LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Commons

March 2016

About Liberty

Liberty (The National Council for Civil Liberties) is one of the UK's leading civil liberties and human rights organisations. Liberty works to promote human rights and protect civil liberties through a combination of test case litigation, lobbying, campaigning and research.

Liberty Policy

Liberty provides policy responses to Government consultations on all issues which have implications for human rights and civil liberties. We also submit evidence to Select Committees, Inquiries and other policy fora, and undertake independent, funded research.

Liberty's policy papers are available at
http://www.liberty-human-rights.org.uk/policy/

Contact

Bella Sankey
Director of Policy
Direct Line 020 7378 5254
Email: bellas@liberty-human-rights.org.uk

Rachel Robinson
Policy Officer
Direct Line: 020 7378 3659
Email: rachelr@liberty-human-rights.org.uk

Sara Ogilvie
Policy Officer
Direct Line 020 7378 3654
Email: sarao@liberty-human-rights.org.uk

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line
Email: silkiec@liberty-human-rights.org.uk

Sam Hawke
Policy Assistant
Direct Line
Email: samuelh@liberty-human-rights.org.uk

Introduction

1. The Investigatory Powers Bill will receive its Second Reading in the House of Commons on Tuesday 16 March 2016. Liberty has called for a new surveillance legal framework for almost a decade and fully supports the use of targeted, proportionate and necessary surveillance powers. However we are gravely concerned that this Bill is rushed and contains a significant number of measures that breach human rights protections. Following publication of the Draft Bill in November 2015, parliamentary committees, experts, and tech companies all called on the Government to make significant reforms. Instead, the Government took no time to reflect and within the space of weeks has returned to Parliament with a Bill containing even more expansive powers than contained in its draft. Subject to the insertion of the word "privacy" in the title of Part 1 of the Bill, the safeguards remain resolutely inadequate to the task of protecting privacy and the Government has adduced no evidence that the huge powers in this Bill would be effective in keeping us safe. We call on MPs to reject this Bill and to require the Government to consider and incorporate improvements to the Bill as recommended during the pre-parliamentary scrutiny period. In particular, we urge the removal of mass surveillance powers.

2. This document is a summary of the main powers and purported safeguards. Liberty has also published a full analysis of the Bill along with detailed recommendations for change.

Authorisation process for surveillance warrants

3. The Bill would introduce a new requirement for a judicial commissioner (JC) to review a warrant before it is issued. The Bill states in terms that a "judicial commissioner" is restricted to reviewing a minister's conclusions by *"applying the same principles as would be applied by a court on application for judicial review."*[1] Warrants can last for 6 months and be renewed indefinitely. Surprisingly, the Bill provides for many types of warrant to be retrospectively modified without judicial authorisation. Modifications can relate to the names, premises, organisations etc. to be targeted. Warrants that are no longer considered justified are to be cancelled by Ministers rather than JCs.

4. Liberty has long called for judicial authorisation for all public authority requests to conduct surveillance, as is required by human rights legislation. It is the proper constitutional function of the independent judiciary to act as a check on the use of intrusive and coercive powers by State bodies and to oversee the application of the law to individuals. Additionally, judges are professionally best equipped to apply the legal tests of necessity and proportionality to ensure that surveillance is conducted lawfully. English law has long recognised the need for a specific judicial warrant before a person's home can be searched by police when serious crime is suspected, but sadly the process for authorising electronic surveillance has lagged behind.

[1] For example clause 21. See also 97, 123, 139, 157, 179.

5. However Liberty believes that the authorisation system laid out in the Bill is wholly inadequate for the UK to fulfil its human rights obligations and to provide a 'world leading oversight regime'. The Government has sought to portray the authorisation process as a "double lock" implying that both the Minister and the judge have a substantive role in issuing warrants. This is highly misleading. The JC powers are so circumscribed that the Bill risks creating the illusion of judicial control over surveillance while achieving little change from the status quo. Parliamentarians who would like to see a substantive role for the judiciary in authorising surveillance warrants should support a straightforward one-stage process that gives the task to a JC and removes Ministers' involvement. This would be much more in keeping with practice in comparable jurisdictions such as the US.

Legal Thresholds for surveillance

6. The Bill re-legislates for RIPA's three broad statutory grounds for issuing surveillance warrants. The Secretary of State may issue warrants for interception, hacking, communications data retention and acquisition and for the use of all bulk powers when he/she considers it necessary and proportionate: *"in the interests of national security", "for the purpose of preventing or detecting serious crime", or "in the interests of the economic well-being of the UK so far as those interests are also relevant to the interests of national security".* This final ground can apply only where it relates to the acts or intentions of persons outside the British Islands. Retention and access to communications data can be authorised on many more grounds and by many more public authorities.

7. All three main statutory grounds for authorising surveillance are unnecessarily broad and vague and left dangerously undefined. This means that individuals are not able to foresee when surveillance powers might be used, and grants the Secretary of State discretion so broad as to be arbitrary. The Joint Committee on the draft Bill recommended that the Bill should include definitions of national security[2] and economic well-being[3]. The three grounds contain no requirement for reasonable suspicion that an individual has committed or intends to commit a serious criminal offence, nor even suspicion or evidence that a serious crime has been or is going to be committed. This gives licence for speculative surveillance.

8. The national security ground is particularly problematic, as the Courts have responded with considerable deference to Government claims of 'national security', viewing them not as a matter of law, but as executive led policy judgements.[4] National security as a legal test is therefore

[2] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 82
[3] Ibid. Recommendation 83
[4] Lord Hoffman at para 50, *Secretary of State for the Home Department v Rehman* [2001] UKHL 47: Lord Hoffman has stated that whether something is 'in the interests' of national security "is not a

meaningless. The second ground is similarly broad and open-ended and the Government has not sought to clarify the circumstances in which 'national security' as opposed to 'the prevention and detection of serious crime" will be in play.

Communications data retention and acquisition

9. Parts 3 & 4 of the Bill seek to re-legislate for the existing communications data retention and acquisition regime under RIPA and DRIPA but with an additional requirement for communications providers to generate and retain "internet connection records" and establish a Request Filter as previously proposed, and rejected, in the Draft Communications Data Bill, 2012.[5]

10. Part 4 gives the Secretary of State the power to issue a retention notice to require telecommunications operators to retain all communications data for up to twelve months. Communications data is defined as data which may be used to identify or assist in identifying the sender, recipient, time, duration, type, method, pattern, or fact of a communication, along with system used to make a communication, its location and the IP address or other identifier of any apparatus used. Part 3 grants a long list of public authorities the power to self-authorise access to communications data for a list of ten broadly defined purposes where it is necessary and proportionate for them to do so. As well as the three main grounds on which interception and hacking can be authorised, these include: in the interests of public safety; for the purpose of protecting public health; assessing or collecting any tax, duty or levy payable to any government department; exercising functions relating to the regulation of financial services and markets or financial stability; identification of the deceased; or assisting investigations into alleged miscarriages of justice.[6] Judicial authorisation is required only for local authority access to communications data and requests by public bodies for communications data in order to identify a journalist's source.[7] In all other cases, a senior officer within a public authority will grant an authorisation and in exceptional circumstances this person does not even need to be independent from the investigation. This largely mirrors the existing regime under DRIPA, RIPA and associated Orders.

