 140(5)). This lack of specificity – *i.e.* the absence of any assessment of suspicion – is intrinsically disproportionate and runs afoul of explicit guidance from the ECtHR.[95]

148. It may be useful to look at the American context where judicial authorisation is the norm. Under the US Wiretap Act, the Attorney General "may authorize an application to a Federal judge for . . . an order . . . approving the interception of wire or oral communications".[96] The judge may only approve a wiretap order if he or she "determines on the basis of the facts submitted by the applicant" that, *inter alia*: (a) there is probable clause for belief that an individual is

---

92 The Courts and Tribunals Judiciary has also adopted this interpretation on their website:

> [J]udicial reviews are a challenge to the way in which a decision has been made, rather than the rights and wrongs of the conclusion reached. It is not really concerned with the conclusions of that process and whether those were "right", as long as the right procedures have been followed. The court will not substitute what it thinks is the "correct" decision.

Courts and Tribunals Judiciary, "Judicial review", https://www.judiciary.gov.uk/you-and-the-judiciary/judicial-review/.

93 Joint Committee on Human Rights Submission, paras. 51-56.

94 *Id*. at para. 20.

95 *Id*. at paras. 21-22 (discussing Gillan and Quinton v United Kingdom and S and Marper v. United Kingdom).

96 18 U.S.C. §§ 2510-2522.

committing, has committed, or is about to commit a particular offense enumerated in the Act; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[97]

149. In the US, the notion of independent judicial authorisation of warrants is sacrosanct and for good reason. In the words of the US Supreme Court in the landmark "Keith" case:

> "Inherent in the concept of a warrant is its issuance by a "neutral and detached magistrate." . . . The [Constitution] does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility are to enforce the laws, to investigate, and to prosecute. But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursing their tasks. The historical judgment . . . is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."[98]

150. Importantly, the Court continued that this risk is particularly acute in the national security context "because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."[99]

151. The US is hardly unique in this respect. In fact, the passage of the draft IP Bill with the current authorisation process would continue to make the UK an outlier among other democratic countries and the only state in the Five Eyes Alliance (which also includes the US, Australia, Canada and New Zealand) that does not vest the power to approve surveillance activities in the judiciary.[100] It would also fly in the face of Anderson's explicit recommendation that "the warrant-issuing powers currently vested in the Secretary of State . . . be exercised only by Judicial Commissioners".[101] For all of these reasons, we believe the authorisation process currently proposed in the draft IP Bill is

---

97 *Id*. at § 2518. These requirements are enshrined in Rule 41 of the Federal Rules of Criminal Procedure with respect to "Search and Seizure" more generally.

98 United States v. United States District Court for the Eastern District of Michigan ("the Keith case"), 407 U.S. 297, 316-17 (1972). In the Keith case, the Supreme Court unanimously held that the government was obligated to obtain a warrant before conducting electronic surveillance even for the purposes of domestic threats to national security.

99 *Id*. at 320.

100 Liberty, "Safe and Sound", https://www.liberty-human-rights.org.uk/campaigning/safe-and-sound.

101 Anderson Report, para. 14.95(b); *see also id*. at Recommendation 22 ("Specific interception warrants, combined warrants, bulk interception warrants and bulk communications data warrants should be issued and renewed only on the authority of a Judicial Commissioner."). The RUSI Report recommended a modified regime whereby warrants "sought for a purpose relating to the detection or prevention of serious and organised crime . . . should always be be authorised by a judicial commissioner" whereas warrants "sought for purposes relating to national security . . . be authorised by the secretary of state subject to judicial review by a judicial commissioner." RUSI Report, Recommendation 10.

inappropriate.

152. Recommendation:

1. Vest the power to issue warrants in Judicial Commissioners or, in the alternative, remove the "judicial review" standard in the approval clauses as described in paragraph 87 above.

2. Ensure prior judicial authorisation for the acquisition of communications data and the modification of warrants.

153. Question

1. In the context of bulk powers, how can necessity and proportionality be judged in the authorization process?

Will the oversight bodies be able adequately to scrutinise their operation?

154. Clauses 180 and 181 add to RIPA's provisions on the role of the Investigatory Powers Tribunal (IPT). The IPT has operated as a secret court and "sits outside the regular structures of British justice"[102]. Notably, both the Anderson and RUSI reviews called for an overhaul of the IPT.[103] The draft Bill does not address the flaws of the IPT, although clause 180 does encouragingly allow an appeal to be made to a UK court. Below, we propose some specific reforms of the IPT and this new right of appeal in response to the question, "Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?"

155. The establishment of a new IP Commissioner, which would replace the Interception of Communications Commissioner, the Chief Surveillance Commissioner, and the Intelligence Services Commissioner, is a welcome step.

156. Clause 167(1) states that the Prime Minister will appoint the IP Commissioner. This is inappropriate as it means that the IP Commissioner's role will not be properly independent from the Executive. The Judicial Appointments Commission (JAC) should appoint the IP Commissioner and the related Judicial Commissioner, which will give both the public and Parliament greater confidence that this vital role is independent.

157. Ensuring an appropriate level of resourcing for the IP Commission will be crucial in enabling the public and Parliament to ensure surveillance powers are properly used. We understand that the current proposal is to appoint one IP Commissioner and only seven Judicial Commissioners. In order to provide an appropriate level of oversight, there needs to be a much more substantial body of Judicial Commissioners.

---

102 Murphy, C. C. & Simonsen, N. (5 November 2015) Interception, Authorisation and Redress in the Draft Investigatory Powers Bill, *UK Human Rights Blog* [Online], available at http://ukhumanrightsblog.com/2015/11/05/interception-authorisation-and-redress-in-the-draft-investigatory-powers-bill/ [Accessed 15 December 2015]

103 *See* Anderson Report, paras. 14.103-08; RUSI Report, Recommendations 11-16.

158. While we welcome the three roles that need to be carried out, namely authorisation, inspection, and informing the public and Parliament about "the need for and use of investigatory powers", there will be an irresolvable conflict of interest if the same body both authorises and then also somehow independently reviews those authorisations to ensure they were lawful and carried out properly. In order to engender public trust, oversight of the use of surveillance must be separate from authorisation of surveillance.

159. The draft Bill has very little to say about redress. While Clause 171(1) does state that the new IP Commissioner "must inform a person of any relevant error", Clause 171(2) sets a very high bar, in that both the IP Commissioner and IPT must agree that it is a "serious" error and that it is in the public interest for that person to be informed of the error. What is considered "serious" needs further explanation, and what the public interest test will be is not clearly defined. We suggest deleting both requirements and allowing the IP Commissioner to reveal any error in the interest of transparency and public accountability.

160. In our prior submission to the Joint Committee on Human Rights, we discussed how the draft IP Bill contains a range of provisions that prohibit and, in some cases, criminalise unauthorised disclosure (see Clauses 43-44, 66, 77, 102, 133, 148, and 190).[104] We noted that these gagging clauses, by prohibiting notification of surveillance measures, might be violative of the ECHR. If individuals are unaware that a public authority has obtained their data, they will not be able to seek redress.

161. Recommendations:

    1. Clause 167 - Subsection 167(1) – delete "Prime Minister" and replace with "Judicial Appointments Commission".

    2. Remove the "serious error" requirement and "public interest" test from Clause 171 and delete clause 171(4).

    3. Add language to provide further detail about how the IPT will be transparent and accountable, as we suggest in paragraph 295.

    4. Soften strict non-disclosure clauses by permitting a public interest defence for unauthorised disclosure and permitting service providers, with limited exception, to notify individuals.

What ability will Parliament and the public have to check and raise concerns about the use of these powers?

162. Privacy International is concerned that surveillance oversight bodies often operate at a disadvantage. For instance, an advanced understanding of technology is required to comprehend analytical capabilities, modern interception capacities, and the security implications of hacking activities. The oversight bodies mentioned in the IP Bill do not always have that expertise.

163. Current oversight also relies too heavily on self-reporting by the relevant

104 Joint Committee on Human Rights Submission, paras. 61-68.

investigatory agencies. Parliamentary oversight committees and former senior government officials have been surprised by the use of some powers, and many of these powers were only admitted as a side-effect of an investigation and not necessarily through simple reporting, e.g. the use of bulk personal data sets.

