LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's written evidence on the Draft Investigatory Powers Bill

December 2015

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

CONTENTS **PAGE**

Executive Summary

Liberty welcomes the publication of a new law to regulate State surveillance in the UK. We support the lawful, targeted and proportionate use of intrusive powers to detect and prevent serious crime. But since the inception of the Regulation of Investigatory Powers Act 2000 (RIPA) we have argued that the authorisation, scope and oversight arrangements for the UK's surveillance regime are in need of urgent and radical overhaul. The Government's Reviewer of Terrorism's investigatory powers review condemned the status quo under RIPA and other enabling legislation as *"undemocratic, unnecessary and – in the long run – intolerable."*[1] This stark and realistic assessment of the need for transparency and reform was in glaring contrast to the Government's repeated claims since 2013 that the current legislative framework contains "robust" safeguards to meet our human rights obligations.

The Snowden revelations of 2013 and subsequent litigation brought by Liberty and others shows how far we have moved from a model whereby those under suspicion are targeted and the innocent are left free from state intrusion. We have in so doing moved far away from the requirements of human rights law. Liberty currently has litigation pending both before the European Court of Human Rights (ECtHR) in Strasbourg & the Court of Justice of the European Union (CJEU) challenging key aspects of the current legislative framework which is replicated and extended in the Draft Bill. While we await further judgment in both cases, the CJEU judgment in *Digital Rights Ireland*[2] in 2014 and the recent judgment of the ECtHR in *Roman Zakharov v Russia*[3] are instructive on the many ways in which the Draft Bill falls woefully short of ECHR standards.

This briefing examines the various powers, mechanisms and purported safeguards in the Draft Bill. We identify a number of the ways in which the claims made about the value and utility of the Bill are not supported by the evidence. We examine and make recommendations on the **process for authorisation of surveillance warrants** and in particular the need for **one-stage judicial authorisation for all warrants** and **reform of the legal tests** for the use of intrusive powers. We **critique the existing framework for communications data retention and acquisition replicated at Parts 3 & 4 of the Draft Bill and challenge the so-called operational case for bulk 'ICR' retention and the Request Filter.** We make recommendations **to improve the system for targeted interception contained in Part 2 and targeted hacking in Part 5 to make both capabilities compliant with our human rights framework and capable of producing legitimate and reliable evidence in criminal trials.**

We examine the Part 6 & 7 proposals to legislate for **new and unusual mass surveillance powers**, including: bulk interception; bulk communications data acquisition; bulk hacking and the acquisition of

[1] David Anderson QC, A Question of Trust, paragraph 35.
[2] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).
[3] Roman Zakharov v. Russia, 4th December 2015,*(Application no. 47143/06)* available at - http://hudoc.echr.coe.int/eng-press#{"itemid":["001-159324"]}

Bulk Personal Datasets and make the **case against mass surveillance which is simultaneously unnecessary, disproportionate, counter-productive and a stain on our human rights record**. **We suggest reforms to provide overdue statutory protection to the confidential and privileged communications of MPs, Peers, MSPs, AMs, MLAs, MEPs, journalists and lawyers**. We point out the many ways in which the authorities can use targeted means to seek access to suspicious encrypted communications and **advocate for the preservation and promotion of global encryption standards** as an increasingly important social good. We comment on the **absence of a statutory framework for intelligence sharing in the Draft Bill** and examine proposed changes to the oversight regime, arguing for **the conflicting functions of the newly created Investigatory Powers Commission to be vested in two institutionally separate bodies and for the creation of a legislative presumption in favour of post-notification to those subjected to targeted surveillance.**

The authorisation process for surveillance warrants

1. The Draft Bill retains the power for the Secretary of State to issue interception warrants and provides new powers for the Secretary of State to issue hacking and bulk warrants. Bulk and targeted warrants of all types are issued by the Secretary of State, on application from the three intelligence agencies, where she considers it necessary and proportionate on the basis of three broad grounds.[4] The Secretary of State can also issue targeted interception and targeted hacking warrants to a range of law enforcement bodies. Chief constables are granted the power to issue targeted hacking warrants on application from police constables.

2. The process for issuing warrants is similar to the present process for issuing interception warrants subject to a new requirement for a judicial commissioner (JC) to review a warrant before it is issued. The Bill stresses that the decision to issue a warrant is taken *personally* by the relevant Minister or, in urgent cases, by a designated senior civil servant.[5] 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."*[6] If a JC decides to refuse to approve a decision to issue a warrant he/she must give reasons and the Minister issuing the warrant can make a fresh application to the Investigatory Powers Commissioner (IPCr).[7] 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. In urgent cases warrants can be issued without the authorisation of a JC, but the JC must give ex post facto authorisation within 5 days. In these circumstances a JC may, but is not required to, order the destruction of the material obtained. There is no requirement for JCs to notify those subjected to surveillance after the surveillance has ceased.

3. Part 8 of the Draft Bill provides for the creation of the IPCr and the JCs who will be appointed directly by the Prime Minister, for three year renewable terms, following consultation with the Scottish Ministers and the First Minister and Deputy First Minister in NI.[8] The Commissioners functions are twofold: to review surveillance warrants issued by Ministers and to undertake the oversight functions currently carried out by a plethora of different surveillance commissioners. The Secretary of State responsible for providing the judicial commissioners with such staff, accommodation, equipment and other facilities as she considers necessary for carrying their functions. By clause 177, she is able to modify the functions of the JCs by regulations. JCs may

[4] In the interests of national security; for the purpose of preventing or detecting serious crime; and in the economic interests of the UK, so far as those interests relate to national security.
[5] Clauses 22, 88, 110, 124, 139, 158.
[6] For example clause 19. See also 90, 109, 123, 138, 155.
[7] For example clause 19(5).
[8] Clause 167 gives the PM the power to appoint the IPC and JCs from those who have held high judicial office.

be removed from office by the IPCr (on consultation with the PM) on the ground of inability or misbehaviour or a ground specified in the JC's terms and conditions of appointment.[9]

4. Liberty has long called for judicial authorisation for all public authority requests to conduct surveillance. 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. Liberty was therefore delighted when the Government's own Reviewer of Terrorism legislation, David Anderson QC, recommended judicial authorisation for intrusive surveillance, following the most comprehensive review of investigatory powers undertaken in a generation. As the Reviewer observed, making judges responsible for issuing warrants would improve public trust and confidence in the system of surveillance.

5. 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'[10]. 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.

Judicial review is not judicial authorisation

6. 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 Bill sets out that the judicial review standard should be applied when JCs consider warrants issued by the Secretary of State. In conducting judicial review of Executive decisions the courts apply a varying standard of review that is highly dependent on the context of the matter before it. At one end of the spectrum is a strict "Wednesbury" standard of review which will only interfere with an Executive decision that is manifestly unreasonable. At the other end of the spectrum is a more intense standard of review that will substantively assess the proportionality of the Executive decision.

[9] Clause 168 (5) provides that Commissioners can be removed from office if convicted of an imprisonable offence, bankruptcy and a range of court orders – insolvency etc. But clause 168(6) further provides that Commissioners may be removed from office by the IPC (on consultation with the PM) on the ground of inability or misbehaviour or a ground specified in the JC's terms and conditions of appointment. Otherwise, Commissioners cannot be removed from office without a resolution approving removal being approved by both Houses of Parliament.

[10] Secretary of State for the Home Office the Right Honourable Theresa May, Oral Statement to Parliament on 4 November 2015.

7. It has been argued that in the context of the authorisation process in the Draft Bill the more intensive standard of review will be triggered. The point has been made that in a case concerning control orders, *MB,* the Court of Appeal stated that judges applying a judicial review test must consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the courts have taken a more substantive approach to judicial review in relation to control order and TPIMs cases. But these types of cases, which deal with severe infringements on liberty, do not set a general rule for the standard of judicial review. In fact the intensity of the review to be applied in loss of liberty cases will likely be at the highest end of the spectrum. This is because the liberty of the individual is one of the more tightly protected freedoms in the HRA and at common law; while it is not absolute, it can only be limited in six tightly defined circumstances and for no longer than is necessary.

8. By contrast the Supreme Court held in *Tariq* in 2011 that in civil proceedings not related to any deprivation of liberty, the requirements of *MB* and related cases could be watered down.[11] This case concerned an immigration officer who had his security clearance revoked by the Home Office which resulted in his suspension. He claimed the Home Office had unlawfully discriminated against him on grounds of his religion and ethnicity. Lord Mance, speaking for the majority, said that TPIMs "*impinge directly on personal freedom and liberty in a way to which Mr Tariq cannot be said to be exposed*"[12] and made clear that in cases not concerning the liberty of the individual the standard of review will be different. If the Supreme Court felt unable to apply an intensive standard of review in Tariq, in circumstances where a man had lost his job and feared discrimination on the part of his employer, then a JC is highly unlikely to invoke an intensive standard of review in the context of a privacy intrusion where the practical and tangible consequences of infringement can be said to be much less immediate and obvious. The standard of review will be further influenced by the extreme deference that will be shown to those warrants that concern national security.[13] JCs may therefore consider themselves unable to refuse a warrant unless it is so manifestly unreasonable that no reasonable Minister could have decided to issue it.

9. A merits review is also made practically impossible by the two-stage model in the Bill. The issuing authority will be the body with the practical ability to probe and test the requesting agency or law enforcement body as to the necessity and proportionality of a warrant. The secondary role given to JCs under the model in the Bill will mean that JCs are restricted to considering ministerial decisions to issue warrants on the papers, in secret, with no opportunity to question the requesting agency, nor to probe as to whether less intrusive methods or capabilities could be deployed or ask for further material to justify the request. In order to ensure that JCs have a

[11] *Home Office v Tariq,* [2011] UKSC 35.
[12] *Home Office v Tariq,* paragraph 27.
[13] *Home Office v Rehman* [2001] UKHL 47.

substantive role in issuing warrants, they must receive applications directly from requesting bodies and be provided with expert technical support to ensure a substantive assessment of warrants.[14]

Independent authorisation is required by human rights law

10. The ECtHR has stressed the importance of effective supervision of State surveillance by an independent judiciary. In *Klass v Germany* the Court made clear that, in an area where abuse is easy in individual cases and abuses have such harmful consequences for democratic society as a whole, it is desirable to entrust supervisory control to a judge: *"The rule of law implies, inter alia, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary, at least in the last resort, judicial control offering the best guarantees of independence, impartiality and proper procedure".*[15] More recently in *Dumitru Popescu v Romania (no. 2)*,[16] the Court expressed the view that the body issuing authorisations for interception should be independent and that there must be either judicial control or control by an independent body over the issuing body's activity. Most recently and most pertinently the ECtHR ruled in *Roman Zakharov v Russia* that the Russian regime for interception violated Article 8. One feature highlighted by the Court was that while Russian law requires prior judicial authorization for interception measures, Russian judges in practice only apply purely formal criteria in deciding whether to grant an authorization, rather than verifying the necessity and proportionality of imposing such measures.[17] Strasbourg case law, taken together, is clear on the need for a fully independent body, with sufficient expertise and agency to engage in a review of the evidence put forward to justify a surveillance warrant.

A two-stage authorisation is unnecessary and risks delay*.*

11. This apparently and understandably concerns the Agencies. David Anderson reports, "*There was some resistance on the part of intercepting authorities to the idea of double authorisation, which was perceived as unnecessarily time-consuming."* He further reports that *"Most intercepting*

[14] The explanatory notes say that Government will make tech expertise available to the IPC but there are no details and no particular obligations are provided on the face of the Bill. Explanatory Notes, p. 8, para. 13: The Investigatory Powers Commissioner will be able to draw on extensive legal and technical expertise. Guide to powers, p.31, para. 75: The IPC will oversee how the agencies use bulk personal datasets: "Supported by a team of Judicial Commissioners and technical and legal experts, the Commissioner will audit how the agencies use them and they will report publicly on what they find". 176: On how the JCs will be funded, and the Sec of State will provide staff, accommodation, equipment and 'other facilities' as necessary, after consultation with the IPC.
In the explanatory notes on 176 (p. 54, para 409): "It is intended that the resources afforded to the Investigatory Powers Commissioner will ensure that the office is fully staffed with judicial, official, legal and technical support to ensure that the Commissioners are fully able to perform their oversight and authorisation functions and to hold those that use investigatory powers to account".
[15] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978.
[16] No. 71525/01, § 61, 26 April 2007; 70-73, and cited with approval in *Case of Iordachi v Moldova*, 25198/02, 10 February 2009.
[17] Roman Zakharov v Russia (47143/06) 4 December 2015, paragraph 263.

authorities did not mind whether their warrants were issued by the Secretary of State or by a judge, so long as a quick turnaround could be achieved and urgency procedures were in place".[18]

12. In recognition of concerns that have been expressed regarding warrants that may have international relations ramifications, Liberty advocates for an amendment to the internal processes in place for MI6 which could require a certain category of warrants to receive internal approval by the Foreign Secretary before the formal authorisation process is triggered.