---

question of law, it is a matter of judgment and policy" to be determined not by judges but to be "entrusted to the executive".

[5] Public authorities must operate a "single point of contact system". Authorisations will last for one month and can be renewed. Telecommunications operators must take reasonable steps to provide information requested. Where an authorisation under Part 3 relates to conduct outside the UK, any requirements or restrictions imposed by the law of the country in which the activity will take place may be considered when establishing whether the operator took reasonable steps to comply. The Bill would place a series of obligations on the telecommunications provider to protect the data, with a view to ensuring its integrity, protect it from deletion, and prevent unlawful or unauthorised access or disclosure. A telecommunications operator would not be permitted to disclose the existence of a notice. The duty to comply with a retention notice would only apply extraterritorially to the extent that there is a duty to have regard to the requirement or restriction.

[6] Clause 53(7).

[7] Section 37 of the *Protection of Freedoms Act 2012* introduced a requirement for prior judicial authorisation for access to communications data by local authorities which is replicated in clause 66 of the Bill. Clause 68 of the Bill provides for judicial commissioner approval to identify or confirm journalistic sources.

11. Liberty supports the important role of communications data in missing persons situations, preventing and investigating serious crime. We do not believe however that the role of communications data in the investigation of crime justifies the *blanket* retention of the historic communications data of the entire population for 12 months. We also object to the lax access regime that currently exists under RIPA and is replicated in the Bill. The regime is also incompatible with recent court judgments and out of step with the legal direction taken by other European countries.

12. Liberty is currently representing David Davis MP and Tom Watson MP in their legal challenge to Data Retention and Investigatory Powers Bill, the provisions of which this Bill largely replicates. In July 2015 the High Court upheld their challenge and struck down sections 1 & 2 DRIPA, finding them incompatible with the British public's right to respect for private life and communications and to protection of personal data under Articles 7 and 8 of the EU Charter of Fundamental Rights. The High Court has found sections 1 and 2 of DRIPA unlawful on the basis that: they fail to provide clear and precise rules to ensure data is only accessed for the purpose of preventing and detecting serious offences, or for conducting criminal prosecutions relating to such offences; and: access to data is not authorised by a court or independent body, whose decision could limit access to and use of the data to what is strictly necessary. The ruling observes that: "*The need for that approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome."*[8]

13. The Government appealed the judgment to the Court of Appeal. In November 2015 the Court of Appeal referred two questions to the CJEU. The case will be heard on 12 April and the outcome of these references will have significant bearing on the lawfulness of the Bill.

Internet connection records

14. The Bill describes a new category of information – an internet connection record – and provides significant new powers (a) for the Home Secretary to require telecommunications operators to generate and retain 'internet connection records' (ICRs) for up to 12 months and (b) for a multitude of public authorities to gain access to ICRs. Current legislation specifically excludes the obligation to retain the most revealing data, previously described as 'web logs' but presented here as ICRs, that would explicitly identify the websites or internet communications services users have accessed.[9] The exact fields of information that would constitute an ICR have not been defined.

15. A plethora of public authorities will have access to ICRs, including HMRC, the Department for Work and Pensions (and a range of other government departments), NHS Trusts, the Gambling Commission, the Food Standards Agency, and several ambulance services.[10] The scale of public

[8] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin)
[9] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[10] *Investigatory Powers Bill 2016,* schedule 4, part 1

authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

16. Public authorities will not need a warrant to obtain an individual's detailed internet connection records. Provisions in the Bill would permit law enforcement and public authorities to gain access to ICRs for four purposes: to identify who or what device has sent a communication or used an internet service; to identify what internet communications services have been used, when and how; to identify when and where a person has accessed or made available illegal material; and now in the revised Bill, the additional power to reveal all internet connections of an identified person.[11]

17. ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. The Bill and accompanying documents have consistently failed to define the exact fields of information that would constitute an 'internet connection record' – indeed, there is nothing on the face of the Bill to limit the potential data fields within ICRs. In practice, ICRs would provide a detailed record of internet connections for every person in the UK and comprise a 12 month log of websites visited, communications software used, system updates downloaded, desktop widgets used (e.g. calendars, notes), every mobile app used (e.g. Whatsapp, Signal, Google Maps), and logs of any other device connecting to the internet, such as games consoles, baby monitors, digital cameras and e-book readers.

18. Liberty believes the case supporting this expanded data collection by ISPs, including its claimed benefit to law enforcement, is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[12] The difficulty of tracking some online criminals is a real problem. However, it is not a problem that mass surveillance programs – least of all this one - can solve. Bulk ICR retention will not be able to meet these three investigative purposes with greater efficacy than the targeted surveillance methods available for investigations. Further, there is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[13]. In fact, David Anderson noted that "*such obligations were not considered politically conceivable by my interlocutors in Germany, Canada or the US*", and therefore, "*a high degree of caution*" should be in order.[14] As the CJEU ruled in 2014,[15] the indiscriminate collection and storage of communications data is a disproportionate interference with citizens' right to privacy. It is unacceptable that Government is attempting to bypass this ruling, and to extend its policy of blanket data retention.

[11] *Investigatory Powers Bill 2016,* clause 54, subsection (4)
[12] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[13] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[14] Ibid
[15] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014

19. The population's detailed internet connection records will be collected and stored by ISPs. This has generated significant concern among ISPs and the public alike, as this new trove of extremely valuable data will be attractive to criminal hackers and difficult to protect. When a similar plan to collect 'web logs' was proposed in 2012, the Joint Committee on the Draft Communications Data Bill concluded that it would create a "*honeypot for casual hackers, blackmailers, criminals large and small from around the world and foreign states*".[16] This wealth of data in the wrong hands could be used for identity theft, scamming, fraud, blackmail, and even burglaries, as connection records can show when internet access occurs in or out of the house, representing a daily routine. This is an unacceptable level of risk to inflict on innocent internet users.

The Request Filter

20. The Bill contains provisions for a communications data 'Request Filter'[17] – a feature previously proposed in almost identical terms in the draft Communications Data Bill. The only change is that the Secretary of State must consult the Investigatory Powers Commissioner "*about the principles on the basis of which the Secretary of State intends to establish"* the filter.[18] The Request Filter is a search mechanism, allowing public authorities to conduct simple searches and complex queries of the databases that telecommunications operators are required to build and hold. The Joint Committee on the Draft Communications Data Bill described the 'Request Filter' proposed in that Bill as "*a Government owned and operated data mining device*",[19] which significantly positions the Government at the centre of the data retention and disclosure regime. Access to the Filter, and the data it produces, would be subject to the same self-authorisation process as all communications data. In practice, the 'Request Filter' would be a search engine over a "*federated database*"[20] of each and every citizen's call and text records, email records, location data, and now internet connection records, made available to hundreds of public authorities.