164. Within the IP Bill, the IPC will report on a yearly basis to the Prime Minister, and the Prime Minister must publish the report and lay a copy before Parliament (Clause 174(6)). We are concerned that the Prime Minister can exclude from publication any part of a report if, in the opinion of the Prime Minister, the publication would be contrary to the i) public interest, or ii) prejudicial to national security, prevention or detection of serious crime, or the economic well-being of the United Kingdom. While we recognise there will be some legitimate reasons to withhold certain operational information, the presumption should be in favour of transparency. It thus seems highly unlikely that the public interest will weigh in favour of redaction unless there is also a threat to national security or the prevention and detection of serious crime. The language of clause 174(6) could therefore be tightened to allow for more transparency.

165. In order to reduce reliance on whistleblowers, we suggest softening the offence of making an unauthorised disclosure in clauses 43, 66 and 102 as there seems to be little opportunity for any disclosure beyond the mere number of warrants received (see paragraph 160). In particular with regards to clause 102 within equipment interference, there are no authorised disclosures, and this prevents companies from openly discussing how (bulk and targeted) equipment interference warrants may interfere with their service delivery, the implications of the imposition of the warrant, and any steps taken. This further stems the public's ability to understand how the powers are used and will adversely affect global cybersecurity.

166. Recommendation:

1. We believe that the public needs more information on how investigatory powers and capabilities have been developed and used.

167. Questions:

1. How will the Secretary of State and Parliament ensure that the oversight bodies have sufficient independent technological understanding?

2. How will the oversight bodies regularly be made aware of the investigatory capabilities that are being developed and deployed?

3. Why is there no ability of operators and services to notify customers of the receipt of a warrant or other notice if such notification would not interfere with necessary secrecy?

4. Why are transparency reports limited to only the numbers of warrants received?

5. Why does the IPC report to the Prime Minister and not directly to Parliament?

Specific questions

General

To what extent is it necessary for (a) the security and intelligence services and (b) law enforcement to have access to investigatory powers such as those contained in the Draft Investigatory Powers Bill?

168. We respectfully refer the Committee to our responses to the questions:
    1. "Has the case been made, both for the new powers and for the restated and clarified existing powers?" (paragraphs 13-37)
    2. "Are the power compatible with the Human Rights Act and ECHR?" (paragraphs 38-58)
    3. "Is the requirement that they be exercised only when necessary and proportionate fully addressed?" (paragraphs 59-64)

169. In those responses, we articulated why the Government has failed to demonstrate the operational and legal (under the "necessary and proportionate" test) necessity for either the security and intelligence services or law enforcement to have access to the following investigatory powers:
    1. bulk warrants
    2. acquisition of ICRs as part of communications data
    3. data retention
    4. equipment interference
    5. thematic warrants

Are there any additional investigatory powers that security and intelligence services or law enforcement agencies should have which are not included in the draft Bill?

170. While we do not comment on whether the security and intelligence services or law enforcement need any powers that are not already in the IP Bill, we would like to reinforce that any powers that are claimed should be made clear and foreseeable in statute, as is required by the rule of law and so that any interference with privacy will be "in accordance with law". Significant new powers must not be brought about through the reinterpretation of the IP Bill or within Codes of Practice. If a new power is sought which is not reasonably foreseeable within the existing law, it must be authorised through a change to the primary legislation. This will allow a legislative debate about the power, a clear case to be made for their use, and further explanation of how the new power is necessary and proportionate.

171. Unfortunately, the IP Commissioner is not permitted to review "the exercise of any function of a relevant Minister to make or modify subordinate legislation," (Clause 169(4)(a)). If the IP Commissioner is not reviewing such power, who will to ensure it does not result in a significant change to the primary legislation? The answer is currently missing from the draft IP Bill.

172. Questions:

1. What is the process for any new power or re-interpretation of existing powers to be debated, passed and communicated to the public?

2. How does the IP Bill stop another situation like the one described by Anderson in his review of RIPA and his opening lines of A Question of Trust: "RIPA, obscure since its inception, has been patched up so many times as to make it incomprehensible to all but a tiny band of initiates. A multitude of alternative powers, some of them without statutory safeguards, confuse the picture further. This state of affairs is undemocratic, unnecessary and – in the long run – intolerable"?

Are the new offences proposed in the draft Bill necessary? Are the suggested punishments appropriate?

173. Clause 2 sets out the offence of unlawful interception and clause 6 sets out the penalties. In particular, subsection 6(b) identifies a penalty that "must not exceed £50,000". Privacy International does not have a view of the appropriate monetary penalty, but as this is a serious offence, we do believe that there should be serious commensurate penalties.

174. Clause 8 sets out the offence of unlawfully obtaining communications data. While we agree it is correct that this is an offence, again we do not have a view on what the appropriate punishment should be.

175. As discussed in paragraph 160 the draft IP Bill contains a range of provisions that prohibit and, in some cases, criminalise unauthorised disclosure (see Clauses 43-44, 66, 77, 102, 133, 148, and 190).[105]

176. Privacy International believes it is inappropriate to ban and make criminal all forms of disclosure. There are some circumstances under which telecommunications operators and services should be able to notify their customers that their personal information has been shared with the state. The current prohibitions are both potentially violative of the ECHR and run counter to the purported aim of the draft Bill to create greater transparency. While it might not be appropriate for all operational details to be published, high-level information should be published about the types of warrants and notices that are being served on telecommunications providers.

177. Recommendations

    1. Soften strict non-disclosure clauses by permitting a public interest defence for unauthorised disclosure and permitting CSPs, with limited exception, to notify individuals.

Interception

Are there sufficient operational justifications for undertaking (a) targeted and (b) bulk interception?

178. We respectfully refer the Committee to our response to the question:

    1. "Has the case been made, both for the new powers and for the restated and

105 Joint Committee on Human Rights Submission, paras. 61-68.

clarified existing powers?" (paragraphs 13-37)

179. In that response, we articulated why the Government has failed to make a compelling operational case for undertaking bulk interception. We also detailed how the Government has similarly failed to make a compelling operational case for expanding targeted interception to include the use of "thematic warrants".

Are the proposed authorisation processes for such interception activities appropriate? Is the proposed process for authorising urgent warrants workable?

180. In terms of whether the proposed authorisation processes for interception activities are appropriate, we respectfully refer the Committee to our response to the question:

1. "Is the authorisation process appropriate?" (paragraphs 144-153)

181. In that response, we explain why the authorisation process articulated in the draft IP Bill for all proposed powers, including interception activities, is not appropriate. For similar reasons, we also submit that the proposed process for authorising urgent warrants is, in general terms, not workable.

182. The urgent warrant authorisation process is also problematic for three additional reasons. First, the term "urgent" is not defined anywhere in the draft IP Bill and could therefore be interpreted to encompass a wide array of circumstances. By way of comparison, the US Wiretap Act, which regulates the interception of wire and electronic communications, strictly limits "urgent" interception – *i.e.* without prior judicial authorisation – to the following "emergency situations": (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime.[106] We urge the Committee to consider defining "urgent" to a similar set of limited and specific circumstances.

183. Second, the urgent warrant authorisation process requires the Secretary of State to inform a Judicial Commissioner that such a warrant has been issued but does not indicate the timeframe in which this notification is to occur (Clauses 20(2), 91(2), 156(2)). As another point of comparison, the US Wiretap Act requires that where an urgent warrant is issued, "an application for an order approving the interception" must be made to a judge "within forty-eight hours after the interception has occurred".[107] In contrast, the draft IP Bill provides that a Judicial Commissioner has five "working" days to review the issuance of the warrant. Others have argued that five days is too long of a timeframe.[108] We note here that five "working" days can potentially elongate

106 18 U.S.C. § 2518(7)(a).
107 *Id*. at § 2518(7)(b).
108 *See, e.g.*, The Bar Council, "Bar Council comments on Draft Investigatory Powers Bill", 5 Nov. 2015, http://www.barcouncil.org.uk/media-centre/news-and-press-releases/2015/november/bar-council-comments-on-draft-investigatory-powers-bill/ ("As all lawyers know, there is a duty judge available through the Royal Courts of Justice 24 hours a day. There is no reason why such provision could not be made available in cases where investigatory powers are being sought.").

that timeframe even further. As an example, a warrant issued on Thursday, March 24 2016 would not have to be approved until over one week later, on Monday, 4 April 2016, taking into account weekends and bank holidays. The lack of a specific timeframe for notifying a Judicial Commissioner combined with the long timeframe for review creates the risk that unlawful urgent warrants may, in practice, operate for inappropriately long periods of time before they are struck down.