The sheer volume of surveillance warrants - set to increase under the expanded powers in the Draft Bill – is unsuitable for small number of Cabinet ministers.

13. This was the primary reason given by David Anderson for recommending judicial authorisation. He cited the "*remarkable fact (at least to an outsider) that the Home Secretary routinely signs thousands of warrants per year, most of them concerned with serious and organised crime and the remainder with national security."*[19] In 2014 the Home Secretary personally authorised 2345 interception and property warrants and renewals i.e. about 10 per working day. Liberty shares the Reviewer's concerns that this may not be the best use of the Home Secretary's time given her responsibility for a huge department of State. Removing primary responsibility from one individual who already bears huge responsibility for policing, immigration and other services, is supported by the reflections of a former Home Secretary, David Blunkett, who has written of his time as Home Secretary *"my whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign Government warrants in the middle of the night. My physical and emotional health had cracked."*[20] Liberty also questions whether Ministers are best placed to decide the legality of warrants. In 2014 during an oral evidence session with the Intelligence and Security Committee, Phillip Hammond MP, the Secretary of State for Foreign and Commonwealth Affairs, appeared to misunderstand a number of key RIPA terms – in particular the distinction between internal and external communications – and appeared confused about how the warrant system for surveillance operates.[21] This is a cause for concern, given his huge, current, responsibility for authorising 8(4) RIPA warrants.

Arguments concerning Ministers' democratic or political accountability for surveillance warrants are misconceived and misplaced.

14. In its March 2015 report, the ISC concluded that Ministers should retain responsibility for authorising warrants: "*ministers, not judges, who should (and do) justify their decisions to the*

[18] David Anderson QC, A Question of Trust, paragraph 14.54
[19] David Anderson QC, A Question of Trust, paragraph 14.49.
[20] Blunkett: How I cracked under the strain of scandal, The Guardian, 7 October 2007, available at: http://www.guardian.co.uk/politics/2006/oct/07/uk.davidblunkett.

[21] See, for example: http://www.theguardian.com/politics/2014/dec/11/philip-hammond-powers-warrants-understanding

public".[22] The Reviewer responded to this argument in his report in June by righty observing that ministers are not currently democratically accountable for their role in issuing warrants as disclosure of the existence of a warrant is criminalised and will remain under clause 43 and similar provisions of the Draft Bill.[23]

15. A corollary to this argument is that ministers are politically accountable for the Agencies and will be required to resign if things ever go wrong. This is also incorrect. While the Home Secretary is responsible for setting the strategic direction of the Government's counter-terrorism policy and the Cabinet Minister responsible for MI5, MI5 - like the police - is operationally independent. MI5's Director General retains operational independence for day-to-day decision-making. Historically, when terrorist attacks have tragically succeeded, this has not led to political resignations. Despite inquests and inquiries following the 7/7 attacks and the murder of Fusilier Lee Rigby uncovering internal errors in the Agencies' handling of information relating to those responsible for the attacks, this has not resulted in the 'political accountability' now being claimed. One significant error revealed in the ISC report into the murder of Lee Rigby was an Agency delay in requesting intrusive surveillance for one of the men convicted of the murder – without the delay, intrusive surveillance would have been in place in the weeks before the murder.[24]

16. In reality, oversight and accountability for Agency activities is instead provided by a patchwork of mechanisms – including public inquiries, the ISC, and legal challenges brought against the Government. Liberty believes there are many ways in which this oversight and accountability could and should be enhanced but it is not correct to argue that political accountability is provided by the ministerial sign off on warrants.

17. Against the background to the publication of the Draft Bill, whereby senior Ministers have colluded with Agency heads to grant and authorise intrusive powers that have not been granted by Parliament, the claim that Ministers provide 'democratic accountability' should be given short shrift. On the very day the Bill was published the Home Secretary announced that the Agencies had been secretly conducting bulk communications data surveillance on the entire UK population for the last ten years. Nick Clegg has described his astonishment when he and a handful of Cabinet Ministers were told of this by officials in 2010.[25] Far from providing accountability, ministers have been complicit in keeping undemocratic secrets.

---

[22] Paragraph 203GG.
[23] Clauses 43 & 44 of the Draft Bill continue to criminalise the disclosure of the existence of an interception warrant without authorisation to do so.
[24] For example, the ISC report into the murder of Fusilier Lee Rigby revealed a catalogue of administrative errors by the Agencies in handling information concerning the two men ultimately convicted of his murder. (paras 318-333).
[25] *Only 'tiny handful' of ministers knew of mass surveillance, Clegg reveals,* The Guardian, 5 November 2015, available at - http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying

One-stage judicial authorisation is the norm in comparable jurisdictions.

18. In America,[26] federal investigative or law enforcement officers are generally required to obtain judicial authorisation for intercepting 'wire, oral and electronic' communications, and a court order must be issued by a Judge of a US District Court, US Court of Appeals or FISA judge. In Australia, law enforcement interception warrants must be issued by an eligible Judge or a nominated Administrative Appeals Tribunal judge.[27] In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,[28] and in New Zealand police can only intercept a private communication in tightly prescribed circumstances, including requiring a warrant or emergency permit that can only be issued by a High Court Judge.[29] If the UK wants to be able to claim it is in a world class league for good practice in surveillance, it must at the very least adopt one-stage judicial authorisation.

Judicial authorisation would encourage co-operation from US tech firms.

19. The need for reform that guarantees true independence was pressed home to the Reviewer by the Silicon Valley tech firms who, given the US tradition for judicial warrants, feel uncomfortable with the UK model of political authorisation. These firms operate in a global marketplace and need to adhere to procedures fit for a world-leading democracy. The UK is alone among democratic allies in permitting political authorisation.

Recommendations

- Liberty believes there should be a one-stage surveillance authorisation process undertaken by a JC who is supported by technical experts and therefore is in a position to assess the application and accompanying evidence and make a reasoned decision as to the necessity and proportionality of the application sought.[30]
- IPC and JCs should be appointed by the Judicial Appointments Commission, as is the case for appointments to comparable Tribunals, and not directly by the Prime Minister. Prime ministerial appointment undermines the perception of independence and does not amount to 'world leading' oversight.

---

[26] Under Title III of the *Omnibus Safe Streets and Crime Control Act 1968*, 18 U.S.C. §§ 2510-22, as amended by the *Electronic Communications Privacy Act* (ECPA) of 1986, the *Communications Assistance to Law Enforcement Act* (CALEA), by the *USA PATRIOT Act* in 2001, by the *USA PATRIOT Reauthorization Acts* in 2006, and by the *Foreign Intelligence Surveillance Act (FISA) Amendments Act* of 2008.

[27] *Telecommunications (Interception and Access) Act 1979*, section 39, as amended by the *Telecommunications Act 1997*. Note that Federal warrants relating to national security can be authorised by the Attorney General. See also the various States and Territories that have enacted legislation in order to make the Federal provisions applicable to State and Territory Police, see for example the *Telecommunications (Interception) (State Provisions) Act 1988* (Victoria).

[28] Canada *Criminal Code*, Part VI, section 186.

[29] Part 11A of the *Crimes Act*, and under the *Misuse of Drugs Amendment Act 1978*.

[30]

- The IPC should not have the power to unilaterally remove a JC.
- If a JC refuses a request for interception, an appeal should lie with the IPC. This process should replace the provisions in the Draft Bill that allow the Secretary of State to simply make a fresh application to the IPC which has the effect of rendering a JCs powers illusory.
- The power to modify surveillance warrants should lie with a JC and not the Secretary of State.
- Judicial authorisation should be a pre-requisite for all surveillance requests including retention of and access to communications data, and warrants for encryption keys under Part III RIPA.
- Warrants should only be available for targeted and not thematic or mass surveillance. The scope of warrants permitted under the Draft Bill undermines the requirement for a necessity and proportionality assessment. “Thematic warrants” for hacking and interception and the provisions for bulk warrants in Part 6 are designed to licence surveillance on a disproportionate scale, placing those charged with issuing/reviewing warrants in the position of either impugning the fundamental aims of the legislative scheme, or accepting the highly dubious premise that routine, daily, surveillance of billions of communications can amount to a proportionate action.

Legal Thresholds for surveillance

20. The Draft 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 acquisition of communications data can be authorised on many more grounds (see paragraph 25 below) and by many more public authorities.

21. All three main statutory grounds for authorising surveillance are unnecessarily broad and vague and left dangerously undefined. As the decision will continue to lie with the Secretary of State, the test will be met by whatever he or she subjectively decides is in the interests of national security or the economic well-being of the UK. This means that individuals are not able to foresee when surveillance powers might be used, and grants the Secretary of State a discretion so broad as to be arbitrary.

22. 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.

23. 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.[31] National security as a legal test is therefore 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.

24. The use of broad and vague notions such as 'national security' and 'economic well-being' risks interference with political and other lawful activity that ought to go unimpeded in a democratic society. In an era when Members of Parliament have been labelled *"domestic extremists"* and when the Prime Minister has stated *"The Labour Party is now a threat to national security"* the continued undefined use of these terms in enabling legislation is not sustainable.

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

Recommendation

- Liberty believes that these grounds should more tightly defined on the face of the Bill and linked to the objective threshold of reasonable suspicion of criminality. A significantly higher level of specificity is required if these three grounds are to act as an effective check on the use of intrusive powers.

Communications data retention and acquisition

25. Parts 3 & 4 of the Draft 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.[32]

26. 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 capable of justifying interception and hacking, 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.[33] 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.[34] 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.

27. 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

[32] 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.

[33] Clause 46(7).

[34] 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 59 of the Draft Bill. Clause 61 of the Draft Bill provides for judicial commissioner approval to identify or confirm journalistic sources.

regime that currently exists under RIPA and is replicated in the Draft Bill. We do not believe an operational case has been made either for blanket ICR retention or The Request Filter and we believe that both proposals would violate human rights law.

Revealing nature of communications data

28. Communications data provides a detailed and revealing picture of somebody's life in the digital age. As defined under DRIPA and RIPA it can disclose the date, time, duration and type of communication, the type of communication equipment used, its location, the calling telephone number and the receiving telephone number. This can reveal personal and sensitive information about an individual's relationships, habits, preferences, political views, medical concerns and the streets they walk. As the CJEU has put it:

> *"those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them."*[35]

29. In December 2013 US District of Colombia Judge Richard J Leon found that a lawsuit challenging the NSA's previous regime of bulk metadata collection demonstrated a "substantial likelihood of success"[36] and said of modern data metadata:

> *"I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval…Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment."*

30. The Government seeks to diminish the importance and sensitivity of communications data by distinguishing it from the content of communications. At one time a firm distinction between communications data and content would have been more credible, for example when much communication was by letter: everything inside the envelope is content, everything on the outside communications data. However, this distinction has been eroded by the scale of modern internet and mobile phone usage. As communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a

[35] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).
[36] Klayman v Obama in the United States District Court for the District of Colombia, 16 December 2013, available at: http://apps.washingtonpost.com/g/page/world/federal-judgerules-nsa-program-is-likely-unconstitutional/668/.

complete and rich picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is expansive, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner. In 2015 the ISC remarked: *"We were surprised to discover that the primary value to GCHQ of bulk interception was not in reading the actual content of communications, but in the information associated with those communications."*[37]

31. Indeed in many circumstances the picture of someone's life that can be created through examination of communications data will be more revealing than the content of may of their communications. As Stewart Baker, former senior counsel to the US NSA observed in 2013, metadata *"absolutely tells you everything about somebody's life. If you have enough metadata you don't really need content."*[38] The value of metadata and the use that the UK's closest ally is prepared to make of it was left beyond doubt following comments by the former head of the NSA, Michael Hayden in 2014: "*We kill people based on metadata*."[39] Furthermore, consider the range of situations in which just the fact of a single communication and the identity of the parties speaks volumes: the phone call from a senior civil servant to a reporter on a national newspaper immediately before a major whistle-blower scandal fills the front pages; the email to a civil liberties watchdog from a police officer during the course of an inquest into a death in police custody.