21. The Government is keen to portray the Request Filter as a 'safeguard' that "*will minimise the interference with the right to privacy".*[21] However, in reality it is a portal with power to put together a comprehensive picture of each of our lives. It raises many of the same concerns as a large and centralised store, with added security concerns of protecting multiple distributed databases. The ability to conduct complex queries could increase the temptation to go on 'fishing expeditions': that is, to sift data in search of 'relationships' and infer that any concurrences are meaningful. For example, given this power, authorities could use communications data to identify attendees at a demonstration and correlate this with attendance at other public or private locations in the 12 month period; or to identify those regularly attending a place of worship, and correlate this with

[16] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[17] Investigatory Powers Bill 2016, clause 58
[18] Investigatory Powers Bill 2016, clause 58, subsection (5); see also *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 232
[19] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[20] Ibid.
[21] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23

access to online radio websites, inferring risk.[22] Thus, this new ability could risk casting undue suspicion on thousands of innocent citizens.

Targeted interception

22. Powers for "targeted interception" of communications are contained in Part 2 of the Investigatory Powers Bill. There are three types of warrant – a "targeted warrant", a "targeted examination warrant" which permits the examination of domestic communications intercepted via Part 6 bulk interception powers, and a "mutual assistance" warrant which would be granted to an international partner who requests assistance under mutual legal assistance treaty. A targeted interception warrant can be issued by Secretaries of State (and in certain circumstances by Scottish Ministers[23]) on application by the intelligence services, the National Crime Agency, London Met, PSNI, PSS, HMRC and the Chief of Defence Intelligence subject to the weak judicial review process. Warrants can be issued on the three main grounds (which replicate existing RIPA grounds). The Bill provides for each warrant to last a minimum of six months – whereas under RIPA, serious crime warrants last three months.

Thematic warrants

23. While the Government has announced that it considers that under current legislation it has the power to issue thematic warrants, RIPA is in fact clear that warrants for targeted interception are required to name "*one person as the interception subject*" or "*a single set of premises*".[24] Clause 15 of the Bill radically reforms this requirement and prescribes that warrants may cover "*a particular person or organisation or a single set of premises*" or "*a group of persons who share a common purpose or who carry on, or may carry on, a particular activity* " or "*more than one person or organisation, or more than one set of premises, where the conduct authorised or required by the warrant is for the purposes of a single investigation or operation*" or for "*testing or training activities"*. This allows warrants to be issued in respect of people whose names are not known or knowable when the warrant is sought. The creation of thematic warrants in the Bill means that "external" communications intercepted in their billions under Part 6 could be trawled thematically for groups sharing a common purpose or carrying on a particular activity. It provides for an open-ended warrant that could encompass many hundreds or thousands of people. The expansive scope of these warrants, combined with the broad grounds for which they can be authorised, do not impose sufficient limits on the authorities' interception powers.

[22] GCHQ appears to practice similar data mining on the basis of supposed risk factors: *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities* – Ryan Gallagher, The Intercept, 25 Sept 2015.
[23] See clauses 19 & 20; where the application relates to persons or premises reasonably believed to be in Scotland.
[24] Section 8(1)(a) RIPA.

24. Liberty believes the scope of warrants permitted under clause 15 fails to comply with both common law and ECHR standards. In Zakharov v Russia[25] where the ECtHR found Russia's interception scheme in violation of Article 8 of the Convention, the Court cited the fact that Russian "*courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed."* [26] While thematic warrants do not relate to geographical location, they are sufficiently broad to violate Article 8 and need considerable amendment on the face of the Bill.

Bar on admissibility of intercept material in criminal justice system

25. Clause 48 maintains the section 19 RIPA bar on admissibility of interception material in criminal trials and Inquiries Act 2005 proceedings. There is not justifiable reason for maintaining the bar on intercept admissibility. The first consequence of lifting the ban would be an increase in successful prosecutions for serious offences. The latest Privy Council review into the issue, which reported in December 2014, concluded that a properly funded use of intercept material as evidence may result in a "*significant increase in the number of successful prosecutions*."[27]

26. Removal of the ban would also ensure that criminal defendants' rights are not breached in cases where interception has formed part of the investigation. The ECtHR has ruled that failure to disclose intercept evidence in certain circumstances will breach Article 6 ECHR.[28] Furthermore, the current ban has fuelled a corruption of domestic fair trial standards and abusive counter-terrorism laws, from control orders to TPIMs, to the corrosive growth of Closed Material Procedures across our justice system.

27. The Agencies have previously sought to block the admissibility of intercept on grounds that it would reveal sensitive methods or subject their activities to too great a scrutiny. In this new post-Snowden age of transparency, this argument cannot hold. Further, the existence of public interest immunity certificates and mechanisms to protect sensitive information will easily be able to protect matters which are genuinely sensitive. If material obtained by bugging, interception by foreign authorities and – under the terms of the Bill - hacking can be made admissible, there is no logical or coherent case for excluding intercept.

28. Successive Government-initiated reviews over the past two decades have concluded that intercept should be made admissible. A remaining objection from the Agencies seems to be on cost grounds. No doubt the requirement to transcribe and disclose intercept evidence would impose an additional burden on the authorities – as do all requirements to ensure that the criminal process is effective, efficient and just. But it would only be material that fulfills the test for

[25] (47143/06) 4 December 2015.
[26] Paragraph 265.
[27] See *Intercept as Evidence*, December 2014, Page 23.
[28] *Natunen v Finland* (Application no. 21022/04).

disclosure at trial that would need to be presented.[29] Given the current volumes of interception it would likely be only an infinitesimal fraction, and could have the salutary effect of focusing the authorities' minds on the primacy that should be given to criminal investigations, prosecutions and trials over speculative, intelligence gathering fishing expeditions.

Targeted hacking

29. Part 5 of the Bill makes provision for targeted hacking, euphemistically termed "*equipment interference*". There are two types of warrant: "targeted equipment interference warrants" and "targeted examination warrants", the latter of which can be issued in relation to material obtained via the bulk hacking powers in Part 6. Secretaries of State (and in certain circumstances Scottish Ministers[30]) can issue both types of warrants to the intelligence agencies and the Chief of Defence Intelligence where he or she considers it necessary and proportionate on the three main grounds. In contrast to the scheme for interception, the power to issue hacking warrants is also extended to chief constables, deputy chief constables, assistant chief constables and senior HMRC officers on application from junior HMRC and police officers '"or the purpose of preventing and detecting serious crime".[31] Warrants last for six months and can be renewed potentially indefinitely. Warrant applications will be subject to the weak system of judicial review discussed elsewhere in this document. Warrants can be modified by Ministers without the approval of a JC and modification can include changing the name, descriptions and scope of the warrant.[32] Chief constables are required to have their decisions to modify warrants reviewed by a JC, unless they consider the modification to be urgent.[33]

30. A hacking warrant authorises a person to interfere with any equipment for the purpose of obtaining "communications", "equipment data", or "any other information".[34] Therefore, there would be no limits as to what information could be obtained. Information can be obtained by *"monitoring, observing or listening to a person's communications or other activities and recording anything that is monitored, observed or listened to*".[35]

31. Hacking is potentially much more intrusive and damaging than any other forms of traditional surveillance such as bugging, interception and acquisition of communications data. Hacking can grant access to a large amount of highly sensitive data that has never been communicated or transmitted and can give the hacker access to all historical and future data stored on a device. Uniquely, it also grants the hacker total control over a device – phones and computers can be

[29] Section 3 of the Criminal Procedure and Investigations Act 1996.
[30] Clause 92.
[31] The majority of police forces can only hack devices and networks with a "British Isles connection" (although NCA has global powers) and this requirement is made out if any of the conduct, equipment interfered with or private info sought is in the British Islands.
[32] Investigatory Powers Bill 2016, clause 104
[33] Investigatory Powers Bill 2016, clause 106 subsection (3)(b)
[34]Equipment data is defined at clause 89.
[35] Clause 88(4).

turned on or off, have their cameras or microphones activated, and files added or deleted. Furthermore, all this can be done without the fact of the hack being known or knowable to the target.