184. Finally, we note that the urgent warrant authorisation process provides that where a Judicial Commissioner refuses to approve a warrant, he may but is not directed to order that the material obtained under the warrant be destroyed (Clauses 21(3), 92(3), 157(3)). Indeed, he may simply "impose conditions as to the use or retention" of the material. We question why it should ever be permissible for the Government to use or retain material that was unlawfully acquired and therefore urge the Committee to consider requiring destruction of the material in such circumstances.

185. Recommendations:[109]

1. Define the term "urgent" as used in Clauses 20, 91 and 156.

2. Provide a timeframe within which the Secretary of State must inform a Judicial Officer that an urgent warrant has been issued in Clauses 20(2), 91(2) and 157(2).

3. Provide a shorter timeframe than five "working" days within which a Judicial Commissioner must review the issuance of an urgent warrant.

4. Change the word "may" to "must" in Clauses 21(3), 92(3) and 157(3). Delete Clauses 21(3)(b), 92(3)(c) and 157(3)(b).

Are the proposed safeguards sufficient for the secure retention of material obtained from interception?

186. Intercepted data is highly sensitive. Large organisations often face problems in securing retained information, particularly valuable information that is to be accessed by many users. In a modern society where physical storage devices have dramatically dropped in price, we are too slowly realising that the limitation on generation, collection, and retention of information involves costs other those associated with mere storage. The various data breaches over the years, including the recent breaches of government agencies and telecommunications companies should give us pause (see paragraph 234 for more details).

187. Even systems designed to detect intrusions and prevent them can themselves be corrupted.[110] Given their access to data, such systems are an extremely

[109] While making these recommendations, we maintain the criticisms of the underlying powers that we make elsewhere in this submission which in some cases might dictate the complete removal of certain referenced clauses.

[110] See Steve Ragan, "Researcher discloses zero-day vulnerability in FireEye," CSO Online (6 Sept.

attractive target for malicious third parties.

188. The IP Bill contains no details regarding how information in storage is to be made "secure." At the very least, the Bill should specify the minimum technical requirements for securing retained data, and describe how any breaches will be addressed and revealed to oversight bodies and the public.

189. Recommendations

1. Include detailed provisions describing how retained data will be secured.

2. Include a mechanism by which oversight bodies and the public will be informed of breaches.

How well does the current process under Mutual Legal Assistance Treaties (MLATs) work for the acquisition of communications data?

190. Looking at the regime between the UK and the US and taking the example of the UK as the requesting party, the Mutual Legal Assistance (MLA) process to obtain content data currently functions as follows: the UK sends a request for communications content data stored by a US company to the US Department of Justice (DOJ) Office of International Affairs (OIA). OIA works with the UK to ensure the request satisfies US legal standards and then works with a US Attorney to send the request to the District Court. The judge reviews the request and grants it, or sends it back to OIA for further iterations with the requesting country. If granted, the request goes to the company, which sends a response to OIA, which checks the response and in turn sends the response to the UK.[111]

191. Notably, this process only applies to requests for content data; companies have discretion about how to respond to foreign requests for communications data.

192. The IP Bill currently contains a proposed mutual assistance warrant (Clause 12) through which the UK will provide assistance in intercepting communications where required by an MLAT. Clause 39 provides for a separate authorisation for the interception of communications in accordance with overseas requests. Privacy International is unclear as to how these two clauses interact (Clause 12 and Clause 39) and encourages members of the Committee to seek clarification from the Home Office on this point.

193. When it comes to communications data, the IP Bill provides no specific procedure for the acquisition of such data under an MLAT. Instead, Clause 69 specifically notes that acquisition of communications data power has an extra-territorial application, by noting that an authorisation to obtain communications data may relate to persons or telecommunications providers outside the UK.

194. This provision is of significant concern, particularly in light of the fact

---

2015), available at: http://www.csoonline.com/article/2980937/vulnerabilities/researcher-discloses-zero-day-vulnerability-in-fireeye.html

111 Swire, Peter, and Hemmings, Justin. "Re-Engineering the Mutual Legal Assistance Treaty Process." NYU Law and PLSC Conferences. 14 May 2015.

communications data authorisations may be issued without judicial approval. We address the problems raised by extraterritorial powers more generally in paragraphs 93 to 94, and in response to the following question.

195. Question:

1. How do the mutual legal assistance warrants described in Clause 12 and Clause 39 interact in connection with an overseas request for interception assistance? Does Clause 39 permit a telecommunications service to respond to an MLAT request even if a warrant is not issued under Clause 12?

What will be the effect of the extra-territorial application of the provisions on communications data in the draft Bill?

196. Clause 69 makes foreign telecommunications operators subject to the UK's power to acquire communications data. While clause 69(4) provides potential exemptions, based on the requirements and restrictions on data acquisition in operators' own countries, placing such obligations on service providers in the first place sets a bad precedent for the rest of the world, as discussed above in paragraphs 93 to 94.

197. Clause 79(2) asks foreign telecommunications providers to retain communications data. Unlike in Clause 69, there is no obligation to "comply", only a "duty to have regard to the requirement or restriction" regarding data retention. This puts an ambiguous responsibility on foreign companies. It will also reduce customer trust in these companies, as the customers will not know whether their service provider is complying with retention requests or not. The obligation, whether to comply or to have "regard" should be completely removed from the Bill.

198. Placing extraterritorial obligations on companies can have other negative consequences. For example, Google withdrew their operations from China[112] based on the Chinese government placing similar obligations on technology companies.

199. As discussed in paragraph 94, foreign companies are more likely to comply with requests if they are authorised by a judge.[113] It would set a very worrying international precedent if foreign companies were to hand over their customers' data based on the request of a UK politician. Should UK companies ever be required to hand over their customers' data based on a warrant approved by the Chinese government?

200. The recent case of WhatsApp being shut down across Brazil, because they were unable to comply with an order to place wiretap requests on some customer accounts, highlights the problem of placing unreasonable obligations on a company to provide customers' personal data to a foreign government.[114]

---

112 Criticism and regret in China over Google, *BBC News* [Online] http://news.bbc.co.uk/1/hi/world/asia-pacific/8583006.stme

113 David Anderson, *A Question of Trust: Report of the Investigatory Powers Review* (June 2015), at para. 11.19, available at https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Web-Accessible1.pdf

114 Goel, V, and Sreeharsha, V. Brazil Restores WhatsApp Service After Brief Blockade Over Wiretap

201. Recommendations

1. Delete clauses 69 and 79

Communications Data

Are the definitions of content and communications data (including the distinction between 'entities' and 'events') sufficiently clear and practical for the purposes of accessing such data?

202. As we state above, we have difficulty understanding and parsing these definitions. Please see our response to the question, "Are the technological definitions accurate and meaningful (e.g. content vs communications data, ICRs etc.)?"

Does the draft Bill allow the appropriate organisations, and people within those organisations, access to communications data?

203. Schedule 4 of the draft Bill lists the public authorities that will be able to access communications data. However, Clause 55(2a) enables the Secretary of State to add to or remove public authorities from this list. The circumstances under which changes will be made needs to be set out, as should the mechanisms for consulting and notifying the public of any changes. As currently drafted, the public will not be provided with any clarity or assurance of which public authorities will be able to collect their communication data.

204. It is inappropriate that such a long list of public authorities has access to individuals' communications data and for such broad purposes. This is a problem in its own right, but it also further reinforces the need for judicial authorization, which we discuss in more detail below in response to the question, "Is the authorisation process for accessing communications data appropriate?"