Regime incompatible with recent court judgments

32. We believe that the current retention and access regimes - let alone the proposal to impose further obligations on ISPs to generate and retain ICR data in the Draft Bill - violate human rights law and will be found in breach of the European Charter of Fundamental Rights and Freedoms, when the CJEU considers communications data retention and acquisition once again in 2016. In April 2014 the CJEU ruled in *Digital Rights Ireland* that the EU Data Retention Directive which mandated blanket data retention between 6 -24 months was invalid due to its sweeping interference with privacy rights.[40] The CJEU acknowledged the important role of data retention and access for the prevention and detection of serious crime but laid out the following ten principles to ensure compliance with human rights standards –

    1. restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and / or suspects or persons whose

[37] Intelligence and Security Committee, Privacy and Security: a modern and transparent legal framework, paragraph 80.
[38] Stewart Baker, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/
[39] General Michael Hayden, quoted in David Cole, 'We Kill People Based on Metadata', New York Review of Books blog (10 May 2014), available at http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-killpeople-based-metadata/

[40] *Digital Rights Ireland (C-293/12) and Seitlinger and Others* (C-594/12).

data would contribute to the prevention, detection or prosecution of serious offences (paragraph 59);

2. provide exceptions for persons whose communications are subject to an obligation of professional secrecy (paragraph 58);

3. distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned (paragraph 63);

4. ensure retention periods are limited to that which is 'strictly necessary' (paragraph 64);

5. empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary (paragraph 62);

6. restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes (paragraphs 60-61);

7. limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary (paragraph 62);

8. ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access (paragraph 66);

9. ensure destruction of the data when it is no longer required (paragraph 67); and

10. ensure the data is kept within the EU (paragraph 68).

33. Three months after the judgment, the UK Government responded with emergency legislation – the *Data Retention and Investigatory Powers Act 2014* (DRIPA) - which was rushed onto the statute book in 7 days in July 2014. Prior to the decision in *Digital Rights Ireland*, senior courts across Europe had annulled domestic legislation seeking to implement the EU Directive– including Bulgaria[41], Romania[42], Germany[43], Cyprus and the Czech Republic. Following the

[41] In 2008 the Bulgarian Supreme Administrative Court, found the legislation implementing the EU Data Retention Directive incompatible with the country's constitutional protection of personal privacy.
[42] In October 2008, the Romanian Constitution Court became the first to declare legislation transposing the EU Directive in breach of its Constitution. The Court found that the mandatory retention of communications data scheme engaged a number of fundamental rights, namely the right to freedom of movement, the right to intimate, family and private life, privacy of correspondence and the right to freedom of expression. In finding its transposing legislation disproportionate, the Court relied on, amongst other issues, the reversal of the ordinary presumption of innocence and the lack of a reasoned basis for the retention period required, finding also that retention on the scale required was 'likely to prejudice, to inhibit the free usage of the right to communication or expression'. Decision no 1258 of the Romanian Constitutional Court, 8 October 2009. Available at: http://www.legiinternet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decisionregarding-data-retention.html.
[43] In March 2010, Germany's Constitutional Court declared the provisions of its law transposing the Directive unconstitutional. In finding the communications data retention regime incompatible with constitutional protection for personal privacy, the Court commented that 'the protection of communication does not include only the content but also the secrecy of the circumstances of the

judgment, courts in a further six Member States, including five courts of final appeal, have relied on DRI in holding national data retention legislation invalid – including courts in Austria, Slovenia, Belgium, Romania, Netherlands, Slovakia.

34. Liberty is currently representing David Davis MP and Tom Watson MP in their legal challenge to DRIPA. 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."*[44]

35. The Government appealed the judgment to the Court of Appeal. In November 2015 the Court of Appeal referred two questions to the CJEU, namely (1) Did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law with which the national legislation of Member States must comply? And (2) Did the CJEU in Digital Rights Ireland intend to expand the effect of Articles 7 and/or 8 of the Charter beyond the effect of Article 8 ECHR as established in the jurisprudence of the ECtHR? On 4 May 2015 another CJEU reference on data retention post DRI was made by a higher court in Sweden asking whether a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime is compatible with EU law taking into account the Charter.[45] The outcome of these references will have significant bearing on the lawfulness of the Draft Bill.

---

communication, including if, when and how many times did some person…contact another. The Court went on to find that 'the evaluation of this data makes it possible to make conclusions about hidden depths of a person's private life and gives under certain circumstances a picture of detailed personality and movement profiles; therefore it can not be in general concluded that the use of this data presents a less extensive intrusion than the control of the content of communications. Bundersverfassungsgericht, 1 BvR 256/08. English press release at http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg10- 011en.html (judgment only in German).

[44] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin)

[45] Request for a preliminary ruling from the Kammarrätten i Stockholm (Sweden) lodged on 4 May 2015 — Tele2 Sverige AB v Post- och telestyrelsen
(Case C-203/15) available at - http://curia.europa.eu/juris/document/document.jsf?text=&docid=165124&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=1126567.

Recommendations

- The Draft Bill should provide for a system of **targeted retention and acquisition which allows law enforcement bodies to request retention and acquisition of communications data for specific individuals on suspicion of serious criminality.** Liberty believes it would be feasible and desirable to construct a targeted communications data retention and acquisition regime. Instead of the Secretary of State issuing speculative retention notices, law enforcement would be able to apply to a judge for retention and acquisition of communications data in an intelligence-led manner when investigating serious crime. The ten vague purposes for which data can be accessed should be replaced with a requirement for named individuals and reasonable suspicion of serious crime.
- Judicial authorisation – by the newly created tribunal of JCs – should be required for all public authority access to communications data. But in the case of privileged and confidential communications a stricter legal threshold for access should be met (see page 54).
- This scheme would have the benefit of complying with the DRI judgment, preventing further litigation and providing for a more effective and efficient communications data regime. The volume of communications data used in serious crime investigations is an infinitesimal fraction of that retained – at huge cost – on millions of innocent people. Just as the ECtHR judgment in *S and Marper* v UK[46] required a new policy on police retention of innocents' DNA so too does the CJEU judgment in DRI require a new policy on the retention of innocents' communications. In response to *S and Marper* the Government legislated for a new policy and has undertaken the deletion of over 1 million DNA profiles. Yet no attempt has been made to explain or justify the different approach it has taken here.

[46] *S and Marper v United Kingdom* [2008] ECHR 1581.

Internet connection records

36. The Draft 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. Under current legislation in DRIPA 2014, public telecommunications operators may be required to retain "*relevant communications data"* for up to 12 months[47], including data which may be used to identify the internet protocol (IP) addresses of senders and recipients of communications. However, this specifically excluded 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.[48]

37. ICRs are defined in the Bill as "*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".*[49] In explanatory notes accompanying the Bill, ICRs are described as "*a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet".*[50]

38. 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.[51] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

39. Public authorities will not need a warrant to obtain an individual's detailed internet connection records. Applications by law enforcement and public authorities to acquire ICRs relating to suspects will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[52] within the public authority, and then by a 'single point of contact.'[53]Provisions in the draft Bill would permit law enforcement and public authorities to gain access to ICRs for three 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; and to identify when and where a person has accessed or made available illegal material.[54]

---

[47] *Data Retention and Investigatory Powers Act 2014,* section 1
[48] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[49] *Draft Investigatory Powers Bill 2015,* clause 71, subsection (9)(f)
[50] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.29
[51] *Draft Investigatory Powers Bill 2015,* schedule 4, part 1
[52] *Draft Investigatory Powers Bill 2015,* clause 46
[53] *Draft Investigatory Powers Bill 2015,* clause 60. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[54] *Draft Investigatory Powers Bill 2015,* clause 47

Defining ICRs

40. ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. The draft Bill failed to define the exact fields of information that would constitute an 'internet connection record'. The Home Office's accompanying ICR factsheet says that ICRs "*will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address (e.g. www.facebook.com or www.google.com) along with a time/date*".[55] Therefore, in practice, an ICR will comprise identifying connection information, likely to include client and server IP addresses, port connections, time, DNS (Domain Name System) logs, and possibly MAC addresses.

41. "*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) has expressed concern that ICRs have not been properly defined.[56] In a recent meeting between ISPA members and the Home Office, civil servants were still unable to define the fields of information that would constitute an ICR.[57] This indicates a failure to identify exactly what data is necessary for the stated purposes, and what data retention would be excessive.

42. 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.

43. Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways. First, they can request telecommunications operators to retain the data of specific targets on a forward-looking basis.[58] Secondly, they can request retrospective 'internet connection' data on specific targets from operators who temporarily store it for their own business purposes.[59] Thirdly, if they are seeking to prevent or detect serious crimes (such as child sex abuse, financial crime, drug smuggling, etc.) they can request data or assistance from GCHQ, which has a remit to provide intelligence for these purposes.[60] Intelligence sharing to tackle online child sexual exploitation will be fortified by the establishment of the NCA and GCHQ Joint Operations Cell (JOC), which was launched in November 2015[61].

44. 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

---

[55] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[56] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015
[57] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html
[58] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25
[59] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[60] *The threat from serious crime* – GCHQ, 2015 http://www.gchq.gov.uk/what_we_do/the-threats-we-face/the-threat-from-serious-crime/Pages/index.aspx
[61] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015

been accurately described as "*overstated and misunderstood*".[62] Further, there is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[63]. 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[64]. As the CJEU ruled in 2014[65], 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.

45. Access to ICRs will be granted for the furtherance of one of three purposes. However, the need for further powers in relation to each of these purposes is flawed.

Rebuttal to Purpose 1: Identifying the individual device that has sent a communication online

46. The Metropolitan Police and National Crime Agency (NCA) have suggested that without ICRs, they cannot resolve IP addresses (that is, identify web users) and continue investigations in a minority of cases (approximately 14%[66]).

47. In the *Operational Case for the Retention of Internet Records*, published with the draft Bill, three case studies of discontinued investigations relating to child sexual exploitation and three relating to fraud are presented to support the argument for retaining ICRs. It is claimed that ICR retention would be required in order to progress those investigations and increase chances of accurately identifying a web user.[67] However, the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of serious crime has been questioned by ISPs and technologists.[68] The justification relies on the assumption that online criminals offend using a regular browser or public file sharing service on their own device, using personal internet connections, without employing the most basic of the widely available anonymity tools to avoid detection. The use of privacy-enhancing and anonymising tools such as Virtual Private Networks (VPNs), which securely 'tunnel' internet connections; Tor, a secure browser that anonymises users' location and identity; and proxy web browsers that bypass filters and anonymise web browsing, is widespread and increasing exponentially. ICRs will be unusable and in fact

---

[62] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[63] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[64] Ibid
[65] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014
[66] It is argued that the retention of ICRs would improve the chances of being able to resolve an IP address in 14% of cases in a sample from the US based National Centre for Missing and Exploited Children, NCMEC - as cited in the ICR evidence base: *Operational Case for the Retention of Internet Connection Records,* 2015, p.14
[67] *Operational Case for the Retention of Internet Connection Records,* 2015, p.20
[68] *Written evidence regarding draft Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25065.html

misleading where such privacy tools have been used. Furthermore, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This inevitable digital shift will render ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

48. In the limited cases where the ICRs might assist in resolving an IP address they will provide limited assistance in identification of suspects as they can only help to identify a device, such as a laptop or PC – not an individual user. Identifying a specific user requires a context of information that would typically be gathered in a targeted surveillance operation. Devices such as laptops, PCs, tablets and even smart phones are commonly shared within families, workplaces and public institutions, further diminishing the value of bulk ICRs in identifying an individual suspect. Indeed, ICR data is "inexact and error-prone".[69]