32. The potential for intrusion is intensified in the digital age, when computers and mobile devices have replaced and consolidated our filing cabinets, photo albums, video archives, personal diaries and journals, address books, correspondence files and landline telephones. Increasingly these devices are also replacing our formal identification documents as well as our bank and credit cards. Devices may contain not only details about the user's personal circumstances (age, gender, or sexual orientation), but also financial information, passwords, privileged legal information and so on.

33. The repercussions for security can be hugely significant. When malware is deployed, there is often a risk of contagion, both overseas and at home. This was dramatically demonstrated by the Stuxnet virus, believed to be an American-Israeli cyberweapon, which intended to hack a single Iranian uranium enrichment facility but infected energy giant Chevron among many other companies as well as Microsoft PCs around the world.[36] The risks of hacks spreading 'in the wild' cannot be overstated: Professor of Security Engineering at Cambridge University, Ross Anderson wrote to the Science and Technology Select Committee, "*it is only a matter of time before interference with a safety-critical system kills someone"*.[37] There is also the risk that hacks can malfunction, with severe consequences for critical infrastructures and even international relations. For example, Snowden revealed that NSA hacking malfunctions were responsible for the outage of Syria's internet in 2012,[38] which may have caused simultaneous flight-tracking issues, and led government and opposition forces to erroneously blame each other for the incident.[39]

34. Given the potential damage to computer security and corresponding vulnerability to criminal elements that results from hacking, the use of this technology poses clear risks to those it is used against in a way that engages more rights than traditional forms of communications surveillance. Parliamentarians should consider the cost of widespread hacking by the authorities. Hacks create and maintain permanent vulnerabilities that can be further exploited by criminal elements, raising the potential for hacking to be counterproductive in the fight against serious crime. Cybercrime already costs the UK £34bn per year, and these proposed powers seem certain to ensure that this cost rises.

[36] *Obama Order Sped Up Wave of Cyberattacks Against Iran* – David E. Sanger, The New York Times, 1 June 2012
[37] *Written evidence regarding draft Investigatory Powers Bill* – Prof. Ross Anderson, 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25159.html
[38] *The Most Wanted Man in The World* – James Bamford, Wired, Aug 2014
[39] *Internet Shutdown Reported Across Syria* – Anne Barnard & Robert Mackey, The Lede: The New York Times Blog, 29 Nov 2012

35. As hacking by its nature requires the alteration of content on a target device or network, it also raises new questions concerning the potential for electronic surveillance to undermine the integrity of a device or material located on a device that may later be sought to be used in evidence in the justice system.

Thematic hacking

36. Clause 90 provides for thematic hacking warrants which amount to general warrants to hack groups or types of individuals in the UK A hacking warrant can further authorise hacking "equipment in a particular location" or "equipment in more than one location, where the interference is for the purpose of the same investigation or operation" or "equipment that is being, or may be used, for the purposes of a particular activity or activities of a particular description" as well as testing, developing or maintaining capabilities. In addition the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest."

Mass interception

37. Bulk interception results in billions of communications being intercepted each day without any requirement of suspicion or even any discernable link to a particular operation or threat. Liberty understands that the Agencies are currently handling 50 billion communications per day. To place this in context there are only 7 billion people in the world and only 3 billion with access to the internet. The ISC reported that at the end of 2014, there were just 20 section 8(4) warrants in place authorising the vast volume of interception under this power.

38. Part 6 Chapter 1 provides for the intelligence agencies to conduct bulk interception of "external communications". At first glance, the mass interception these powers permit appears targeted at overseas communications. This includes communications where either the sender or recipient is in the UK but their correspondent is not. Internet based communications have further eradicated the distinction between external and internal communications. As first disclosed through Liberty and other NGOs' litigation against the Government,[40] the ISC confirmed that Government considers that an "external communication" occurs every time a UK based person accesses a website located overseas, posts on a social media site overseas such as Facebook, uses overseas cloud storage or uses an overseas email provider such as Hotmail or Gmail. Searches on Google are counted as an external communication. The Joint Committee on the draft Bill reported, "*given the global nature of the internet, the limitation of the bulk powers to 'overseas-related' communications may make little difference in practice to the data that could be gathered*

[40] https://www.liberty-human-rights.org.uk/sites/default/files/Witness%20statement%20of%20Charles%20Farr%20on%20behalf%20of%20the%20Intelligence%20Services%2016th%20May%202014.pdf#original

under these powers. We recommend that the Government should explain the value of including this language in the Bill".[41] However, no such explanation has been given.[42]

39. Material collected under a bulk interception warrant can be examined in accordance with "specified purposes" written into the warrant. The only guidance the Bill provides as to what these purposes may cover is a requirement that it must be more than simply e.g. "the interests of national security", but that "the purposes may still be general purposes". Reporting on the draft Bill, the ISC noted that no details had been made available as to what the operational purposes may be, finding it to be, *"completely unsatisfactory: it contradicts the primary purpose of the draft Bill, to provide some much-needed transparency in this area".*

40. While the criteria for selection cannot be "referable to an individual known to be in the British Islands at that time" where "the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual"[43] it is likely that for the vast majority of communications intercepted, the Agencies will have no knowledge as to where the senders and recipients are located. If it later becomes apparent that a target is in the UK (even if they have, in fact, been here all along) that process of selection and examination can continue for 5 days.[44] It seems likely that there will be many cases in which it will be unclear where an individual is currently located. The high threshold of 'knowing' that somebody is in the UK will allow for widespread examination in cases where there is an element of doubt about an individual's current whereabouts. If examination would be in breach of the weak prohibition in clause 134 outlined above, the relevant agency can apply for a targeted interception warrant to examine the material anyway.[45]

Bulk communications data acquisition

41. On the day that the draft Bill was published, the Home Secretary announced that the Agencies have been acquiring the communications data of the UK population in bulk under the vaguely worded section 94 of the Telecommunications Act 1984 since 2005. This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers. Parliamentarians had previously been led to believe that communications data retention and acquisition by the Agencies took place under RIPA and DRIPA as the legislation specifically permits the Agencies to acquire communications data on national security and serious crime grounds.

[41] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 24
[42] The point is avoided in *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny,* March 2016, p.52
[43] Investigatory Powers Bill 2016, clause 134, subsection (4).
[44] Investigatory Powers Bill 2016, clause 134, subsection (7).
[45] Investigatory Powers Bill 2016, clause 13.