205. Furthermore, Clause 60(1) of the draft Bill sets out the requirement for a designated senior officer to consult a 'single point of contact' (SPOC) before granting an authorisation to obtain communications data. This is often cited as important safeguard on communications data requests.

206. The SPOC does not have any authority over the requests, however. Instead there is only a requirement to "consult" the SPOC, which falls short of even being a rubber stamp. The SPOC should have greater involvement in approving requests.

207. But the SPOC should not have overall responsibility for approving requests for communications data. Given how revealing communications data is about an individual, access to it must be subject to judicial authorisation.

208. Our concerns about the number of people who can access communications data are compounded by Clause 46(7), which sets out an overly broad range of purposes for which communications data may be obtained. Clause 46(7b) in particular, which is about preventing or detecting crime or disorder, is too broad

---

Request, *New York Times* [Online], Available from http://www.nytimes.com/2015/12/18/world/americas/brazil-whatsapp-facebook.html?ref=americas&_r=0

and enables intrusive 'fishing expeditions'. The provision should be amended to 'serious crime'.

209. Recommendations:

1. Require judicial authorisation for obtaining communications data, and give the SPOC a more substantial role in the authorization process.

2. Significantly limit the purposes for which communications data can be obtained.

Are there sufficient operational justifications for accessing communications data in bulk?

210. We respectfully refer the Committee to our response to the question:

1. "Has the case been made, both for the new powers and for the restated and clarified existing powers?" (see paragraphs 12-37).

211. In that response, we articulated why the Government has failed to make a compelling operational case for any of its bulk powers, including for accessing communications data in bulk.

Is the authorisation process for accessing communications data appropriate?

212. No. There is no prior judicial authorisation (with the only exceptions for local authorities under Clause 59; and if the authorisation is required in relation to obtaining communications data for the purpose of identifying or confirming a source of journalistic information, Clause 61.) Ordering the disclosure of communications data only requires authorisation by a designated senior officer of the public authority undertaking the collection. The limited safeguard of requiring the authorisation not be granted by an officer involved in the investigation or operation is undermined by the broad set of circumstances under which such requirement can be overridden (Clause 47).

213. The collection and use of communications data interferes with the right to privacy.[115] In fact, it is not disputed that communications data allow "very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.[116] As such authorisation for the collection and use of such data needs to fulfill the minimum standards of independence and impartiality.

214. The UN Human Rights Committee, when considering the UK periodic report under the ICCPR in July 2015, recommended the UK begin "ensuring that access to communication data is [...] dependent upon prior judicial

115 See report of the UN Special rapporteur on the promotion and protection of the freedom of opinion and expression, UN doc. A/HRC/23/40, 17 April 2014; report of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, UN doc. A/69/397, 23 September 2014, and report of the UN High Commissioner for Human Rights, Right to Privacy in the Digital Age, UN doc. A/HRC/27/37, 30 June 2014.

116 See Court of Justice of the European Union, Judgment in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, Judgment of 8 April 2014.

authorization".[117]

215. Recommendation:

1. Judicial Commissioners should authorize the obtaining of communications data.

Data Retention

Do the proposed authorisation regime and safeguards for bulk data retention meet the requirements set out in the CJEU Digital Rights Ireland and the Court of Appeal Davis judgments?

216. Part 4 regulates the retention of communications data. Under Clause 71 the Secretary of State can require any description of telecommunication operators to retain all or any description of communications data (and entity data) for up to 12 months. He or she may also impose requirements in relation to generating or processing the retained data (Clause 71.8). Retention of communications data is authorised by the Secretary of State only, with no judicial authorisation.

217. The blanket, untargeted retention of communications data provided for in the IP Bill is in breach of existing EU provisions protecting the right to privacy, such as the Data Protection Directive 1995/46 and the Directive on privacy and electronic communications 2002/58/EC. It is also a violation of applicable international human rights law, such as the EU Charter on Fundamental Freedom, the European Convention on Human Rights and the International Covenant on Civil and Political Rights.

218. The mandatory data retention regime under the IP Bill will go much further than what was prescribed under the invalidated EU Data Retention Directive (2006/24/EC): for one, it will not only be limited to the detection or prevention of serious crimes, but for any of the ten grounds under which communication data can be requested (Clause 46.7).

219. The proposed retention regime also goes further than the types of data that can be retained under the current Data Retention Regulations 2014;[118] there is a new retention requirement relating to the "pattern" of communications, and one related to "the internet protocol address, or other identifier, of any apparatus to which a communication is transmitted for the purpose of obtaining access to, or running, a computer file or computer program".[119] Communications service providers may be required to retain not only data they save in their normal course of business, but also anything they may be able to generate or obtain, including ICRs.[120]

220. As such, the IP Bill's proposed data retention regime will lead to the generation, collection, and storage, for up to a year, of highly revealing information pertaining to virtually all communications data sent, received or otherwise created by everyone. The retained data will potentially include, but also go well

117 Human Rights Committee, concluding observations on the UK, July 2015.
118 See: http://www.legislation.gov.uk/uksi/2014/2042/schedule/made
119 See Clause 71(9)
120 Clause 71, Part 4, Draft Investigatory Powers Bill

beyond, the who, what, where, when, and how relating to every communication that a person has online.

221. In Digital Rights Ireland v Minister for Communications and others, the Grand Chamber of the CJEU concluded that the 2006 Data Retention Directive (Directive 2006/24/EC of the Parliament and the Council of 15 March 2006), which required communications service providers to retain customer data for up to two years for the purpose of preventing and detecting serious crime, breached the rights to privacy and data protection under Articles 7 and 8 respectively of the EU Charter of Fundamental Rights.[121]

222. The CJEU noted that the Directive was flawed for not requiring any relationship between the data whose retention was provided for and a threat to public security (see §59). The Grand Chamber concluded that the Directive amounted to a "wide-ranging and particularly serious interference" with the rights to privacy and data protection "without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary" (§65.)

223. The same concerns apply to the proposed data retention regime under the IP Bill.

224. Privacy International notes that on 20 November 2015 the Court of Appeal's judgment in the case of David Davis and others (to which Privacy International is an intervener) referred to the CJEU the question as to whether the requirements included in the Digital Rights Ireland's judgment are mandatory requirements with which the national legislation of EU member states must comply.

225. Privacy International believes that the Digital Rights Ireland requirements are mandatory and that existing EU law rules out data retention regimes of the kind proposed in the IP Bill. Irrespective of the decision of the CJEU on this matter, there is growing consensus that the blanket retention of communications data, without suspicion, violates the right to privacy, as well as putting the security of personal data at risk of attack by criminals and others. In this context, it is notable that a significant number of European countries have moved away from blanket data retention regimes because of its incompatibility with EU law and the right to privacy.[122]

226. Recommendation:

    1. Delete Part 4 of the IP Bill and amend other parts accordingly. Instead of pursuing the regime of blanket retention of personal data, consider introducing “data preservation orders”, under which the retention of specific individuals' communications data is requested by the authorities and

121 Digital Rights Ireland v Minister for Communications and others, 8 April 2014, C-293/12.

122 Even before the CJEU issued its judgment in *Digital Rights Ireland*, the constitutional or administrative courts of Bulgaria, Cyprus, the Czech Republic, Germany and Romania declared part or all of the relevant national legislation implementing the Data Retention Directive to be unlawful. Following the *Digital Rights Ireland* judgment, the courts of Austria, Slovenia, Belgium, Bulgaria, the Netherlands, Poland, Romania, and Slovakia have struck down national laws that had implemented or replicated the Data Retention Directive (or, in the case of Romania and Bulgaria, subsequent amendments to the original implementing laws).

authorised by judges.

Is accessing Internet Connection Records essential for the purposes of IP resolution and identifying of persons of interest? Are there alternative mechanisms? Are the proposed safeguards on accessing Internet Connection Records data appropriate?