49. In evaluating the efficacy of ICRs in serving the purpose of IP resolution and identification of a suspect, we are informed by the case study of Denmark's Data Retention Law (*Logningsbekendtgørelsen*), effective 2007-2014, which required communication service providers to retain internet session logs. Denmark's data retention law compelled telecommunications operators to store internet session data for 12 months including client and server IP addresses, port numbers, transmission protocols and timestamps.[70] The data retention excluded DNS logs (i.e. the names of the websites the server IP addresses corresponded to). **A self-evaluation report published by the Danish Ministry of Justice in December 2012 found that several years of collecting internet session data had not yielded any significant benefits for law enforcement - session data had played a minimal role in only one case.**[71] In fact, Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[72] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[73] In June 2014, the Danish government repealed the obligation on operators to retain session data

[69] *Written evidence regarding draft Investigatory Powers Bill* - Tim Panton, 1 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/investigatory-powers-bill-technology-issues/written/25104.html
[70] *Logningsbekendtgørelsen 2006* (https://www.retsinformation.dk/forms/r0710.aspx?id=2445). An English translation produced by the Ministry of Justice is available at https://itpol.dk/sites/itpol.dk/files/TFR40200.pdf
[71] *Redegørelse om diverse spørgsmål vedrørende logningsreglerne* – Justitsministeriet, Dec 2012 (http://www.ft.dk/samling/20121/almdel/reu/bilag/125/1200765.pdf). There is no English translation. The article "*In Denmark, Online Tracking of Citizens is an Unwieldy Failure*" - TechPresident, 22 May 2013, discusses the report (http://techpresident.com/news/wegov/23918/denmark-government-will-not-allow-ordinary-citizens-have-digital-privacy).
[72] Ibid.
[73] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2

on the basis that it was "*questionable whether the rules on session logging can be considered suitable for achieving their purpose*".[74]

Rebuttal to Purpose 2 - identify what ISPs an identified suspect has used, when and how**[75], in **order to inform law enforcement as to which communications service providers to request further information from.

50. The second part of the Home Office's case for mass ICR retention rests on the idea that this is required to help inform law enforcement request further information on identified suspects. This argument overlooks the range of intrusive powers already on the statute book. It is far more preferable, from both a human rights and law enforcement perspective, to employ robust targeted powers on identified suspects than intrude on the rights of the entire population. Existing powers for obtaining further information about communications of suspects include: using targeted interception, making targeted requests for communications data from service providers, and seizing and forensically examining a device. However, the Home Office presents these targeted approaches as less favourable than the mass retention of ICRs.

51. The argument in favour of this new, invasive category of bulk data retention rests, in part, upon the claim that there is an "*extremely high threshold*"[76] and "*very limited circumstances in which the interception of communications content can be authorised*", and therefore targeted interception "*cannot be used in most law enforcement cases".*[77] This is a peculiar argument, as interception is used for three broad statutory purposes: the prevention and detection of serious crime (which accounts for 68% of interception warrants[78]), the interests of national security and for the economic well-being of the UK.[79] The case studies provided to support the case for ICR retention all qualify as serious crimes[80], for which interception can be used, as they relate to child sex abuse, fraud and human trafficking.

52. Additionally, it is claimed that law enforcement bodies cannot request data from popular online service providers who store communications data for their own purposes, such as Facebook, without ICR evidence proving that the individual or device in question definitely accessed their service.[81] Without this data, they argue that such a request "*is unlikely to be necessary and proportionate*".[82] Liberty does not recognise this explanation. If the authorities have objective and

---

[74] *Justitsministeren ophæver reglerne om sessionslogning ("The Ministry of Justice repeals the rules about session logging*) – Justitsministeriet, 2 June 2014, http://www.justitsministeriet.dk/nyt-og-presse/pressemeddelelser/2014/justitsministeren-oph%C3%A6ver-reglerne-om-sessionslogning
[75] *Draft Investigatory Powers Bill 2015,* clause 47 (4)(b)
[76] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[77] *Operational Case for the Retention of Internet Connection Records,* 2015, p.16
[78] *HM Government Transparency Report 2015: Disruptive and Investigatory Powers,* p.34
[79] *Draft Investigatory Powers Bill 2015,* clause 14 (3)
[80] Serious crimes are those that incur a sentence of 3 years or more; violent crimes; crimes involving substantial financial gain, or conduct by a large number of persons in pursuit of a common purpose. *Draft Investigatory Powers Bill 2015,* clause 195 (1),
[81] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25
[82] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4

reasonable grounds for suspecting serious criminality and further believe that the suspect's use of a telecommunications platform may have furthered/provide evidence of the offence a request for communications data will be necessary and proportionate.[83] If the suspect did not use the communications service, the data will simply not be there to obtain.

53. As a third argument for ICR retention, law enforcement bodies say it is "*thanks to seizure of devices*" that it has thus far been possible to identify communications services used by suspects, but that seizure of a device "*will not always be the preferred course of action in an investigation, as it is an overt action that will normally involve an arrest*"[84]. Investigators would rather "*develop intelligence on the group covertly*" and establish any possible "*previous linkages"* between group members. However, links between group members can be covertly discovered through a targeted communications data retention order; through requests for retrospective data from the operators who store it for their own purposes; or through interception.

54. The value of ICRs in consistently and accurately identifying what internet communications services a suspect or suspected victim has used and when has been over-estimated and misunderstood. In an ICR Factsheet produced by the Home Office, it is claimed that ICR retention would identify what communications services a person has used and when, and thus "*allow the police to determine whether a missing person was using a particular smartphone app or social media website prior to his or her disappearance".*[85] Similarly, in a recent Home Office meeting to discuss the concerns of the Internet Service Providers Association (ISPA), civil servants claimed ICRs could help police discover when a missing person last accessed a communications service such as Twitter on a smart phone. In response, "*ISPA members immediately pointed out the huge flaw in this argument*".[86] ICRs may not accurately show *when* communications services have been used, and therefore are not helpful for informing an accurate time frame for further communications data requests. This is because communications software (especially on smartphones) often stays connected in the background whether in current use or not, remaining connected for a period of days, weeks or months[87]. Connection records show connection timestamps rather than access timestamps, and one such 'internet connection' could exceed the 12 month retention period by the time it is logged. ISPs and technologists have expressed serious concern that the Home Office has based an extensive, invasive data collection policy on a

[83] Indeed, many online public services are co-operative with law enforcement: Facebook, for example, co-operates with the NCMEC and has an established system for law enforcement data requests[83]. In the period January 2015 – June 2015, UK law enforcement made 3,384 requests to Facebook alone for various types of data, relating to 4,489 accounts; Facebook found legal basis to comply with 78.04% of these requests[83].
[84] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[85] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[86] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html
[87] The main transmission protocol used online, TCP, can maintain a connection for hours, days, or even years; whilst protocols such as SCTP and MOSH aim to keep a connection active indefinitely, even with changes to IP addresses at each end or changes in connection.

fundamental misunderstanding, or worse misguidance, as to how internet connections work, and has provided misleading descriptions of what purposes ICRs will serve accordingly.

Rebuttal to Purpose 3 - to "identify the accessing of illegal online services or websites"[88].

55. The value of ICRs in consistently and accurately identifying access to illegal websites has also been over-estimated and misunderstood. The bulk collection of ICRs raises concerns about inaccurate and possibly incriminating representations of innocent individuals' internet use.

56. Each 'internet connection' involves the exchange of multiple packets of data. Some of these packets of data relate to the scripts, images and styles that constitute various elements of a webpage. An image or video embedded on a webpage may be hosted elsewhere and generate a separate 'internet connection', which may relate to a server the individual had no intention, or even knowledge, of accessing. Similarly, it is unlikely that ICRs will be able to distinguish between a webpage visited out of an individual's own volition and a pop-up. Bulk ICR retention could be exploited by hackers for nefarious purposes – for example, by embedding 'suspicious' scripts into webpages, or spamming individuals with suspicious pop-ups. In addition, many browsers and apps pre-cache links – that is, store data from linked webpages before they are even visited by the user, to improve access speed if it is selected. Clearly, bulk ICRs collected on a population-wide scale will lead to misleading, inaccurate and potentially suspicious information as to innocent internet use.

Threat to privacy and security posed by bulk retention of ICRs

57. 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*"[89].** In their final report, the Joint Committee noted that *"storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn*"[90]. 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. At a time when the UK is plagued by prolific hacks (e.g. TalkTalk, Vodafone, Vtech), taking the title as the most hacked country in Europe and the second most

[88] Draft Investigatory Powers Bill 2015, clause 47 (4)(c).
[89] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[90] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29

hacked in the world,[91] it is extraordinarily irresponsible to coerce private companies with the burden of generating, storing and securing vast swathes of revealing data on the general public. Companies are unable to guarantee protection of the customer information they already have – entrusting them with new data of unprecedented volume and value will have disastrous effects for the UK's internet industry and the safety of British internet users. In addition to the obligation on UK telecommunications operators, the draft Bill places a duty on overseas operators to collect and retain ICRs on UK citizens.[92] This creates an extra set of concerns for UK citizens' privacy and the protection of extremely revealing data in other jurisdictions. The UK Government's general insistence on extraterritorial application of bulk communications data retention powers sets a "*disturbing precedent*" for other, more authoritarian countries to follow, as Anderson pointed out in his independent review.[93]

58. 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 usual targeted surveillance methods for investigations; in fact, it could easily cause false suspicion. Arguably, the £175 million budgeted to fund reluctant telecommunications operators to spy on their customers would be better spent on hiring more officers to conduct targeted, warranted surveillance on suspects of serious crime.

Recommendations

- Liberty believes that clause 71 (9)(f) should be removed from the Bill, and mass internet connection record retention in any form should be wholly rejected.
- Explore and produce more information on the law around access to targeted communications data and the threshold for intercept. As this system is not currently subject to judicial oversight it may be the case that requests are being refused in circumstances where the legal threshold has been made out. A system of judicial authorisation of communications data requests would help ensure uniformity and the furtherance of investigations in circumstances where the requirements of necessity and proportionality are made out.

[91] Internet Security Threat Report, 2015 – Symantec, http://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf. Reported on in, British companies bombarded with cyber attacks – Sophie Curtis, The Telegraph, 14 April 2015.
[92] Draft Investigatory Powers Bill 2015, clause 79
[93] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207

The Request Filter

59. The Draft Bill contains provisions for a communications data 'Request Filter[94]' – a feature previously proposed in almost identical terms in the draft Communications Data Bill. 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*"[95], 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 (see paragraph 25). In practice, the 'Request Filter' would be a search engine over a "*federated database*"[96] 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.

60. The Government is keen to portray the Request Filter as a 'safeguard' that "*will minimise the interference with the right to privacy".*[97] However, the processing of personal data represents a significant privacy intrusion. Whilst a useful tool for complex data searches, the 'Request Filter' cannot be viewed as a straightforward safeguard. Rather 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.

61. Public authorities' permanent ability to access to the 'Request Filter' makes it an enticing and powerful tool that could be used for the broad range of statutory purposes - recently declared unlawful by the High Court.[98] 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. This was one of the many concerns about this proposal expressed by the Joint Committee on the Draft Communications Data Bill.[99]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 access to online radio

[94] Draft Investigatory Powers Bill 2015, clause 51
[95] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[96] Ibid.
[97] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23
[98] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin).
[99] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 126, p.37

websites, inferring risk.[100] Thus, this new ability could risk casting undue suspicion on thousands of innocent citizens.

62. Allowing hundreds of public authorities direct access to sensitive databases complicates the issue of protecting such stores (for example, stores of internet connection records). The duty to "*put in place and maintain an adequate security system"*[101] outlined in the draft Bill is clearly resides with the Secretary of State, but there is no information available as to what that security system would be.

Recommendations

- Liberty's primary concern is the indiscriminate collection, generation, and storage of billions of items of data on innocent citizens. Liberty believes that Article 8 requires that individuals' privacy should not be interfered with unless there is clear reason to suspect crime, and as such, expansive distributed databases of innocents' communications are unlawful. Liberty believes that further processing personal data, without judicial authorisation and for purposes unconnected with serious crime would constitute a further unjustified interference with Article 8 rights.