42. By contrast with bulk interception, where a half-hearted attempt is made to tie surveillance to "overseas" communications, acquisition has as its main purpose the acquisition of data held by UK based companies. The power also purports to have extraterritorial effect.

Bulk hacking

43. The use of targeted hacking by the Agencies was only very recently acknowledged by Government through the publication by the Home Office of an Equipment Interference Code of Practice although it made no mention of bulk hacking capabilities. The scope of a bulk equipment interference warrant under the Bill is astonishingly broad, paving the way for intrusions over and above those revealed by Snowden, pinpointing hacking as the modus operandi of our expanding surveillance state. As with bulk interception, the main (but not sole) aim of the warrant must be to facilitate the obtaining of overseas data, but this does not prevent data on UK residents being collected as a subsidiary objective, or in pursuit of the main aim. A bulk hacking warrant can authorise interference with any equipment whatsoever, for the purposes of obtaining communications, equipment data or "information". Bulk warrants can be issued in the interests of national security, economic wellbeing, or for the prevention and detection of serious crime.

44. Following scrutiny of the draft Bill, the ISC reported that "*the Committee has not been provided with sufficient compelling evidence as to why the Agencies require Bulk Equipment Interference warrants"* and "*therefore recommends that Bulk Equipment Interference warrants are removed from the new legislation"*[46]*.* However, this unjustified power remains in the revised Bill against the ISC's recommendation. In fact, in response to the ISC's recommendation, the Home Office admitted that "*the Secretary of State is not able to fully assess at the time of issuing the warrant the necessity and proportionality of each interference".*[47]

45. Bulk hacking is by its nature indiscriminate, as acknowledged by the Draft Bill's Explanatory Notes: "*bulk equipment interference is not targeted against particular person(s), organisation(s) or location(s) or against equipment that is being used for particular activities".*[48] Instead, systems, services and software that have been carefully constructed to provide security are intentionally corrupted to impose the eyes and ears of the intelligence agencies on every phone call, text message and web click. In the offline world, granting this power would mean allowing secret services to break into and bug every house, leaving broken windows[49] for anyone else to get in but all without the individual whose house it is knowing this has happened. In the digital world, even more rich and revealing data can be gathered as computers and mobile devices have taken the place of our filing cabinets, diaries, calendars, video archives, photo albums, book shelves,

[46] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation D
[47] *Investigatory Powers Bill: Government Response to Pre-legislative Scrutiny,* March 2016, p.80
[48] *Draft Investigatory Powers Bill 2015: Explanatory Notes*, p. 83
[49] A US intelligence official described state hacking using a similar analogy: *"You pry open the window somewhere and leave it so when you come back the owner doesn't know its unlocked, but you can get back in when you want to".* Quoted in, *U.S. spy agencies mounted 231 offensive cyber-operations in 2011, documents show* – Barton Gellman & Ellen Nakashima, 30 Aug 2013

address books and correspondence files. Furthermore, this digital forced entry does not only entail intrusion into highly personal spaces, but control over them. For example, spies can alter, add or delete files, send messages, turn devices on or off, or covertly activate cameras and microphones. As demonstrated by GCHQ's OPTIC NERVE program,[50] this could literally mean subverting millions of webcams into covert home surveillance cameras. Such extraordinary power over the private lives of citizens fundamentally alters the relationship between citizen and state, and will breed distrust in law enforcement while having potentially significant repercussions for the Rule of Law. In human rights terms, such sweeping and speculative powers can never meet a test of necessity and proportionality.

46. Bulk hacking critically damages the security of complex modern technologies upon which modern society is built. The Five Eyes intelligence agencies find security flaws in software and stockpile them for later 'equipment interference', rather than inform developers so that they can be fixed or responsibly dealt with. As such, mass hacking goals prevent intelligence agencies from protecting the public's cybersecurity. President Obama's Review Group of Intelligence and Communications Technologies criticised this approach, concluding: "In almost all instances, for widely used code, it is in the national interest to eliminate software vulnerabilities rather than to use them for US intelligence collection. Eliminating the vulnerabilities – 'patching' them – strengthens the security of US Government, critical infrastructure, and other computer systems."

47. "Bulk equipment interference" is an especially excessive, dangerous and destructive power designed to achieve international mass surveillance by any means. If passed, this and other bulk powers will gradually eradicate private spaces from modern society whilst damaging national security. Bulk hacking is one of the most objectionable powers in the Bill, jeopardising human rights in the present and future.

Bulk Personal Datasets

48. Part 7 provides the Agencies with powers to acquire 'bulk personal datasets' (BPDs). This power does not currently exist. BPDs are essentially databases held either by the private or public sector and are defined in the Bill by reference to their nature "as *a set of information that includes personal information relating to a number of individuals* where the *nature of the set is such that it is likely that the majority of the individuals are not, and are unlikely to become, of interest to the intelligence service."* [51]

49. Acquisition, retention and examination of these databases will be governed by a warrant system similar to that for bulk interception and bulk hacking. Warrants are issued by the Secretary of State on application from the three Agencies and the process mirrors the framework in place for

[50] In which several millions of Yahoo users' webcam calls were intercepted to take and store images for a facial recognition program. *Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ* – Spencer Ackerman & James Ball, The Guardian, 28 Feb 2014 (http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo).
[51] Investigatory Powers Bill 2016, Clause 174

warrants for other bulk powers in Part 6. Judicial involvement is limited to the flawed judicial review model.

50. "Class warrants" concern applications for *descriptions* of personal data – for example, 'health data' or 'travel data'. Under the terms of the Bill, this is the default type of BPD warrant. Both the ISC[52] and the Joint Committee[53] recommended that Class Bulk Personal Datasets be removed from the Bill – yet they remain. The ISC reported that the "*acquisition, retention and examination of any Bulk Personal Dataset is sufficiently intrusive that it should require a specific warrant".*[54]

51. 'Specific bulk warrants' can be applied for (a) where the requesting agency wants to request a bulk dataset that doesn't fall within a class described in a class BPD warrant or (b) where it does fall within a class warrant but where the intelligence agency at any time considers that it would be "appropriate" to seek a specific BPD warrant. Specific BPDs may apply to the most sensitive type of databases – such as mental health hospital data, or patient identifiable FGM data. Applications must include a description of the dataset to which it relates and an explanation of the operational purposes for which the intelligence service wishes to examine it. Specific BPD warrants may also authorise obtaining, retaining and examining bulk personal datasets that do not exist at the time the warrant is issued but may "reasonably be regarded as replacements" for the a dataset that has been sought.

52. Despite the requirement of a warrant for human examination of BPDs, the little available information indicates that BPDs are routinely electronically analysed. The power to collect BPDs is almost unlimited and in practice involves far more expansive and intrusive, yet entirely secret, databases on millions of people. These vast, potentially population-level databases are integrated to produce profiles so intrusively detailed that they enable the Agencies to "*understand a subject of interest's behaviour and connections".*[55] This indicates a deeply disturbing practice of data hoarding and further intrusive data mining to speculatively identify "*potential agents"* and generate "*subjects of interest"*.[56] Identifying subjects of interest without evidence of criminality is highly likely to involve discrimination and appears to be more characteristic of an authoritarian regime than a democracy.