227. ICRs offer no additional capability beyond that which is already available to an authority in regards of connecting an Internet Protocol (IP) address with a subscriber. Intellectual property rights holders have been connecting IP addresses to subscriber IDs for some time in cases where they wish to enforce their rights. They have done this by subpoenaing the provider of an IP address, which can be determined by who the address was allocated to, and serving a court order on the provider compelling them to release information in relation to their subscriber. This works reasonably well for fixed line communications. However in relation to a mobile phone communications it may be more complicated as there is no need to register a universal subscriber identity module (SIM) – the equivalent of a hard-ware embedded IP address for mobile phones – to an individual. It is nonetheless probably possible for the provider to know which SIM was registered to which cell (or tower(s)), and quite possibly to determine the location of the user of that SIM through the use of triangulation.

228. The main change the IP Bill would implement is that this and other data would need to be retained by telecommunication operators for up to 12 months (under Part 4).

229. The IP Bill definition of ICR is not technically crafted (see Clause 47(6)), making it impossible to assess exactly what an ICR would contain and who exactly would be required to retain them. Some more details can be glimpsed in the accompanying document "Operational Case for the Retention of Internet Connection Records".[123] In this document a number of scenarios and case studies are explored and the justifications for ICRs are put forward.

230. Privacy International notes that this document provides a very conservative view of the capabilities of that the IP Bill could potentially authorise as the vague nature of the language in the Bill could be interpreted to give considerably more information than this document suggests.

231. Further, the amount of data likely to be generated by capturing every port and IP combination of every connection, by every user in the United Kingdom and retaining that data for 12 months is likely to be a heavy burden upon telecommunication operators.

232. Recommendation:

    1. Clause 47: Delete subsections 47(4), (5) and (6)

    2. If data retention is to remain in the IP Bill, do not allow a retention order that would require telecommunications services to generate and retain ICRs.

123 Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473769/Internet_Connection_Records_Evidence_Base.pdf

Are the requirements placed on service providers necessary and feasible?

233. Clauses 71 and 79 empower the Secretary of State to require communications service providers to retain communications data (and entity data) for up to 12 months. This requirement is mandatory for providers located in the UK, and requested of those outside the UK. Requiring communications service providers to retain all of our revealing and personal data for 12 months treats us all as suspects, undermining the trust we place in government to only exercise its power to intrude upon on personal lives in the most limited and necessary of circumstances.

234. Due to the revealing nature of such data, the database(s) where this retained data is stored are also likely to be targeted by cyber criminals and foreign intelligence agencies. Compelled retention unnecessarily endangers the security of our data, as communications service providers could be subject to increased attacks to access that data. This year alone has seen the successful infiltration and hacking of several large databases. Recent examples include, but are not limited to, TalkTalk, Vodafone, British Gas, as well as the detrimental Office of Personnel Management (OPM) breach in the United States.[124]

235. Clause 74 of the IP Bill imposes some general obligations to protect the security of such retained data, but its broad provisions are far from a guarantee that future attacks such as these would be prevented. Communications service providers bear the brunt of public criticism in the face of data breaches, even where they are being compelled to retain the data, further undermining trust in the security of their services.

236. The IP Bill requires communications service providers to weaken their system security while simultaneously increasing the data they retain. This provides for a perfect storm that will make individuals' personal data far more susceptible to cyberattacks. As David Emm, principal security researcher at Kaspersky Lab points out, "[o]ne of the big issues is the practical aspects for ISPs – how are they going to store it, how is it going to provide access when required, and how secure will both of those things be?".[125]

237. The new regime expands the scope of who could be served with a retention notice. Clause 193(10) defines "telecommunications operator" as a person who either offers or provides a telecommunications service to persons in the UK, or

---

124 (27 February, 2015) Customer Data Stolen in TalkTalk Hack Attack, BBC Technology [Online] Available from: http://www.bbc.co.uk/news/technology-31656613 [Accessed 26 November, 2015], (31 October, 2015) Vodafone customers' bank details 'accessed in hack', company says, The Guardian [Online] Available from: http://www.theguardian.com/business/2015/oct/31/vodafone-customers-bank-details-accessed-in-hack-company-says [Accessed 26 November, 2015], Hern, Alex (29 October, 2015) British Gas denies responsibility for 2,200 user accounts posted online, The Guardian [Online] Available from: http://www.theguardian.com/technology/2015/oct/29/british-gas-denies-responsibility-user-accounts-posted-online-pastebin [Accessed 26 November, 2015], Hirschfeld Davis, Julie (9 July, 2015) Hacking of Government Computers Exposed 21.5 Million People, The New York Times [Online] Available from: http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html [Accessed 26 November, 2015]

125 Allison, P.R. What the Investigatory Powers Bill means for the telecommunications industry, *Computer Weekly* [Online]. Available from http://www.computerweekly.com/feature/What-the-Investigatory-Powers-Bill-means-for-the-telecommunications-industry [Accessed 15 December 2015]

controls or provides a telecommunication system reaching the UK. The IP bill includes not just public telecommunications providers but also private networks. This will mean a very wide range of companies, from a large multinational telecommunication provider to a small tech startup would be subject to a notice.

238. The security concerns raised by retention would be felt not only within the technology sector, but also within related businesses that rely on secure communications and customer trust. Many of these businesses contribute greatly to the British economy, and include the banking, financial, and legal sector, as well as the computer software, hardware, anti-virus, gaming, and start-up industries.

239. Individuals will consequently face a reduction in their privacy and security, which could undermine trust in the entire communications system. The internet offers a democratic space in which personal exploration, growth, change, and development is possible, and without trust in the systems that enable such exploration, such positive growth is curtailed.

240. Recommendation:

    1. Delete Part 4 of the IP Bill and amend other parts accordingly. Instead of pursuing the regime of blanket retention of personal data, consider introducing "data preservation orders", under which the retention of specific individuals' communications data is requested by the authorities and authorised by judges.

Equipment Interference

Should the security and intelligence services have access to powers to undertake (a) targeted and (b) bulk equipment interference?

241. For the first time in the UK, the draft IP Bill includes statutory provisions describing the power of law enforcement and the intelligence services to hack into our computers. This power is called "Equipment Interference", and is detailed in Part 5 and, as a "bulk" power, in Part 6, Chapter 3.

242. Hacking, as undertaken by any actor, including the state, fundamentally impacts on the security of computers and the internet. It incentivises the state to maintain security vulnerabilities that allow any attacker – whether GCHQ, another country's intelligence agency or a cyber criminal – potential access to our devices. Hacking can undermine the security of all our communications, whether we are emailing our loved ones or banking online. One US intelligence official analogised using hacking to a situation in which "[y]ou pry open the window somewhere and leave it so when you come back the owner doesn't know it's unlocked, but you can get back in when you want to."[126]

243. Privacy International has written extensively on the security concerns raised by hacking, and as have security experts. We do not repeat those submissions here,

126 Gellman, B. and Nakashima, E., U.S. spy agencies mounted 231 offensive cyber- operations in 2011, documents show, *The Washington Post* (30 August 2013), available at: https://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

but include some of them for your reference.[127] If hacking is to be used by the state, these security concerns must be addressed.

244. As currently drafted the IP Bill compounds these security concerns by forcing telecommunications services to become complicit in government hacking. Clause 99 requires any person (which could include CSPs) to "provide assistance in giving effect to the [equipment interference] warrant." Clause 101 explicitly applies this duty to "relevant telecommunications providers." Under these two clauses, communications service providers could be compelled to take any steps, unless "not reasonably practicable", to assist the police and the intelligence services to hack our computers and other devices.

245. While we do not know what this assistance will look like in practice, it might include compelling telecommunications services to send false security updates to a user in order to install malware that the police or intelligence services could then use to control the user's computer. As we explained to the Science & Technology Committee, the possibility that security updates might be co-opted would undermine trust in those updates, which are crucial to protecting our devices from unauthorised intrusions from criminals.[128] The general public is likely never to be made aware of what kind of "hacking" assistance has been required of telecommunications providers due to the very strict non-disclosure provision in the IP Bill (Clause 102). It will therefore be very hard to maintain trust if Clauses 99 to 102 remain in the IP Bill.