[100] 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.
[101] Draft Investigatory Powers Bill 2015, clause 53 subclause (5)

Targeted interception

63. Powers for "targeted interception" of communications are contained in Part 2 Chapter 2 DIPB. 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[102]) on application by the intelligence services, the National Crime Agency, London Met, PSNI, PSS, HMIC and the Chief of Defence Intelligence subject to the weak judicial review process (discussed at paragraphs 1- 18). Warrants can be issued on the three main grounds (which replicate existing RIPA grounds). The Draft Bill provides for each warrant to last a minimum of six months – whereas under RIPA, serious crime warrants last three months.

Thematic warrants

64. The most radical departure from the scheme under RIPA relates to the scope of interception warrants. RIPA clearly provided that warrants for targeted interception were required to name "*one person as the interception subject*" or "*a single set of premises*".[103] Clause 13 of the Draft Bill radically reforms this requirement and prescribes that warrants may cover "*a particular person or organization 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 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*" or for the maintenance or development of interception apparatus and training. This allows warrants to be issued in respect of people whose names are not known or knowable when the warrant is sought. This is confirmed by clause 23 which provides that a thematic warrant must describe the relevant purpose or activity and name or describe as many of those persons as is reasonably practicable. The creation of thematic warrants in the Draft 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.

65. This change follows the dramatic disclosure in March 2015 that the Secretary of State is already issuing "thematic" interception warrants. The ISC reported that the significant majority of 8(1) warrants relate to one specific individual, but that some don't apply to named individuals or

[102] See clauses 17 & 18; where the application relates to persons or premises reasonably believed to be in Scotland.
[103] Section 8(1)(a) RIPA.

specific premises but rather groups of people. The current Home Secretary has apparently derived the authority to do so from the broad definition given to "person" found elsewhere in RIPA, despite the unequivocal reference to "one person" in section 8(1). Liberty does not recognise this unorthodox statutory construction and any thematic warrants that have been issued under this power are likely to be *ultra vires.* Like much surveillance practice in recent years, this appears to be a case of the Agencies and Executive claiming powers well beyond those provided on the face of RIPA and other enabling statutes. The existence of "thematic" warrants also represents a huge departure from the position at common law which has long banned "general warrants". The ISC reported that the Interception of Communications Commissioner has "*made some strong recommendations about the management of thematic warrants*" and has in some cases recommended that they are cancelled.[104] The ISC has expressed further *"concerns as to the extent that this capability is used and the associated safeguards. Thematic warrants must be used sparingly and should be authorised for a shorter timescale than a standard 8(1) warrant"*[105]

66. Liberty believes the scope of warrants permitted under clause 13 fails to comply with both common law and ECHR standards. In Zakharov v Russia[106] 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.'* [107] 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 Draft Bill.

Bar on admissibility of intercept material in criminal justice system

67. Clause 42 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*."[108]

68. Removal of the ban will 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.[109] Furthermore the current ban has fuelled a corruption of domestic fair trial standards and abusive counter-

[104] ISC report, paragraph 45.
[105] ISC report, page 24 recommendation D
[106] (47143/06) 4 December 2015.
[107] Paragraph 265.
[108] See Intercept as Evidence, December 2014, Page 23.
[109] *Natunen v Finland* (Application no. 21022/04).

terrorism laws, from control orders to TPIMs, to the corrosive growth of Closed Material Procedures across our justice system.

69. 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 Draft Bill - hacking can be made admissible, there is no logical or coherent case for excluding intercept. As a last resort, the authorities also always have the option of abandoning a particular prosecution. Successive Government initiated reviews over the past two decades have concluded that intercept should be made admissible. The only remaining objection from the Agencies now 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 which fulfills the test for disclosure to a defendant at trial – material capable of undermining the case for the prosecution – which need be disclosed.[110] 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.

Recommendations

- Liberty believes that the scope of targeted interception warrants needs to be significantly curtailed to prevent speculative and abuse interception and comply with the recent ECtHR judgment in *Zakharov v Russia.*
- Liberty also calls for clause 42 to be deleted from the Draft Bill so that material obtained by interception can be made admissible in criminal trials and inquiries under the Inquiries Act 2005.

[110] Section 3 of the Criminal Procedure and Investigations Act 1996.

Targeted hacking

70. Part 5 of the Draft Bill makes provision for "targeted hacking" euphemistically termed "equipment interference" in the Bill. 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[111]) 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 'for the purpose of preventing and detecting serious crime'.[112] In making their determination, chief constables are required to consider whether the warrant's objectives could reasonably be achieved by other means. Ministers are under no such obligation. 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. Chief constables are required to have their decisions to modify warrants reviewed by a JC.

71. A hacking warrant authorises a person to interfere with any equipment for the purpose of obtaining "communications", "private information" and "equipment data".[113] "Communications" can comprise speech, music, sound, visual images, *data of any description* and any form of signal between two individuals, two machines or between a person and a machine. Private information is defined to include any piece of information relating to a person's private or family life. This could include information stored on a device or a network which hasn't been communicated. Communications and private 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".*[114]

72. Hacking is prima facie unlawful as a matter of domestic criminal law[115] and before 2015, hacking was not avowed as an intelligence agency or law enforcement capability. This only changed in

[111] Clause 86.
[112] 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.
[113] Equipment data is defined at clause 82.
[114] Clause 81(4).
[115] Section 1 of the Computer Misuse Act 1990 makes it an offence to cause a computer to perform any function with intent to secure access to any program or data held within it if the access is

February 2015 when the Home Office published a consultation on a Draft Code of Practice for Equipment Interference in response to Privacy International and others' claim in the IPT concerning the hacking disclosures contained in the Snowden documents. This Code referred only to the intelligence agencies and did not make reference to police hacking powers which were not officially acknowledged until the publication of the Draft Bill.

73. There is currently no clear or accessible legal framework governing the hacking of electronic devices and networks making current use of the practice likely unlawful on grounds that it is not in accordance with law to comply with the requirements of the HRA. Government claims the Agencies' hacking powers derive from broad and vague enabling powers contained in sections 5 and 7 of the *Intelligence Services Act 1994*.[116] Yet the enabling power bears no resemblance to the power now contained in the Draft Bill and the legislation pre-dates the powerful electronic hacking capabilities now utilised.

74. Police apparently derive hacking powers from section 93 of the Police Act 1997[117] yet when the head of the Metropolitan Police's Technical Unit gave oral evidence to the Draft Bill Committee he seemed unsure as to legal basis for the Met's powers.[118] Section 93 similarly bears no resemblance to the powers now contained in the Draft Bill and even as recently as 2010, when the related Code of Practice on "*Covert Surveillance and Property Interference*" was issued it referred only to physical property interference and not electronic hacking. Despite this, in a potentially explosive admission before the Draft Bill committee, the Metropolitan Police representative disclosed that equipment interference is used in a "majority" of serious crime cases. Over the past few years, various media outlets have sought to investigate hacking by the police. The Times and Sky News[119] have reported that the Met has purchased and begun using "IMSI catchers" and when the Hacking Team (a private company offering hacking services to

---

unauthorised. Section 3 of the 1990 Act also makes it an offence to do any authorised act in relation to a computer if the intention is to impair its operation, hinder or prevent access to any program or data, to impair the operation of any program or reliability of data. Section 10 provides that section 1 has effect without prejudice to the operation of any enactment relating to the powers of inspection, search or seizure, but this carve out does not apply to section 3.
However, with their practices thrown into the light by Snowden's whistleblowing, the Government sought to immunise the intelligence agencies and amended the Computer Misuse Act 1990 to exempt, presently and retroactively, GCHQ from criminal culpability (*Serious Crime Act 2015*, Section 44).

[116] Section 5 covers activity in the UK and provides that a warrant authorised and issued by the Secretary of State may make lawful any "*entry on or interference with property or with wireless telegraphy* The ISC report sheds some further light on current practice. While the number of section 5 warrants obtained by the Agencies in 2013 is not disclosed, the report reveals that while the majority of warrants are targeted, a percentage were 'thematic' permitting the Agencies to use the same technique on multiple occasions or authorised 'IT Operations'.

[117] Under section 93 police can obtain authorisations for - "the taking of such action, in respect of such property in the relevant area, as [the authorising officer] may specify" and "the taking of such action in the relevant area as he may specify, in respect of wireless telegraphy".

[118] Oral evidence to the Draft Investigatory Powers Bill Committee, 16 December 2015, Detective Superintendent Paul Hudson, Head of Metropolitan Police Service Technical Unit.

[119] Fake mobile phone towers operating in the UK, 10 June 2015, available at - http://news.sky.com/story/1499258/fake-mobile-phone-towers-operating-in-the-uk.

Governments worldwide) was recently itself hacked it was revealed that the Met, NCA and Staffordshire police had shown interest in their products before apparently getting cold feet.[120] Until the publication of the Draft Bill the Met had adopted a NCND approach to hacking.

Highly intrusive nature of hacking

75. 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 gives the hacker access to all historical and future data stored on a device. Perhaps most uniquely it also grants the hacker total control over a device – phones and computers can be turned on or off, have their cameras or microphones activated, files added or deleted. Furthermore, all this can be done without the fact of the hack being known or knowable to the target.

76. 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.

77. 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[121]. 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"*[122]. 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[123], which may

[120] UK Police tried to buy Hacking Team's Spytech leaked emails show, Vice News, 15 July 2015, available at - https://news.vice.com/article/uk-police-tried-to-buy-hacking-teams-spy-tech-leaked-emails-show
[121] *Obama Order Sped Up Wave of Cyberattacks Against Iran* – David E. Sanger, The New York Times, 1 June 2012
[122] *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
[123] *The Most Wanted Man in The World* – James Bamford, Wired, Aug 2014

have caused simultaneous flight-tracking issues, and led government and opposition forces to erroneously blame each other for the incident[124].

78. 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 many more rights than traditional forms of communications surveillance. Parliamentarians may also want to consider the cost of widespread hacking by the authorities. Hacks maintain and create permanent vulnerabilities which can then 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.

Thematic hacking warrants

79. Clause 83 provides for thematic hacking warrants which amount to general warrants to hack groups or types of individuals in the UK. Hacking is not restricted to equipment belonging to, used by or in possession of particular persons. Instead the subject matter of warrants can target equipment "*belonging to, used by or in the possession of a particular organisation*" or "*persons who form a group that shares a common purpose or who carry on or may be carrying on a particular activity*" or more than one person or organisation "*where the interference is for the purpose of the same investigation or operation."* 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 being used, for the purposes of a particular activity or activities of a particular description*" as well as testing or maintaining capabilities. In addition the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest".[125] It is difficult to foresee a more enabling and open-ended framework of the scope of domestic hacking capabilities. Hacking is by its nature much more prone to collateral intrusion than traditional forms of surveillance. ISMI catchers can for example pick up stored content of all mobile phones in a particular area. If use of the capability is to stand a chance of meeting the UK's human rights obligations, it is even more imperative that the legal framework for hacking requires specificity of targets.

Use of hacking material as evidence in the justice system

80. 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

[124] *Internet Shutdown Reported Across Syria* – Anne Barnard & Robert Mackey, The Lede: The New York Times Blog, 29 Nov 2012
[125] Draft Code of Practice on Equipment Interference (February 2014), Home Office.

evidence. There is presently no specific regulation of the use of hacking product in criminal trials.[126] The present position at common law is that the prosecution are under a duty to disclose all material in their possession or that they have inspected which may reasonably be considered capable of undermining the case against the defendant. Following the scandal concerning the non disclosure of the identity of undercover police officers during the trial of Ratcliffe-on-Soar protesters, that principle now extends to material relating to the manner in which evidence is obtained where such material might support and argument that its acquisition has resulted in unfairness or abuse. The Rose Report into the Ratcliffe-on-Soar Power Station Protest found that the CPS and the police had together failed to discharge the prosecution's disclosure duties.[127] In recognition of the unique potential of hacking capabilities and to avoid future miscarriages of justice and collapsed trials, the Draft Bill should contain specific proposals to ensure audit trails and police disclosure where prosecutions result from investigations that utilise hacking capabilities.

Recommendations

- Targeted hacking should be subjected to much stricter safeguards than other forms of electronic surveillance given the unprecedented level of intrusion, the harm to device and network security and the risk of damage to evidence that is inherent to the capability.