53. No argument is even attempted that BPDs are necessary or proportionate for Article 8 HRA purposes. The ISC reported that the Agencies told them that BPDs are an "*increasingly important investigative tool*" to "*enrich*" information obtained through other techniques. "Enriching" and "relevant" does not meet the legal threshold for lawfulness.

---

[52] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation F
[53] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 42
[54] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation F
[55] Supplementary written evidence to the Joint Committee on the draft Investigatory Powers Bill (IPB0165) – Theresa May, December 2015; p.14
[56] Ibid.

Is mass surveillance effective?

54. While Liberty supports the use and value of targeted intrusive surveillance powers, we believe that the speculative mass interception of communications; retention and acquisition of communications data; bulk hacking and bulk personal dataset acquisition as provided for in the Bill is unlawful, unnecessary and disproportionate.

55. The Government has not made a serious operational case for bulk surveillance. The bulk powers are presented in the Bill as "*crucial to monitor known and high-priority threats"* and also as "*a vital tool in discovering new targets and identifying emerging threats".*[57] Following renewed criticism during the Joint Committee's scrutiny of the Draft Investigatory Powers Bill, the Home Office was compelled to produce further written evidence to support the case for bulk powers. It also published an 'Operational Case for Bulk Powers' with the publication of the revised Bill on 1 March 2016. However, the documents have provided only a mix of anecdotal and hypothetical evidence. With only vague and limited information provided, it is impossible to assess whether claimed security outcomes could be achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the Agencies' disposal. In nearly all of the examples, references are made to known terrorists, contact with known suspects, visitation to known illegal sites, or a specific "intelligence operation".

56. In every major terror attack in the Europe and USA since (and including) the 9/11 attack, including the Madrid bombings in 2004, the London 7/7 bombings in 2005, the murder of Lee Rigby in 2013, the Boston bombings in 2013, the January attack on the Charlie Hebdo offices and the Paris attacks in November 2015, some or all of the culprits have been known to the intelligence agencies. The failure to prioritise or action intelligence appropriately is commonly attributed to both human error and pressured resources – these reasons featured in the reports on the London 7/7 bombings[58] and the murder of Lee Rigby.[59]

57. No evidence has thus far been provided to illustrate a unique or critical contribution of bulk powers, as opposed to targeted powers, in combatting serious crime or indeed terrorism. Whilst in some cases bulk powers may offer helpful contributions to intelligence gathering, they have not (as far as is publicly known) proved critical in saving lives nor unique in providing intelligence that can be acquired through targeted methods. Furthermore, bulk powers clearly risk burdening intelligence agencies, whose incredible resources may be more effectively directed in targeted surveillance operations.

Confidential and privileged correspondence

[57] Guide to powers, p.20 para. 33
[58] *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005* – Intelligence and Security Committee, 8 July 2008
[59] *Report on the intelligence relating to the murder of Fusilier Lee Rigby* – Intelligence and Security Committee, 25 Nov 2014

58. Liberty believes that the authorisation process for all types of surveillance in the Bill falls short of that which is required by human rights standards, and proposed 'safeguards' in practice will provide remarkably insufficient protection.

MPs, Peers, MSPs, AMs, MLAs, MEPs

59. The communications data of MPs, Peers and other elected representatives receives no explicit protection in the Bill. Data will remain accessible to a multitude of public authorities through the general system of self-authorisation. MPs' communications and devices would also be subject to mass interception, hacking and communications data acquisition by the Agencies under Part 6 of the Bill and MPs' personal data would be acquired in bulk under Part 7. The only 'safeguard' is around targeted hacking and interception, if the purpose is interception of communications relating to constituency matters – not national matters or private/other matters. The 'safeguard' in that instance would be a requirement that the Secretary of State 'consults' the Prime Minister before authorising activity.

60. Liberty believes it is illogical to suggest that an adequate replacement to the previous complete prohibition on surveillance of politicians as contained in the Wilson Doctrine is to expressly allow surveillance on all politicians, only requiring the Secretary of State to consult with the Prime Minister prior to authorising interception or hacking if the express purpose is the interception of constituency communications. Instead of securing an independent authorisation process, involving two politicians rather than one would make the process more political rather than less. It is difficult to see why Members of Parliament and other elected representatives should have confidence that "consultation" with the Prime Minister can act as a bulwark against unjustified surveillance of constituency communications. Liberty does not suggest that parliamentarians should be above the law, but in recognition of their unique constitutional role we advocate a strong legislative presumption against surveillance of elected representatives, that can only be rebutted in in clear and specific circumstances overseen by judicial commissioners.

Journalists

61. Journalists generally have no protection in the Bill, and have no protection at all from interception, hacking, or any bulk powers. The one supposed safeguard is in clause 68, which would require a public authority to apply to a Judicial Commissioner to confirm an authorisation to obtain communications data if the stated purpose of access is to identify or confirm a journalistic source, However, this is a significant reduction of the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE), which as the NUJ has pointed out, protects not just the identity of sources but related journalistic material:

    "Source protection does not just apply to the identity of the source but also to all matters relating to and communications between the journalist and the source. This includes the

person's name; personal data, voice and image. It also includes the unpublished content of information and the circumstances of acquiring the information".[60]

The Bill fails to define a journalist, and offers a questionable definition of journalistic sources (cl. 68(7)) that is unlikely to meet the standard set by recent case law from ECtHR[61].

62. In September 2014, it was revealed that the Metropolitan Police had used the RIPA internal authorisation route to access communications data of a journalist from The Sun newspaper as part of their "plebgate" inquiry, circumventing the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE). In response to public outcry, the Government updated the Acquisition and Disclosure of Communications Data Code of Practice, advising law enforcement that where an application to access the communications data of a journalist in order to determine the source of journalistic information is made, it must be via the PACE route. PACE sets out the special procedures that must be followed if law enforcement agencies wish to access material that may be journalistic or confidential journalistic material. To access journalistic material, which comes under the broad definition of *"material acquired or created for the purpose of journalism",* an application must be made to a judge. The conditions that must be met before the judge can grant a warrant include: that there are reasonable grounds for believing an indictable offence has been committed; the material is likely to be of substantial value; and, other methods of obtaining the material have been tried or are bound to fail. In addition to these requirements, the judge must be convinced that it is in the public interest to grant access to the materials. In order to access confidential journalistic material – namely information relating to sources – PACE sets out that a warrant will only be granted if prior to PACE it would have been possible to access source material via a power contained in primary legislation. As a result, it is only in very rare circumstances that an order will be made under PACE to reveal confidential journalistic material. Unlike the process contained in the Bill, both these processes are *inter-partes*, giving the journalist the opportunity to make their case to the judge. It is also possible to gain access to confidential journalistic material under the Terrorism Act 2000.

63. The mechanism introduced by clause 68 is inadequate to secure the independence and vitality of our free press. It allows for a circumvention of the established and much more rigorous PACE process, creating a system in which communications data can be accessed without the PACE protections.