246. Hacking is also an incredibly intrusive form of surveillance. When an agent takes control of a computer by hacking it, there are few limits on what can be done.[129] Unlike intercept capabilities, hacking capabilities can be deployed in any number of configurations to do any number of different things. The logging of keystrokes, tracking of locations, covert photography, and video recording of the user and those around them enables intelligence agencies and the police to conduct real-time surveillance. Anything we store on our computers and mobile phones, intentionally or unintentionally, is also fair game, from location records, to saved documents and notes, to draft messages and emails, and more. As

---

127 Please see: Privacy International and Open Rights Group's Submission in Response to the Consultation on the Draft Equipment Interference Code of Practice (20 March 2015), available at: https://www.privacyinternational.org/sites/default/files/PI%20and%20ORG%20Submission%20-%20Draft%20Equipment%20Interference%20Code%2020%20Mar%202015_0.pdf ; Privacy International Submission in Response to Science & Technology Call for Evidence on the Draft Investigatory Powers Bill (27 November 2015) [hereinafter "PI & ORG Science & Technology Committee Submission"], available at: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html ; Expert Report of Professor Ross Anderson, submitted in Privacy International and Greennet Limited et al. in the Investigatory Powers Tribunal (Case nos. IPT 14/85/CH and 14/120-126/CH) (30 September 2015), available at http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25170.html

128 PI & ORG Science & Technology Committee Submission, paras. 22-23.

129 For an overview of the types of information that can be obtained via hacking, please see the Expert Report of Peter Michael Sommer, submitted in Privacy International and Greennet Limited et al. in the Investigatory Powers Tribunal (Case nos. IPT 14/85/CH and 14/120-126/CH) (30 September 2015) [hereinafter Sommer Report], available at: https://www.privacyinternational.org/sites/default/files/PI_PMS_Report_final.pdf

"smart" technology develops, hacking will increasingly provide access to our refrigerators and thermostats, our children's dolls and our cars.

247. Because of its intrusiveness, hacking should only be deployed under the strictest authorisation regime, with stringent safeguards and vigorous oversight. Unfortunately, the draft IP Bill fails to provide these. In particular, as discussed above in paragraphs 67 to 79, the "targeted" equipment interference powers in Part 5 are not in fact targeted but can be deployed in bulk using thematic warrants.

248. Bulk equipment interference, whether carried out under a thematic warrant or under the explicit "bulk" power in Part 6, Chapter 3, destroys the ability of the authorising authority to assess the necessity and proportionality of the hacking being undertaken. Without knowing which computer is to be hacked into – as well as what information might be contained on that computer, who else might be using it, the level of suspicion that attaches to the person or people who might be using the computer, etc. – how can a Judicial Commissioner properly assess if such intrusion is proportionate? Indeed, the Grand Chamber of the European Court of Human Rights recently declared that an authorisation for surveillance must identify "a specific person" or "a single set of premises" in order to facilitate the necessity and proportionality analysis.[130]

249. "Bulk" hacking under Part 6, Chapter 3 is permitted only where the main purpose of the warrant is to obtain "overseas-related" communications, private information and equipment data. This limitation should provide little comfort for those residing in the UK. For instance, much of our data is stored overseas in servers operated by telecommunications services such as Google and Facebook. Given how intrusive hacking is, and how our interconnected world makes it just as easy to hack a computer in Belgium as in Birmingham, drawing a distinction between overseas hacking and internal hacking makes little sense. Equipment interference should only be authorised where a specific target has been identified, and a very strong case has been made as to the necessity of obtaining the information sought from the target.

250. Finally, because hacking involves an active interference with a computer, it raises serious evidentiary concerns. Evidence obtained via equipment interference is admissible in court. Once an agent or officer takes control of a computer by hacking it, however, they have the unfettered ability to alter or delete any information on that device. This raises the risk, in the context of a criminal prosecution, of defence accusations of evidence tampering.[131] The IP Bill currently does not contain any provisions to address this evidentiary concern. Without such safeguards, the efficacy of the use of hacking in investigating and prosecuting crimes is very questionable.

251. <u>Recommendations:</u>

    1. Thoroughly assess the security concerns raised by equipment interference to determine if they can be resolved.

130 Zakharov v Russia 47143/06, 4 December 2015, at paras. 259-267.

131 For a more extensive discussion of these evidentiary concerns, please see Sommer Report at paras. 108-111.

2. Delete clauses 99 to 102.

3. Implement changes recommended above (paragraph 78) to clause 83.

4. Delete Part 6, Chapter 3.

5. Include provisions to address the evidentiary concerns raised by equipment interference.

252. Questions:

1. What sort of "assistance" in interfering with equipment might be required under clauses 99 and 101?

2. How can proportionality be assessed when a thematic warrant or a bulk warrant is being authorised?

Should law enforcement also have access to such powers?

253. Granting law enforcement access to equipment interference powers has the potential to compound security concerns as it will likely increase both the number of devices that will be hacked and the number of officers who will be doing the hacking. For the same reasons stated above, therefore, careful consideration should be given to whether hacking is an appropriate police power in light of the security threat.

254. Hacking for law enforcement purposes also brings the evidentiary problems, discussed in response to the previous question, to the fore. Allowing law enforcement to hack makes the need to address these evidentiary concerns even more pressing.

Are the authorisation processes for such equipment interference activities appropriate?

255. As we contend throughout this submission, intrusive powers such as equipment interference must be subject to robust, independent judicial authorisation (see, e.g., our response to the question "Is the authorisation process appropriate?").

256. Additionally, Privacy International has established ten principles we believe must be met if equipment interference is to be a permitted power. Those principles are outlined in our submission on the draft Equipment Interference Code of Practice.[132]

257. The Sixth Principle sets forth many of the elements we believe should be included in a warrant to ensure effective and human rights compliant authorisation of equipment interference. These include:

1. the specification of an individual target;

2. a statement of the nature of the suspicion that the target is connected to a serious crime or a specific threat to national security;

132 PI and ORG Consultation Response: Draft EI Code, at pages 9-15.

3. a declaration with supporting evidence that there is a high probability evidence of the serious crime or specific threat to national security will be obtained by the operation authorised;

4. a precise and explicit description of the method and extent of the proposed intrusion and the measures taken to minimise access to irrelevant and immaterial information;

5. a declaration with supporting evidence that all less intrusive methods of obtaining the information sought have been exhausted or would be futile;

6. a declaration with supporting evidence that the security of the device targeted or communications systems more generally will not be negatively impacted by the proposed intrusion; and

7. a time limit of one month, although the warrant may be renewed on a monthly basis with sufficient cause, including an explanation of why the information sought has not yet been obtained.

258. None of these elements are included in equipment interference warrants currently proposed in the IP Bill. Indeed, thematic warrants and bulk warrants completely lack any elements of individualized suspicion, and necessarily would not be able to specify the extent of the proposed intrusion given the target is unknown. Nor is there a requirement that hacking be a method of last resort; the Secretary of State need only "take into account" whether the information sought "could reasonably be achieved by other means" (Clause 84(6)). Finally, equipment interference warrants last for 6 months (Clauses 94 and 141).

259. Given how technically complex equipment interference can be, the Judicial Commissioners should have technically competent assistance so they can fully understand and consider the nature of the intrusion being proposed.

260. Recommendations

1. If there is to be the power of equipment interference, require equipment interference warrants to contain the elements listed above, potentially by amending clause 93.

2. Ensure Judicial Commissioners have technically competent assistance in order to fully vet warrants.

Are the safeguards for such activities sufficient?

261. Authorisation is one of the most important safeguards for equipment interference. As we argue above, the authorisation regime needs significant improvement. We add to that concern two problems we see with the safeguards proposed in clauses 103 (equipment interference) and 146-147 (bulk equipment interference).

262. First, if information obtained through equipment interference is to be shared outside the agencies or organization that originally obtained the information, including with overseas authorities, that sharing should be very closely circumscribed in law. The draft IP Bill fails to provide such protections.

263. Instead, clause 103 does not even mention possible overseas sharing. Yet clauses 103(3)-(4) and (8) appear broad enough to allow it. In contrast, clause 146(8) references sharing material acquired via bulk equipment interception with "authorities of a country or territory outside the United Kingdom."