- Hacking warrants should be authorised only by JCs and only on the application of the intelligence agencies and chief constables, in keeping with the proposed framework for

[126] As Archbold explains - "*Neither the Police Act 1997 nor the 2000 Act purports to deal with the question of the admissibility of evidence obtained under their provisions"* (Chapter 15, paragraph 207).

[127] The police's disclosure obligations are set out in section 3 of the Criminal Procedure and Investigations Act 1996. The prosecution are to disclose all material, either in the prosecution's possession or inspected by the prosecution in connection with the case, which "might reasonably be considered capable of undermining" the case against the defendant. Unused material is required to be disclosed if, and only if, it satisfies this test; unused material which does not fulfil this test need not be disclosed to the defence. As Archbold explains: *"Material may assist the case for the accused not only where it could be used to explain the accused's actions, support his case, or provide material for cross-examination of prosecution witnesses, but also where it might support submissions that could lead to the exclusion of evidence, a stay of proceedings, or a finding that any public authority had acted incompatibly with the accused's rights under the ECHR (see the Attorney-General's guidelines, ante, at paras 10 to 14; and see R. v. Barkshire [2012] Crim.L.R. 453, CA, as to the duty to disclose material that might support an application for a stay based on entrapment)."*So it includes not only material which the prosecution may have seen which is capable of suggesting that the defendant did not commit the crime (or capable of attacking the credibility of prosecution witnesses, for example), but also material, for example, relating to the manner in which the evidence was obtained, where such material might support an argument that its acquisition has resulted in unfairness or abuse. This last principle was established in one of the cases that related to Mark Kennedy, where the CPS had failed to disclose the fact of Kennedy's surveillance (which involved taking contemporaneous notes and covert recordings of the protestors in the alleged preparation and commission of the offences). This would have had the capacity to show that he had acted as an agent provocateur and thereby entrapped those convicted.

interception. Hacking requests should not be available to all police constables as currently provided in the Bill.

- Hacking warrants should only be granted where a JC is satisfied that the objectives of the warrant cannot be achieved by other less intrusive means.

- Hacking warrants should specify named individuals or premises. Thematic warrants aimed at particular locations or activities of a particular description should be removed from the Draft Bill.

- Hacking capabilities allow the authorities complete control over devices and the power to delete, alter or create stored content or communications, often leaving no trace of their actions. In the absence of robust safeguards concerning how hacking powers may be used, they present a grave threat to the integrity of electronic evidence, with corresponding implications for the fairness of trials and the safety of convictions. There should be mandatory requirement to record in a verifiable manner all action taken in relation to a device or network for each individual hack that takes place. There should be an absolute prohibition, backed up by criminal sanction, on creating, altering or deleting content on a hacked device beyond what is necessary to effect the hack. Liberty is deeply alarmed by recent disclosures that the police and Agencies have started hacking devices and networks in the absence of statutory authority and despite the lack of safeguards currently in place to protect against evidence tampering. We believe this has serious implications for the integrity of the UK's criminal and civil justice systems.

- Hacking warrants should be granted for a shorter duration than other forms of surveillance in recognition of the acute security implications of hacking.

Mass surveillance

81. Part 6 of the Draft Bill places the breathtakingly broad mass surveillance powers revealed by Edward Snowden and additional bulk surveillance practices on an explicit statutory footing. New powers to intercept, in bulk, 'external' communications (including vast swathes of domestic communications) and to acquire records of the entire nation's communications data are supplemented by powers permitting "industrial scale exploitation" [128] (GCHQ's own words) of electronic devices and networks. Part 7 further extends blanket surveillance powers away from a focus on the population's communications and towards the acquisition and linking of all public and private sector personal data databases.

Bulk interception

82. The intelligence agencies bulk interception programmes were disclosed for the first time by Edward Snowden in June 2013. They have never been debated or voted for by Parliament. The power to conduct mass interception has instead been inferred by GCHQ from the vaguely worded power in section 8(4) of RIPA. In a radical departure from common and human rights law principles, bulk warrants may be targeted at a telecommunications system or entire populations rather than specific, individual persons or premises as required under section 8(1) RIPA. This approach is maintained in clause 106 of the Bill. 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 reports 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.

83. 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. However, whilst the main purpose of a bulk interception warrant must be to collect "overseas-related" communications or CD, 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[129], the ISC has recently 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

[128] *How the NSA Plans to Infect 'Millions' of Computers With Malware* – Ryan Gallagher & Glenn Greenwald, The Intercept, 12 March 2014
[129] 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

overseas email provider such as Hotmail or Gmail. Searches on Google are counted as an external communication.

84. 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 "general purposes" will suffice.[130] The lack of guidance around what can amount to "specified operation purposes" means that the concept offers little practical protection and could in theory be as broad in its nature as the three grounds on which the warrant was originally justified.

85. While the criteria for selection cannot be "referable to an individual known to be in the British Isles at that time" where "the purpose of using those criteria is to identify the content of communications sent by, or intended for, that individual"[131] 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 with only the requirement of an authorisation from a senior official. 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 119 outlined above, the relevant agency can apply for a targeted interception warrant to examine the material anyway.[132]

86. Liberty, along with partner NGOs has lodged a challenge to the practice of mass interception under 8(4) RIPA at the ECtHR. The case was communicated in November 2015. Whilst the central question of the legality of the UK's bulk external interception regime is yet to be resolved, in *Liberty v UK* (2008), the ECtHR that the system for external interception under the pre-RIPA legislation that allowed interception to cover *'such external communications as are described in the warrant'* violated Article 8. The case concerned 'external communications' interception by the Ministry of Defence of Liberty's telephone, fax and email communications between 1990 and 1997 and the violation allowed the interception of almost all external communications transmitted by submarine. The replacement RIPA framework for 'external interception' now subject to challenge is worded almost identically, as is the power in clause 106(4)(a) of the Draft Bill.

Bulk communications data acquisition

87. On the day that the Draft Bill was published, the Home Secretary announced that since 2005 the Agencies have been acquiring in bulk the communications data of the UK population under the

[130] Draft Investigatory Powers Bill, clause 111.
[131] Draft Investigatory Powers Bill, Clause 119(4).
[132] Draft Investigatory Powers Bill, Clause 12.

vaguely worded section 94 of the *Telecommunications Act 1984.*[133] This had never previously been publicly admitted by the Executive and was apparently only known by a handful of Cabinet ministers.[134] 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.

88. 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

89. 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 draft 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.[135] A bulk hacking warrant can authorise interference with any equipment whatsoever, for the purposes of obtaining communications, private information and equipment data or anything else connected with equipment mentioned in the warrant.[136] Bulk warrants can be issued in the interests of national security, economic wellbeing, or for the prevention and detection of serious crime.[137]

90. The Bill draws a broad overarching distinction – within the vast body of data which can be collected from a bulk hack – between "protected material" and other data. Broadly speaking, protected data is private information and the content of communications. A targeted warrant is required for the examination of protected data obtained under a bulk hacking warrant selected by reference to "an individual known to be in the British Isles at the time". However if data is not selected by reference to those criteria it can be examined without a targeted warrant. This does not prevent the examination of the communications or personal information of those in this country in the pursuit of broader objectives, or in order to access communications data. Where it later transpires that an individual who forms the focus for the selection of protected material is in the UK (even if he was there all along),all that is required to continue the process of examination

[133] Secretary of State for the Home Office the Right Honourable Theresa May, Oral Statement on publication of the Draft Investigatory Powers Bill, 4 November 2015 - https://www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill
[134] http://www.theguardian.com/world/2015/nov/05/nick-clegg-cabinet-mass-surveillance-british-spying
[135] *Draft Investigatory Powers Bill 2015,* Clause 135(1)(c)
[136] *Draft Investigatory Powers Bill 2015,* Clause 135(4)(a)(iv)
[137] *Draft Investigatory Powers Bill 2015,* clause 137

for five days is the authorisation of a senior official. Non-protected data is everything not considered above. Equipment data and any other information connected with equipment which is not a communication or private information can be accessed without any additional authorisation.

91. The Home Office says that "*bulk equipment interference*" has been practiced under the Intelligence Services Act 1994[138], which allows for interference with property or "wireless telegraphy"[139]. Under this law, intelligence services can acquire a warrant to search a property or intercept a person's phone calls. There is no mention in the Act of bulk or mass equipment interference. However, under these out-dated Acts, British intelligence agencies have conducted intrusive, destructive and disturbing mass hacks, such as hacking the largest SIM manufacturer in the world to enable interception of millions of users' calls.[140] The Intelligence Services Act 1994 was written prior to the technological revolution of the past twenty years and cannot be considered a lawful basis for the mass hacking of technologies that were not even conceivable at the time of the Act's writing. Indeed, the Snowden documents revealed that British intelligence agencies expressed concern that their mass hacking practices "*may be illegal.*"[141] [142]

Bulk hacking - a significant expansion of power

92. The "Guide to powers" accompanying the draft Bill makes clear that bulk hacking is a significant step beyond conventional and surveillance powers, remarking that bulk equipment interference "*is used increasingly to mitigate the inability to acquire intelligence through* ***conventional bulk interception*** *and to access data from computers which* ***may never otherwise have been obtainable****" (emphasis added).*[143] Labelling mass interception powers as "conventional" when it is this Bill that for the very first time avows them makes a mockery of our parliamentary democracy. It also demonstrates the apparently insatiable demand from the security services to have unbridled access to all information. This is particularly concerning in light of the broad definition of equipment in the Bill. The draft Bill defines "*equipment"* as "*equipment producing electromagnetic, acoustic or other emissions or any device capable of being used in connection with such equipment*"[144]. This is unfathomably open-ended and could even include cars and aircraft, leaving the power open to potential abuses not just by future UK governments, buy by other states that will follow our lead in legislation.

Bulk hacking - Indiscriminate and speculative

---

[138] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21
[139] *Intelligence Services Act 1994,* Section 5
[140] *The Great SIM Heist* – Jeremy Scahill & Josh Begley, The Intercept, 19 Feb 2015
[141] *UK Perspective on MIKEY-IBAKE*, Sept 2010, p.3 (https://www.documentcloud.org/documents/1077367-uk-perspective-on-mikey-ibake.html)
[142] As recently as April 2013, GCHQ was reluctant to extend deployment of QUANTUM malware due to "legal/policy restrictions": *Legal Issues UK Regarding Sweden and Quantum,* (https://www.documentcloud.org/documents/894386-legal-issues-uk-regarding-sweden-and-quantum.html)
[143] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* pp.20-21
[144] *Draft Investigatory Powers Bill 2015,* clause 149 (1).

93. 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".*[145] 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[146] 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, 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[147], 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.

Security repercussions of bulk hacking

94. 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.[148]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*

[145] *Draft Investigatory Powers Bill 2015: Explanatory Notes*, p. 83
[146] 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
[147] 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).
[148] *Mind-blowing secrets of NSA's security exploit stockpile revealed at last* – Shaun Nichols, The Register, 4 Sept 2015

systems."[149] Furthermore, the UN Group of Governmental Experts (UN GGE) recently released a consensus report, recommending that states "*should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions*"[150]. Although the alarm has been raised on the danger of stockpiling exploits, this Bill would proliferate the practice and in fact boost the market for exploits to be created and sold. In addition, security vulnerabilities created or stockpiled by British intelligence agencies can also be exploited by foreign intelligence agencies or any non-state actors who discover them. ,An explicit British bulk hacking law will set a disturbing precedent for other, more authoritarian states to follow and join a cyber-arms race.

95. "*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 draft Bill, jeopardising human rights in the present and future.

Bulk Personal Datasets

96. 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 Draft 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."* [151]They cover manual and electronic records. Personal data is given a broad definition – it has the same meaning as the *Data Protection Act 1998* but also includes data relating to deceased individuals and data is defined to include 'any information which is not data'. Private misuse of a bulk dataset will be an offence, subject to up to 12 months imprisonment.

97. 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 warrants for other bulk powers in Part 6. Judicial involvement is limited to the flawed judicial review model. "Class warrants" concern applications for *descriptions* of personal data – so presumably 'health data' or 'travel data', for example. Under the terms of the Bill, this is the default type of BPD warrant. '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

[149] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies,* 12 Dec 2013, p. 220
[150] *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – UN GGE, 22 July 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[151] Draft Investigatory Powers Bill, Clause 150

time considers that it would be "appropriate" to seek a specific BPD warrant. Specific BPDs will presumably apply to the most sensitive type of databases – such as mental health hospital data, or patient identifiable FGM data. Applications must include a descriptions of the bulk personal 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.