Lawyers

64. Legal privilege is an essential protection in a free society governed by the Rule of Law. The doctrine is intended to ensure fair trial integrity and ensure both defendants and civil claimants

[60] *Written evidence on Investigatory Powers Bill* – NUJ, 21 Dec 2015
[61] *Guseva v Bulgaria* application no. 6987/07, 17 Feb 2015, para 38 and the cases cited.

can communicate with their lawyers without inhibition. Legally privileged communications are those between a client and their lawyer which come into existence for the dominant purpose of being used for legal advice, or in connection with actual or pending litigation. The Bar Council reminded the Joint Committee scrutinising the Bill that, "*The privilege is that of the client, and failure to protect that right against the state amounts to a significant inroad into a long-standing principle, which has formed an important foundation of our rule of law".*[62] Without assured confidentiality, clients feel unable to speak openly with their lawyers and may not know about the proper defences available to them, thus obstructing a fair trial. Breaching privilege can also obstruct justice by jeopardising the integrity of criminal trials, or giving the state an unfair advantage.[63] Legal privilege does not apply where client-lawyer communications are made in furtherance of a criminal activity.

65. Legal privilege has traditionally been protected at common law and under Article 6 HRA. Like the Wilson Doctrine it was considered absolute. However, public interest litigation brought over the course of 2014-15 has revealed a set of internal Government policies that render LPP illusory.

66. Abdel Hakim Belhaj alleges he is a victim of CIA-SIS rendition and torture and is attempting to hold the UK Government to account for this. During the course of legal proceedings and in the wake of the Snowden revelations, his lawyers came to fear that they were under surveillance. In the course of proceedings before the Investigatory Powers Tribunal the Government conceded that *"since January 2010 the policies and procedures for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material have not been in accordance with human rights legislation specifically Article 8(2) of the ECHR."*[64] Instead, they allowed for legally privileged communications of between a victim of SIS-CIA rendition and torture and his lawyer to be targeted for surveillance. It is unacceptable that the Government could have used its surveillance powers to undermine attempts to hold it to account for its complicity in torture, but that is what existing legislation has permitted and this would remain permitted under the terms of the Bill.

67. The Bill therefore represents an important and timely opportunity to ensure statutory protection for LPP. However, the only 'safeguard' for protecting lawyers from targeted interception or hacking, or targeted examination following bulk interception or hacking – if the stated purpose is to intercept or examine material subject to legal privilege (not if the purpose is more generally investigative) – is that there are deemed to be "*exceptional and compelling"* circumstances.[65] This

[62] *Written Evidence on Investigatory Powers Bill* – Bar Council, 21 Dec 2015
[63] Ibid.
[64] "Government concedes policies on lawyer-client snooping were unlawful", Reprieve, 15 February 2015, available at - http://www.reprieve.org.uk/press/government-concedes-policeson-lawyer-client-snooping-were-unlawful/

[65] See clauses 25, 100, 135 and 171

'safeguard' is not accompanied by any objective threshold or definition in the Bill, and therefore is a subjective value judgement that provides no real protection or reassurance.

Encryption

68. Despite the Home Office's claim that the draft Investigatory Powers Bill "*will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA",*[66] it presents a renewed and expanded assault on encryption that will dramatically diminish privacy and security online. Although it is situated rather modestly in the Bill, clause 217 in Part 9 contains the significant power for a Secretary of State to oblige telecommunications operators, both domestic and overseas, to covertly remove encryption from their services, thus enabling the Government to intercept any communications or data.[67]

69. The State already has several means to circumvent encryption. But despite these powers to require decryption and circumvent encryption via hacking, the Bill proposes to renew the power to force "*the removal of electronic protection"* from communications services, and expand capabilities to remove encryption by broadening the framing of the power. RIPA 2000 and paragraph 10 of the Schedule to *the RIPA (Maintenance of Interception Capability) Order 2002*[68] grants the State the power to force "*public telecommunications services"* to remove encryption. Under this Bill, communications services can be imposed with obligations not only to remove "*electronic protection"*, but with additional obligations including those "*relating to the security"* of the service provided, relating to "*apparatus owned or operated"* by the service, and "*obligations to provide facilities or services of a specified description" – "among other things",*[69] which remain undefined. Whereas provisions under RIPA oblige "*public telecommunications services"*[70] [71] to remove encryption, the Bill would oblige any "*telecommunications operator",*[72] which is defined as *"a person who offers or provides a telecommunications service to persons in the United Kingdom, or controls or provides a telecommunications system which is (wholly or partly) in the United Kingdom or controlled from the United Kingdom."*[73] This expanded definition would include not only public services such as Gmail, Facebook, Twitter and Dropbox, but also private offices, businesses, law firms, government department networks (such as the NHS), and institutional networks such as universities. There is no judicial authorisation required for either notice. The recipient of such a notice must comply with it[74] but must not disclose the existence or contents of

[66] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* p.29
[67] Investigatory Powers Bill 2016*,* clause 217, subsection (4)
[68] Regulation of Investigatory Powers Act 2000*,* section 12 (1);
[69] Investigatory Powers Bill 2015*,* clause 217, subsection (4).
[70] Regulation of Investigatory Powers Act 2000*,* section 12 (1).
[71] The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002*,* section 10.
[72] Investigatory Powers Bill 2016*,* clause 217, subsection (2).
[73] Investigatory Powers Bill 2016*,* clause 223, subsection (10).
[74] Investigatory Powers Bill 2016*,* clause 218, subsection (9)

it.[75] Thus, were an Apple v FBI scenario to occur in the UK, Apple would not be able to disclose even the fact that it had been served with a notice, let alone challenge it in court.

70. Encryption is now a widely used standard to protect the ever-expanding uses of communications technologies in an increasingly hostile digital environment: from mobile phones and smart phones to personal hard drives, online banking and e-commerce, critical infrastructures, transport networks, institutional and business computer networks, cloud storage, emailing and messaging, web browsing and online shopping. The renewed and extended assault on encryption in the Bill demonstrates a misguided commitment on the part of the State to undermine secure spaces in the furtherance of mass surveillance ambitions. The Government's coercion of telecommunications operators to maintain covert interception capabilities would force products and services to be designed with the required insecurity built-in.

Intelligence Sharing

71. Liberty is disappointed that the Bill is silent on the intelligence sharing relationship between the Agencies and foreign intelligence agencies, in particular the Five Eyes. The ISC noted that the Bill "does not, therefore, meet the recommendations made in the Committee's Privacy and Security Report that future legislation must set out these arrangements more explicitly, defining the powers and constraints governing such exchanges". The ISC strongly recommended that international data sharing be included in the revised Bill, remarking that "the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception". However, international raw intelligence sharing remains absent from the revised Bill.

72. The Reviewer's report described an "international trade in intelligence" between the Five Eyes partners – the UK, USA, Canada, Australia and New Zealand. Insofar as material gathered by the British services is shared with other countries, the report explained that the security services take the view that under their founding statutes, information can be shared if it is "necessary for the purpose of the proper discharge of the security and intelligence agencies' functions" and that when it is considered that this test is met certain RIPA safeguards apply. However, the report concluded that "in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State." The report also stated that RIPA imposes no limits on the sharing of communications data obtained from service providers with overseas governments, although the Acquisition Code provides some guidance for dealing with requests for information.