264. Clause 146(8) also illustrates the problems with such sharing by removing the safeguards contained in clauses 146(3) (minimizing copying and disclosure of data) and 146(6) (destruction of data) when the data is handed over to overseas authorities. Presumably, these protections are removed because once the data is shared the UK authorities will no longer have effective control over it. This lack of future controls means that if information is to be shared, it must only be in the most limited of circumstances where there is a strong and demonstrable justification for the sharing, and the UK has confidence that the overseas authority that will be receiving the information will not use it for improper purposes (clause 146(9) is not sufficient in this regard). The UK should also negotiate the right to continuing oversight of how the information is used.

265. Also of note, the IP Bill fails to regulate how the UK authorities should treat information obtained by other countries via equipment interference that is then shared with the UK. This is a significant oversight, as such a lack of publicly accessible policies on sharing was found to be unlawful in the context of interception.[133] As discussed above in paragraphs 53 to 54, how the IP Bill addresses overseas sharing needs significant improvement.

266. Second, notification is a common safeguard in warrantry systems around the world.[134] The presumption is that the target of surveillance will be notified when there is no risk of jeopardising an ongoing investigation. This should ordinarily happen within 12 months of the conclusion of the investigation, although that 12-month period may be extended in six-month intervals by judicial authorisation. The draft IP Bill lacks any such presumption of notification.

267. Recommendations

1. Explicitly address sharing of information obtained via equipment

[133] See Liberty & Others v the Secretary of State (2015) UKIPTrib 13_77-H, at para. 23, available at: http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf

[134] Consider the following examples:

- Canada: Section 196.1 of the Canadian Criminal Code requires notification to the target of the interception "within 90 days after the day on which it occurred" subject to extension.
- Germany: Section 101 of the German Code of Criminal Procedure articulates a duty to inform targets of surveillance and others who might have been affected "as soon as it can be effected without endangering the purpose of the investigation, the life, physical integrity and personal liberty of another, or significant assets".
- Japan: The Act on the Interception of Communications provides that the target of intercepted communications must be notified within 30 days of the completion of surveillance subject to extension. *See* UNODC, *Current Practices in Electronic Surveillance* (2009), at page 17, available at https://www.unodc.org/documents/organized-crime/Law-Enforcement/Electronic_surveillance.pdf.
- US: At the federal level, § 2518(8)(d) of the Wiretap Act (18 U.S.C. §§ 2510-2522) requires notification to targets of surveillance and "such other parties . . . as the judge may determine in his discretion that is in the interest of justice" within "a reasonable time but not later than ninety days after . . . the termination of . . . the [surveillance] order". Notification that an application for such an order was sought but denied is also required to the same parties within the same time frame.

interference with overseas authorities (and from overseas authorities to the UK) and strengthen the safeguards that attach to sharing.

2. Include provisions requiring notification of subjects of surveillance when there is no risk of jeopardising an ongoing investigation.

268. Questions

1. Why is sharing with overseas authorities explicitly addressed in the context of bulk equipment interference (Part 6, Chapter 3) but not for regular equipment interference (Part 5)?

2. Why doesn't the IP Bill address the sharing with UK agencies of data obtained via equipment interference by overseas authorities?

3. Why doesn't the IP Bill include notification provisions?

Bulk Personal Data

Is the use of bulk personal datasets by the security and intelligence services appropriate?

269. This answer to the particular aspects of the Bulk Personal Dataset regime should be read in conjunction with Privacy International concerns and objections to the bulk warrants mentioned above.

270. The acquisition, retention and use of Bulk Personal Datasets involves obtaining a set of information that includes personal data relating to a number of individuals, who, as the IP Bill notes, are of not of interest to the intelligence service in the exercise of its functions (Clause 150.) These datasets can be obtained from other public sector bodies or from the private sector.

271. Bulk Personal Datasets can be obtained in two ways, through a specific BPD warrant (Clause 154) and a class BPD warrant (Clause 153). A class BPD warrant authorises an intelligence service to obtain, retain or examine bulk personal datasets that fall within a class described in the warrant. A class warrant must include a description of the Bulk Personal Datasets to which it relates and an explanation of the operational purpose for which the applicant wishes to examine the data collected. No further guidance is provided as to the kind of terms that would suffice to sufficiently describe a class of Bulk Personal Datasets. The case law of the European Court of Human Rights is clear that the minimum safeguards that should be set out in law in order to avoid abuses of power include a definition of the categories of people liable to have their data recorded and retained.[135] Clause 153 fails to provide detailed rules governing the scope of class BPD warrants.

272. Furthermore, as we discuss in paragraphs 88-90, once the datasets have been

135 See S and Marper v United Kingdom (2009) 48 EHRR 50, at §99: "[The Court] reiterates that it is as essential…secret surveillance and covert intelligence-gathering to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, inter alia, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness."

obtained there are not sufficient limitations on how they may be examined.

273. Clause 154 relating to a specific BPD warrant is not any better, as while a specific dataset must be specified in the warrant, there are no limitations on what that dataset might contain or where it might be obtained. Like the other bulk powers, we believe these problems mean that Part 7 should be removed from the Bill. We are bolstered in our suggestion by the fact that the Home Office has yet to make a strong operational case for the BPD power.

274. Recommendations:

1. Delete Part 7

Are the safeguards sufficient for the retention and access of potentially highly sensitive data?

275. If the power to obtain Bulk Personal Datasets remains in the IP Bill, we reiterate the concerns we expressed above in paragraphs 186-188 with regard to security problems created by the retention of large amounts of sensitive personal information.

276. In addition, as pointed out in paragraph 90 above, there are few safeguards on who can access BPDs after they have been collected. This is a failing of the section and inconsistent with the protections placed on the other bulk powers.

Oversight

What are the advantages and disadvantages of the proposed creation of a single Judicial Commission to oversee the use of investigatory powers?

277. Privacy International commends the IP Bill's attempt to simplify what was formerly a "confusing array of mechanisms, with little clarity as to the demarcation between them".[136] Both the Anderson and RUSI Reports documented the concerns raised from many quarters regarding the opacity and unnecessary complexity of a proliferating number of oversight mechanisms and regulators.[137] As a result, both reports also recommended the creation of a single oversight mechanism that would merge the functions of the Intelligence Services Commissioner, Interception of Communications Commissioner's Office and Office of Surveillance Commissioners.[138] A main advantage of the draft IP Bill is the acceptance of this recommendation through the creation of the Investigatory Powers Commissioner.

278. We are concerned, however, that a single Commission will be responsible for conducting both authorisation and oversight and consider this to be a critical flaw in its current form. Authorisation is a distinctly legal function. While we take issue with the judicial review standard to be applied by the Judicial Commissioners in the draft IP Bill, we emphasise here that their role is to make a judicial determination on the legality of a warrant application. By contrast, oversight demands a fundamentally different set of skills, which the Judicial Commissioners should not be tasked to undertake.

136 Anderson Report, para. 12.79.
137 *Id.*; RUSI Report, paras. 4.42-43.
138 Anders Report, Recommendation 82; RUSI Report, Recommendations 17-19.

279. This distinction is documented nicely in the RUSI Report, which noted the following criticism of the current Commissioners:

> "[T]hey are judges, not investigators. They are . . . generally less experienced in identifying problems of process or the application of new technology. . . . [T]he commissioners need to be 'inquisitive troublemakers', with a level of investigatory expertise that is prized by the agencies themselves. There is a need for individuals . . . who can . . . question and challenge people and practices within the relevant organisations. Given the depth of investigations . . . the commissioners require greater assistance from teams of people with appropriate skills and expertise, perhaps in the form of legal and technical 'juniors'."[139]

280. Fusing the authorisation and oversight functions into a single Commission also raises serious conflict of interest concerns. The draft IP Bill essentially proposes that the Commission both participate in authorising warrants and undertake reviews of that very authorisation process. We believe that this structure cannot provide the independence that is so critical to a functioning oversight system.

281. We bring to the Committee's attention that neither the ISC nor RUSI recommended the merging of the authorisation and oversight functions in the manner proposed by the draft IP Bill. In particular, RUSI emphasised that "[t]he judicial commissioners in charge of the authorisation of warrants should not be part of a new [oversight mechanism]".[140] It further explained that the oversight mechanism should cover "four main areas of responsibility: inspection and audit, intelligence oversight, legal advice, public engagement".[141] We note that one of Anderson's own models for the new oversight mechanism proposes that a "Chief Judicial Commissioner" be responsible for authorisation while a separate "Chief Commissioner (non-judge)" be responsible for oversight.[142]

282. Recommendation:

1. Separate the authorisation and oversight functions that are currently combined in a single Judicial Commission.

Would the proposed Judicial Commission have sufficient powers, resources and independence to perform its role satisfactorily?