98. Agencies' acquisition of BPDs was only finally avowed by the ISC in March 2015. In its report, the ISC disclosed limited information about BPDs:

"Bulk Personal Datasets may relate to the following types of information:

a. i)***;

b. ii)***;

c. iii)***;

d. iv)***

e. v)***"

And that, "As of mid-2014:

f. SIS held *** Bulk Personal Datasets;

g. MI5 held ***; and

h. GCHQ held ***"

99. As regards the content and nature of BPDs, the ISC set out that:

"***These datasets vary in size from hundreds to millions of records. Where possible, Bulk Personal Datasets may be linked together so that analysts can quickly find all the information linked to a selector (e.g. a telephone number or ***) from one search query."***[152] And the datasets "***may include significant quantities of personal information about British citizens***".[153] Apparently "*None of the Agencies was able to provide statistics about the volume of personal information about British citizens that was included in these datasets*".[154] The Director General of MI5 has also cryptically explained to the ISC: *"there are datasets that we deliberately*

[152] ISC report, para 156.
[153] ISC report, para 158.
[154] ISC report, footnote 142.

choose not to reach for, because we are not satisfied that there is a case to do it, in terms of necessity and proportionality."[155]

Sensitive information is apparently held in the datasets including an individual's religion, racial or ethnic origin, political views, medical condition, *, sexual orientation, or any legally privileged, journalistic or otherwise confidential information**.[156] The ISC notes in passing that the Agencies **may share the datasets with overseas partners**.[157] Each Agency reported that they had disciplined – or in some cases dismissed – staff for inappropriately accessing personal information held in these datasets in recent years.[158]

100. The acquisition of bulk private and sensitive data on the UK population by the intelligence agencies is a new and radical development. There is currently no legal authority for the Agencies to acquire these datasets. As the ISC diplomatically put it "*the rules governing the use of Bulk Personal Datasets are not defined in legislation*".[159] Government further claims that BPDs may be acquired by using investigatory powers – which means that Government believes it can use surveillance capability, such as hacking or interception to obtain mass data sets from a private company or public body. It also hints that it buys mass datasets from the private sector.[160]

101. **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 and concludes that BPDs are 'relevant' to national security investigations. "Enriching" and "relevant" does not meet the legal threshold for lawfulness.

Recommendation

- Part 7 should be removed from the Bill. There is no operational case for the Agencies to collect, process and link personal data on the entire UK population. It is in principle a deeply offensive proposition. Current law allows data to be transferred across the private and public sector to further national security and the prevention and detection of crime. The Agencies therefore already have gateway powers to obtain information on those it identifies as being subjects of interest.

Are bulk powers necessary?

102. While Liberty supports the use and value of targeted intrusive surveillance powers, we believe that the mass speculative interception of communications; retention and acquisition of

[155] ISC report, para 162.
[156] ISC report, para 163.
[157] ISC report, para 163.
[158] ISC report, para 163.
[159] ISC report, para 157.
[160] Guide to Powers and Safeguards, para 71.

communications data; bulk hacking and bulk personal dataset acquisition is unlawful, unnecessary and disproportionate.

103. The Government has not really attempted to make an operational case for bulk surveillance. The bulk powers are presented in the draft Bill as "*crucial to monitor known and high-priority threats"* and also as "*a vital tool in discovering new targets and identifying emerging threats".*[161] In his July report, David Anderson offered six anecdotes provided by the Agencies in an attempt at justifying mass interception. However, with the vague and limited information provided, it is impossible to assess whether the security outcomes could have been achieved by using the wealth of targeted and operation-led intrusive surveillance powers at the Agencies' disposal. In nearly all of the examples, reference is made to known terrorists or a specific "intelligence operation".

104. The available evidence indicates that mass surveillance powers have not been effective in tackling serious crime, especially not terrorism. Rather, there is evidence that mass surveillance practices impede law enforcement efforts. Bulk telephone data has not proved useful for counterterrorism in the U.S.. The Privacy and Civil Liberties Oversight Board, an independent executive branch board in the U.S., found that the bulk telephone records program conducted under Section 215 of the USA Patriot Act not only raised constitutional and legal concerns, but had no material counterterrorism value:

> *"Based on the information provided to the Board, including classified briefings and documentation, we have not identified a single instance involving a threat to the United States in which the program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.*[162]

105. Similarly, the President's Review Group on Intelligence and Communications Technologies concluded in 2013:

> *"Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."*[163]

[161] Guide to powers, p.20 para. 33
[162] *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* – Privacy and Civil Liberties Oversight Board, 23 Jan 2014, p.11
[163] *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* – 12 Dec 2013, p. 104

106. Both panels' findings refuted Keith Alexander and President Obama's claims that "at least fifty threats" had been averted and "lives have been saved" as a result of bulk metadata retention. Both panels advised that the bulk surveillance program should be shut down. Section 215 was allowed to expire in May 2015.[164] The USA Freedom Act followed, reducing the capacity of the NSA to undertake mass collection of Americans' phone records, requiring instead that a subset of data be requested pursuant to limits set out in the Act.[165]

107. A number of former US intelligence professionals have publicly disclosed "bulk data failures" or blown the whistle on mass surveillance practices. William Binney, former Technical Director of the NSA has spoken out about the risk of "bulk data failure" since retiring after the September 11th 2001 attacks when much of the technology he had designed was subverted for mass surveillance. Binney has submitted evidence to the Joint Committee on the Draft Bill in which he described the bulk proposals as "*flawed and likely seriously to fail to serve current intelligence and data analysis problems for such purposes as Counter Terrorism*"[166]. Binney warned that, "*bulk data over collection from Internet and telephony networks undermines security and has consistently resulted in loss of life in my country and elsewhere, from the 9/11 attacks to date*". Instead, Binney advocates filtering at the point of collection, as he designed his original NSA program, rather than bulk collection and retention. In his evidence, Binney explains that such an approach would protect innocent citizens' privacy, protect privileged communications and relieve analysts of the burden of bulk data. Thomas Drake, a former senior executive at the NSA alongside Binney and later a whistle-blower, has also warned of the dangers of mass surveillance programs, both to civil liberties and national security. He has testified[167] that with a "smaller haystack" of data, the 9/11 attacks would have been preventable.[168] FBI whistleblower Coleen Rowley has also warned against mass surveillance systems following the 9/11 intelligence failures she experienced:

> *"I fear that terrorists will succeed in carrying out future attacks – not despite the massive collect-it-all, dragnet approach to intelligence implemented since 9/11, but because of it. This approach has made terrorist activity more difficult to spot and prevent."*[169]

108. Prior to the Snowden revelations, and in the wake of the murder of Fusilier Lee Rigby, former head of MI5 Dame Stella Rimington warned of the "well-known problem" of big data, drawing comparisons with the East German Stasi's "overdose" of information:

---

[164] *Section 215 Expires – For Now* – Mark Jaycox & Dia Kayyali, EFF, 31 May 2015
[165] USA Freedom Act 2015, available at: http://judiciary.house.gov/_cache/files/1cb59778-0a72-4c09-920d-0e22bf692bb4/fisa-01-xml.pdf.
[166] *Written evidence* – William Binney, 9 Dec 2015, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/draft-investigatory-powers-bill-committee/draft-investigatory-powers-bill/written/25753.html
[167] Drake's testimonies to two Congressional investigations about 9/11 remain classified
[168] *After Paris, be careful what you ask for: an interview with Thomas Drake* – Thomas Drake & Mary Fitzgerald, 24 Nov 2015
[169] *The bigger the haystack, the harder the terrorist is to find* – Coleen Rowley, The Guardian, 28 Nov 2014, http://www.theguardian.com/commentisfree/2014/nov/28/bigger-haystack-harder-terrorist-communication-future-attacks

"Intelligence services can strangle themselves if they have too much information, because they can't sort out from it what they need to know and what they don't need to know."[170]

109. Furthermore, scientists have rightly condemned *"how little of the debate [on mass surveillance] has dealt with the likely success of these tactics (…)",* arguing that *"the efficacy of such surveillance programs must be clearly understood if a rational policy is to be developed"*. The statistics journal *Chance* published a paper on the risk of automatic screening processes (such as those used for bulk interception, bulk data retention and upstream collection), which concluded that whilst a 99% accurate system would indeed report on 99% of the terrorists, the margin of error would also be responsible for producing hundreds of thousands, if not millions, of reports on innocent citizens.[171] This is partly the cause of "bulk data failure" that former intelligence professionals have described.

110. 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[172] and the murder of Lee Rigby.[173]

111. No evidence has thus far been provided to illustrate a unique or critical contribution of bulk 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.

Is bulk surveillance proportionate?

112. It will never be proportionate in a democratic society during peacetime, to mass collect, monitor or process innocent communications in order to find those that threaten our security.

---

[170] *Terror watch lists: Can you keep tabs on every suspect?* – Ruth Alexander, BBC Magazine, 2 June 2013

[171] *Until proven guilty: False positives and the war on terror* – Howard Wainer & Sam Savage, Chance, March 2008, 21(1), pp.59-62, https://www.researchgate.net/publication/242713602_Until_proven_guilty_False_positives_and_the_war_on_terror

[172] *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

[173] *Report on the intelligence relating to the murder of Fusilier Lee Rigby* – Intelligence and Security Committee, 25 Nov 2014

Indeed this is why Britain – as opposed to totalitarian countries - has traditionally rejected this model. To take an example, the British postal service has never been required to intercept or store every letter or parcel it handles nor to make a note of the sender addressee and the time it was posted just in case the content or record of the package may in future be useful to the police or the security services. This important principle remains regardless of the mode of communication. Just because new ways of communicating electronically have made surveillance of innocents less expensive and burdensome than it may have been in the past, does not mean it is in society's interest to allow it.

113. The Government has previously attempted to argue that bulk interception is not intrusive if it is carried out by machines rather than humans. This is analysis is deeply flawed. There is nothing passive about mechanical State interception of communications and acquisition of communications data. The State cannot physically intercept a communication in a way that doesn't interfere with privacy just because it claims that human eyes will not necessarily see it.

114. Bulk surveillance also removes the possibility of safeguarding confidential and privileged communications. As a result of proceedings brought by Liberty and others, the IPT disclosed in June 2015 that **GCHQ had unlawfully intercepted and examined** private communications of **the Egyptian Initiative for Personal Rights (EIPR) and Legal Resources Centre (LRC) in South Africa**.[174] It later amended its ruling to clarify that the Agency had unlawfully intercepted and **examined Amnesty International's communications** rather than those of EIPR. GCHQ's activity was however only deemed unlawful because the Agency had breached its own internal guidance in a technical manner. The judgment provided no explanation as to why human rights NGOs had been bulk intercepted and individually examined and perversely did not find this action to amount to a breach of the ECHR. Indeed on its face the Draft Bill would permit the routine bulk interception and examination of human rights NGOs, lawyers, journalists, elected representatives and others.

115. Mass surveillance has significant and untested implications for the future of our society. David Anderson's report noted:

> *"the collection of vast volumes of data enables the identification of patterns and predictions of future behaviour, a process called predictive analytics, data mining or Big Data. An example of this technique is a predictive policing system called PredPol, which analyses large volumes of crime reports to identify areas with high probabilities for certain types of crime. The system has been used by Kent Police to predict when and where drugs crimes and robberies are likely to take place. PredPol is simply about when and where a crime will take place; other technology is aimed at predicting who will commit them. In 2011, the US Department of Homeland Security tested Future Attribute*

[174] The Tribunal did not make determinations concerning whether the other eight organisations had been intercepted.

Screening Technology, which seeks to identify potential criminals by monitoring individuals' vital signs, such as cardiovascular signals and respiratory measurements. " [175]

116. Liberty is concerned that the Agencies and law enforcement will in future seek to exploit so-called Big Data to predict behaviour. This would be a chilling shift in the relationship between the individual and State and could prove disastrous for the life chances of young people belonging to 'suspect' marginalised or disenfranchised groups.