73. RIPA and the Codes of Practices are silent on British services receiving or accessing information from foreign services, with the security services only limited by the "general constraints" on their

[75] Investigatory Powers Bill 2016, clause 218, subsection (8)

actions in various statutes. It was only during the course of Liberty's legal action against the security services in the IPT that limitation information about the way in which the security services approach such situations was revealed. In its first finding against the Agencies, the IPT held that prior to these disclosures, the framework for information sharing was not sufficiently foreseeable and was not therefore "in accordance with law". The Tribunal held that as a result of the fact that the litigation had resulted in disclosures of information, the security services were no longer acting unlawfully when accessing information from the U.S.

74. David Anderson's report recommended that information sharing with foreign countries be subject to strict, clearly defined and published safeguards. The report added that the "the new law should make it clear that neither receipt nor transfer as referred to in recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK". Such safeguards and guarantees are notably absent from the Bill.

Oversight

75. The Bill proposes that the Investigatory Powers Commission (IPC) will replace the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCom). Their roles will be divested in the newly created Investigatory Powers Commissioner and fellow Judicial Commissioners who will therefore have dual responsibility (a) for reviewing Secretary of State and chief constable surveillance warrants and (b) for oversight of the use of intrusive powers. The IPC is additionally required to keep under review any aspect of the functions of the Agencies as directed by the PM[76] and these directions need not be published if PM considers it would be contrary to the public interest or prejudicial to the three grounds or the continued discharge of the functions of any public authority whose powers are reviewed by the IPC. The IPC must make an annual report to the PM about the carrying out of the functions of the JCs

76. However, this confuses the roles of authorisation and oversight. It is constitutionally inappropriate for those involved in the decision-making process to also bear responsibility for oversight of those decisions. The conflation of these responsibilities gives rise to a conflict of interest. This is demonstrated by clause 196, which imposes obligations on Commissioners not to act in a way that may inhibit the effectiveness of particular operations when undertaking oversight functions. JCs are then told to disregard these obligations in circumstances where the JC is involved in reviewing warrants.

77. The Home Office has refused to establish an independent Intelligence and Surveillance Commission as a statutory oversight body, despite recommendations from the Joint Committee and the Government's Reviewer of Terrorism Legislation, David Anderson QC. Instead, it has

[76] Investigatory Powers Bill 2016, clause 197.

retained the proposal of a team of Judicial Commissioners, appointed by the Prime Minister, funded by the Home Secretary, to both authorise *and* oversee the use of investigatory powers. The Home Office has dismissed recommendations that the Judicial Appointments Commission or the Lord Chief Justice appoints Judicial Commissioners; that their dual functions are separated for proper, independent oversight; and indeed that "*it is inappropriate for the Home Secretary alone to determine the budget of the public body which is monitoring her exercise of surveillance powers".* This authorisation and oversight proposal will clearly be unable to inspire public trust.

Post surveillance notification

78. Liberty believes that JCs should be under a mandatory statutory duty to notify those subjected to surveillance once a particular operation or investigation has ended. At present, unlawful surveillance only comes to light as a result of a chance leak, whistleblowing or public interest litigation brought by Liberty and other NGOs and concerned citizens. This is deeply unsatisfactory.

79. If a person's Article 8 and other HRA protected rights have been infringed, in order to have access to an effective remedy as required under human rights law, the person must first be made aware of a possible breach. This was stated by the ECtHR in *Klass v Germany* in 1978 and reiterated in *Weber and Saravia v Germany* in 2006:

> *"The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively"* (see Klass and Others, cited above, pp. 26-27, § 57).[77]

80. In *Zakharov v Russia* the ECtHR found that that judicial remedies for those subjected to interception in Russia were generally ineffective, particularly in light of the total absence of any notification requirement with regard to the interception subject, without any meaningful ability of retrospective challenges to surveillance measures.

81. The Bill provides a new power for the the Investigatory Powers Commissioner to inform someone subjected to a surveillance error by a public authority (but not a CSP) if the IPC is made is aware of it; considers it sufficiently serious; and that it is in the public interest; and that it does not prejudice national security, the prevention or detection of crime, the economic well-being of the UK, or the continued discharge of the functions of any intelligence service.[78] For it to be serious it must have caused '*significant prejudice or harm to the person concerned'*. The Bill states that a

[77] Weber and Saravia v Germany, 2006, application 54934/2000, paragraph 135.
[78] The definition of an error includes failure to comply with requirements under this Act and in Code of Practice under Schedule 6.

breach of the HRA is not sufficient for an error to be considered a serious error.[79] Before making its decision the IPC must ask the public authority responsible for the error to make submissions to the IPC about the matter concerned. This is a narrow, arbitrary and highly discretionary power that will relate only to the most serious errors that the JCs discover during their very limited audit of the use of surveillance powers. It highlights the conflicted position that JCs may find themselves in and it does not discharge the Government's human rights obligations to provide post-notification by default unless it can justify continued secrecy.

Reform of the Investigatory Powers Tribunal

82. Liberty has long advocated reform of the Investigative Powers Tribunal, the secretive body which hears cases involving state surveillance. The Tribunal is not required to hold oral hearings; hearings do not need to be *inter-partes;* it cannot disclose the identity of a person who has given evidence at a hearing or the substance of the evidence unless the witness agrees. If the Tribunal finds against a complainant it cannot give its reasons for doing so, meaning that the individual does not know whether no surveillance took place or whether lawful surveillance took place, and if it upholds a complaint is it only required to provide the complainant with a summary of its reasoning. Its judgements are therefore opaque.

83. As Justice noted in their 2011 report, half of the successful complainants to the IPT concerned cases where those concerned had been notified of surveillance. Of the three successful claims brought in 2015, the cases were brought only as a result of the Snowden disclosures. To this end, the most significant reform that could improve the effectiveness of the IPT would be a requirement for post-notification of all targeted surveillance.

84. Liberty encourages parliamentarians to establish a principle of open proceedings in the IPT, with the option for the tribunal to determine that closed or partly closed hearings are in the interests of justice. The opposing parties should be made aware of any request for a closed hearing, or to submit closed evidence. In cases where closed sessions are necessary, the IPT should appoint a Special Advocate to represent the interests of the excluded party.

Appeals

85. Liberty welcomes the granting of a right of appeal from the IPT in the Bill which inserts new clause 67A RIPA. This creates a right of appeal and specifies that leave to appeal will only be granted if the appeal would raise an important point of principle or practice or there is another compelling reason for granting leave. Leave for an appeal can be granted by the Tribunal or the Court that would hear the appeal.

86. Liberty believes that the right of appeal should be extended to cover any IPT ruling on a point of law,, as was the case in Liberty's recent claim in the IPT. Liberty further advocates that the IPT

[79] Investigatory Powers Bill 2016, clause 198, subsection (3)

should be given the power to make a declaration of incompatibility under the *Human Rights Act 1998* and notes that David Anderson supported this recommendation.

Silkie Carlo
Bella Sankey
Sara Ogilvie