283. Powers - Privacy International submits that the Investigatory Powers Commission does not have adequate judicial authorisation powers in the draft IP Bill. The draft Bill preserves the power of the Secretary of State to issue warrants while permitting Judicial Commissioners to "review" this decision (see in particular Clauses 19-21, 59, 90, 109, 123, 138, 155). Above we provide criticism of this proposed authorisation system in response to the question "Is the authorization process appropriate?"

284. Privacy International is also concerned that judicial authorisation, even in the weak form expressed in the draft IP Bill, is not required for a range of powers

139 RUSI Report, paras. 4.80-83.
140 RUSI Report, para. 5.60.
141 RUSI Report, Recommendation 18.
142 Anderson Report, Annex 18.

that interfere with the right to privacy. In our prior submission to the Joint Human Rights Committee, we outlined these powers, which include obtaining communications data, issuing data retention notices and modifying interception warrants.[143] We also articulated that the lack of judicial authorisation for such powers may fall short of requirements under international human rights law.

285. Resources - The Anderson, ISC and RUSI reports all emphasised the need to ensure that the surveillance oversight mechanisms – whatever form they should take – are well-resourced.[144] We reiterate that position with respect to both authorisation and oversight, which as we explain above must remain separate from each other. In terms of authorisation, we highlight the need to ensure that there is an adequate number of Judicial Commissioners. While we do not think that the Secretary of State must play a role in authorising warrants, we note the criticism levied at the sheer number of warrants she and her predecessors have been asked to authorise under the current system.[145] With respect to oversight, we urge the Committee to consider the resources necessary "to compare practice across the whole range of different public authorities", "to inspect the whole range of surveillance techniques", "to attract excellent specialists", and to enhance the public profile of such work.[146] For both authorisation and oversight, we highlight the critical importance of technical expertise.

286. Clause 176(2) articulates that the Secretary of State is to provide the Judicial Commissioners with the staff and "accommodation, equipment and other facilities" she "considers necessary for the carrying out of the Commissioners' functions". We question the appropriateness of granting the Secretary of State the power to determine the resources of the Investigatory Powers Commission as it may undermine its independence. We would also urge the Committee to consider adding more precise language to this clause laying out the types of resources, in particular technical expertise, to be provided to the Commission.

287. Independence - Privacy International submits that the proposed IP Commission is not sufficiently independent to perform its role satisfactorily. First, the appointment of Judicial Commissioners by the Prime Minister, rather than through the Judicial Appointment Commission, subverts the very independence that their participation is meant to bring to the authorisation process (Clause 167(1)). Permitting the executive to appoint the Commissioners inappropriately blurs the line between the branches, risking political bias on the part of the Commissioners.[147] This concern is exacerbated by the three-year terms of office

143 *Id*. at paras. 51-56.

144 *See* Anderson Report, paras. 14.94-97; ISC Report, para. 211; RUSI Report, para. 5.66.

145 *See* Big Brother Watch, Joint Committee on the Draft Investigatory Powers Bill – Written Evidence, Dec. 2015, pages 3-4, available at https://www.bigbrotherwatch.org.uk/wp-content/uploads/2015/12/Draft-Investigatory-Powers-Bill-Consultation-Big-Brother-Watch-Response.pdf; Anderson Report, para. 7.33 (noting that the Home Secretary personally authorised "2,345 interception and property warrants and renewals" in 2014).

146 Anderson Report, para. 14.97.

147 While Anderson observed that "[t]he Chief Commissioner should be appointed by the Prime Minister", he at least suggested that "[c]onsideration . . . be given to allowing the ISC a voice in the appointment or confirmation of the Chief Commissioner." He did not indicate how Judicial Commissioners, sitting under the Chief Commissioner, should be appointed. Anderson, Recommendation 105.

for Commissioners proposed by the draft IP Bill (Clause 168(2)). The brevity and renewable nature of these terms renders the Commissioner role inherently insecure, increasing the risk that their decisions will be biased towards the executive.

288. Second, the draft IP Bill further undermines the independence of Judicial Commissioners by permitting the Secretary of State to appeal refusals to approve a warrant or authorisation to the IP Commissioner (Clauses 19(5), 109(4), 123(4), 138(4), 155(3)). The right to appeal is not constrained in any way and simply gives the Secretary of State a second bite at the apple if displeased with the decision of a Judicial Commissioner. This right is particularly troubling given the executive influence in appointing the Judicial Commissioners, including the IP Commissioner, discussed above.

289. Recommendations:

1. Vest the power to issue warrants in Judicial Commissioners or, in the alternative, remove the "judicial review" standard in the approval clauses.

2. Ensure prior judicial authorisation for the acquisition of communications data and the modification of interception warrants.

3. Consider granting the power to determine resources for the Judicial Commission to an authority other than the Secretary of State.

4. Consider adding more specific language to Clause 176(2) to require particular resources, especially technical expertise, be provided to the IP Commission.

5. Ensure Judicial Commissioners are independently appointed by the Judicial Appointments Commission and serve fixed-length terms.

Are the appointment and accountability arrangements for Judicial Commissioners appropriate?

290. As we state in the preceding section, we think the Judicial Appointment Commission should appoint Judicial Commissioners, not the Prime Minister. Further, the Secretary of State's ability to appeal a decision of a Judicial Commissioner should be circumscribed so as not to merely give him or her a "second bite at the apple."

Are the new arrangements for the Investigatory Powers Tribunal including the possibility of appeal adequate or are further changes necessary?

291. The Investigatory Powers Tribunal is an important yet imperfect component of the oversight regime. The IPT and its procedure are handicapped in several ways that, if remedied, could improve the openness and fairness of the process through which claims against the intelligence services are adjudicated.

292. The IPT should operate under a presumption of openness unless a compelling case is made that allowing specific information to be made public would harm national security. To facilitate this openness, we recommend the IP Bill be amended to:

1. Include a presumption of openness;

2. Require any party requesting a closed hearing or to submit closed evidence to provide the national security reasons for the request to the IPT (opposing parties should also be made aware of the existence of the request); and

3. Require the IPT to determine if a request for a closed hearing or to submit closed evidence is justified on national security grounds, while also giving the IPT the related power to compel the production of evidence if there are not sufficient reasons to keep it secret. There should be an especially strong presumption in favour of the production of internal policies and legal interpretations given how important they are to a full consideration of the lawfulness of the intelligence services' activities.

293. Where portions of a proceeding cannot be held in open because of the harm to national security, the IPT must appointment a Special Advocate to represent the interests of any excluded party in the closed sessions.

294. While the ability to appeal an IPT decision is a welcome change, the right to appeal proposed in the Bill is a limited one. For instance, an appeal may only be taken with leave of the IPT or the court that will hear the appeal (Clause 180(3)). Not every issue can be appealed – only those which are deemed to "raise an important point of principle or practice" or where there is "another compelling reason for granting leave" (Clause 180(4)). Careful consideration should be given to whether such limitations are appropriate. In the context of other tribunals, appeals are permitted where they would have a real prospect of success; or there is some other compelling reason why the appeal should be heard.[148]

295. Recommendations

1. The IPT should operate under a presumption of openness.

2. Any request for a closed hearing or to submit closed evidence must be justified to the IPT on national security grounds. The IPT must them determine if the request if justified.

3. The opposing parties should be made aware of the existence of any request for a closed hearing or to submit closed evidence.

4. The IPT should have the power to compel the production of evidence if there are not sufficient reasons to keep it secret.

5. The IPT must appoint a Special Advocate who can represent the interests of any excluded party during closed sessions.

6. Appeals from the IPT should be allowed where they would have a real prospect of success; or there is some other compelling reason why the appeal should be heard.

[148] See CPR 52.3(6), available at: https://www.justice.gov.uk/courts/procedure-rules/civil/rules/part52