117. The digital and technological revolution of the past fifteen years has led the Agencies to seek to collect ever-increasing troves of data and to devise mechanical programs to search databases for so-called suspicious patterns. Coupled with this, the current oversight model contains no checks on the Agencies overarching strategy which is instead self-determined and evaluated. However the current direction is unsustainable. Data is increasing exponentially. Liberty understands the agencies now have the capacity to hoover up 15 times the amount of data being collected when Edward Snowden blew the whistle in 2013. We urge independent parliamentarians and policy makers to reflect on the broader strategy and assess the value of harvesting overwhelming amounts of information.

[175] David Anderson QC, A Question of Trust, paragraph 4.40

Confidential and privileged correspondence

118. Liberty believes that the authorisation process for all types of surveillance in the Draft Bill falls short of that which is required by human rights standards. We are additionally alarmed by the complete absence of safeguards for the protection of confidential and privileged communications on the face of the Draft Bill.

MPs, Peers, MSPs, AMs, MLAs, MEPs

119. The communications data of MPs, Peers and other elected representatives receives no explicit protection in the Draft Bill. Data will remain accessible to a multitude of public authorities through the general system of self-authorisation.[176] MPs communications and devices will also be subject to mass interception, hacking and communications data acquisition by the Agencies under Part 6 of the Bill and MPs personal data will be acquired in bulk by them under Part 7. The only 'safeguard' against targeted hacking and interception is a requirement that the Secretary of State will 'consult' the Prime Minister before such targeted warrants are authorised.[177]

120. Until October 2015, it was widely understood that the communications of MPs were protected from interception by the Wilson Doctrine. On the 17th November 1966 the then Prime Minister, Mr Harold Wilson, said in a statement in the House of Commons:

> *"As Mr Macmillan once said, there can only be complete security with a police state, and perhaps not even then, and there is always a difficult balance between the requirements of democracy in a free society and the requirements of security. With my right hon. Friends, I reviewed the practice when we came to office and decided – on balance – and the arguments were very fine – that the balance should be tipped the other way and that I should give this instruction that there was to be no tapping of telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it. I am aware of all the considerations which I had to take into account and I felt that it was right to lay down the policy of no tapping of telephones of Members of Parliament."*[178]

This protection, extended to members of the House of Lords in 1966, was repeated in unequivocal terms by successive Prime Ministers. Tony Blair clarified in 1997 that the policy

[176] This follows the Government's statement March 2014 that it does not consider the Wilson doctrine to apply to communications data (HC Deb, 12 March 2014, column 306).

[177] Clause 16 and clause 85.

[178] HC Deb 17 November 1966 Vol 736, columns 634-641.

"applies in relation to telephone interception and to the use of electronic surveillance by any of the three Security and Intelligence Agencies."[179]

121. Despite this clear and unambiguous statement that MPs and Peers would not be placed under electronic surveillance, in a recent decision the Investigatory Powers Tribunal held that the doctrine had been unilaterally rescinded by the Executive.[180] Liberty disputes this finding. The unequivocal statement made by Prime Minister Wilson back in 1966 was a constitutional convention protecting vital discourse between the people and their ultimate representatives, creating a legitimate expectation on the part of parliamentarians and their constituents that their correspondence was protected. However, there is currently no right of appeal against decisions of the IPT.

122. Liberty believes it is illogical to suggest that an adequate replacement to the previous complete prohibition on surveillance of politicians is to require the Secretary of State to consult with the Prime Minister prior to signing a targeted interception or examination warrant. Instead of securing an independent system, involving two politicians rather than one makes 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. 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

123. Clause 61 would require a public authority to apply to a Judicial Commissioner to confirm an authorisation to obtain communications data for the purpose of identifying or confirming journalistic sources. A Judicial Commissioner may approve the authorisation if the requirements of Part 3 are met. The Bill is silent on protections against the interception or hacking of journalists.

---

[179] HC Deb 4 December 1997 Vol 302, Col 321.

[180] In October 2015, the IPT held that the Wilson Doctrine was not absolute and in any case not legally binding and that the protection of politicians' correspondence was instead regulated by secret security service Internal Guidance which was only disclosed over the course of the litigation. Under this Guidance, targeting of a politician will be "exceptional" but not prohibited, and politicians may have their communications gathered by mass interception powers. Where targeted interception takes place, the usual process of political warrantry will apply with "particularly careful consideration" given to the necessity and proportionality of surveillance. A number of individuals within the relevant agency must be informed and their advice invited, which must be recorded on the Central Record. The DG must be consulted before the application is made to the Secretary of State and before deciding on a warrant. Before deciding whether to issue a warrant *"the Secretary of State will need to consult the Prime Minister via the Cabinet Secretary".* This process is now referenced in the Draft Bill.

124. 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. 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: 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 Draft 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.

125. The mechanism introduced by clause 61 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.

126. Liberty believes that the PACE protections should be restored for access to journalistic communications data and that equivalent protections should be in place to safeguard against the equally if not more intrusive hacking powers contained in the Draft Bill.

Lawyers

127. 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 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. Legal privilege does not apply where client-lawyer communications are made in furtherance of a criminal activity.

128. 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.

129. 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."**[181] 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 Draft Bill.

130. The Draft Bill therefore represents an important and timely opportunity to ensure statutory protection for LPP. However, as weak as the protections in the draft Bill are for politicians and journalists, LPP – along with the communications of other professions who handle confidential material such as medical doctors and NGOs - is not even granted the dignity of a name check. The Government intends that the only protection to be offered to these communications will come via a Code of Practice, likely to mirror the weak and ineffective Codes of Practice that already govern this area.[182] This is a wholly unacceptable position which risks fatally and fundamentally undermining fair trial rights in the UK.

Recommendations

- For as long as mass surveillance powers prevail, there is no way to ensure that confidential and privileged communications content and records will not be intercepted, hacked and transferred in bulk to the Agencies with the rest of our communications. To that end the Draft Bill proposes to enshrine in law for the first time, the power to subject MPs, journalists' and

[181] "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/

[182] See for example, the revised Interception Code of Practice, published in 2015. Liberty's response to the consultation on the Draft Code is available at - https://www.liberty-human-rights.org.uk/sites/default/files/Liberty's%20response%20to%20the%20Home%20Office%20consultation%20on%20the%20Interception%20of%20Communications%20Code%20of%20Practice%20(Mar%202015).pdf.

lawyers' communications to bulk surveillance practices. As we argue at paragraphs 80-116) Liberty strongly advocates an end to undemocratic mass surveillance.

- **In addition to ending mass surveillance practices, Liberty believes there should be an extremely strong legislative presumption against the targeted interception, hacking, and acquisition of communications data and all other forms of targeted surveillance against elected representatives, journalists and lawyers. The conditions that must be met before a judicial commissioner can grant a surveillance warrant targeting a member of these groups should mirror the current regime for production orders of journalistic material under PACE, namely (a) there are reasonable grounds for believing an indictable offence has been committed, (b) the material is likely to be of substantial value, (c) 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.**

Encryption

131. Computer security, like all data security, centres on the aim of protecting information from unauthorised access. Encryption is the leading tool in computer security. Encryption is a method of protecting communications or data from unauthorised access and is widely used to protect online browsing, credit card details, online retail, emailing and messaging, medical data, transport infrastructures, proprietary business information, and much more. 'Third party encryption' is that which is supplied by a communications service (such as Google, Facebook), and which is most affected by this Draft Bill. Greater security is found in client-side encryption, whereby the user encrypts information using keys they have generated and that only they (not their service provider) possess. This personally managed encryption features in popular free software such as TrueCrypt (file encryption) and PGP (email encryption).

132. 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"*[183]*,* 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 draft Bill, clause 189 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.[184]

133. The State already has several means to circumvent encryption. Under Section 49 of RIPA 2000, a person using encryption can be compelled to decrypt any information, thus providing it in plaintext, intelligible form; or to hand over the relevant encryption key.[1] Notices can also be issued to attain any information which would facilitate the obtaining or discovery of a key. Police and intelligence agencies also currently claim the power to hack devices, thus circumventing encryption, under the Police Act 1997 and the Intelligence Services Act 1994 respectively. This power is restated and broadened in Part 5 of the draft Bill, with further provisions to perform mass hacking without suspicion in Part 6 (Chapter 3).

134. Despite these powers to require decryption and circumvent encryption via hacking, the Draft 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*[185] grants the State the power to force "*public telecommunications services"* to remove encryption. Under the Draft 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*

[183] *Draft Investigatory Powers Bill 2015: Guide to Powers and Safeguards,* p.29
[184] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (4)
[185] *Regulation of Investigatory Powers Act 2000,* section 12 (1);

owned or operated" by the service, and "*obligations to provide facilities or services of a specified description" – "among other things"*[186]*,* which remain undefined. Whereas provisions under RIPA oblige "*public telecommunications services"*[187] [188] to remove encryption, the draft Bill would oblige any "*telecommunications services"*[189], which are defined as *"any service that consists in the provision of access to, and of facilities for making use of, any telecommunication system (whether or not one provided by the person providing the service)"*[190]. 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. Obligations to remove electronic protection can be issued in either a 'national security notice' or more likely, a 'technical capability notice' from the Secretary of State.[191] There is no judicial authorisation required for either notice. The recipient of such a notice must comply with it[192] but must not disclose the existence or contents of it.[193]

135. 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 Draft Bill demonstrates a misguided commitment on the part of the State to undermine secure spaces in the furtherance of mass surveillance ambitions.

136. These powers do not require prior judicial authorisation or a test of necessity and proportionality. This means that the specific risks and technical consequences that removal of electronic protections and other measures to maintain interception capabilities may incur are not considered when warrants are issued under other Parts of the Bill. It is also concerning that obligations under clause 189 may not necessarily relate to an existing warrant or authorisation. Therefore, a service provider could be compelled with obligations to remove encryption and security measures, perhaps with a view to seeking a warrant for interception in the future, but not necessarily currently holding that warrant. This means that the obligations could be served without even an indirect consideration of necessity and proportionality. It also means that the unprotected material would be easier for any actor to intercept with or without a warrant.

137. Encryption is a critical tool for protecting individuals' rights to privacy and freedom of expression – particularly for those in sensitive professions, and discriminated and minority groups.

[186] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (4).
[187] *Regulation of Investigatory Powers Act 2000,* section 12 (1).
[188] *The Regulation of Investigatory Powers (Maintenance of Interception Capability) Order 2002,* section 10.
[189] *Draft Investigatory Powers Bill 2015,* clause 189, subsection (2)(b).
[190] *Draft Investigatory Powers Bill 2015,* clause 193, subsection (11).
[191] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (1)
[192] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (9)
[193] *Draft Investigatory Powers Bill 2015,* clause 190, subsection (8)

In a 2015 report, David Kaye, the United Nations Special Rapporteur on Freedom of Expression, described encryption as a leading vehicle for online security and freedom, giving individuals:

> *"a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organisations, members of ethnic or religious groups, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression."*[194]

138. In addition to protecting freedom of expression, Kaye found encryption "*essential"* for the exercise of further vital rights, including "*economic rights, privacy, due process, freedom of peaceful assembly and association, and the right to life and bodily integrity"*[195]*.* Kaye analysed submissions on the laws and policies of member states as well as submissions from civil society groups, leading him to conclude:

> *"States should not restrict encryption (…) which facilitate(s) and often enable(s) the rights to freedom of opinion and expression* (…) *States should avoid all measures that weaken the security that individuals may enjoy online, such as backdoors, weak encryption standards and key escrows"*[196]

139. Undermining encryption seriously jeopardises the security of technologies, their users, and modern digital society as a whole. David Anderson found:

> *"Few now contend for a master key to all communications held by the state, for a requirement to hold data locally in unencrypted form, or for a guaranteed facility to insert back doors into any telecommunications system. Such tools threaten the integrity of our communications and of the internet itself."* [197]

However, these practices would indeed be the consequence of clause 189 in the draft Bill. The Information Technology Industry Council (ITI), which represents 62 of the largest technology companies worldwide including Apple, Microsoft, Google, Samsung, Twitter, and Facebook released a statement following the publication of the draft Bill in defence of encryption:

> *Encryption is a security tool we rely on every day to stop criminals from draining our bank accounts, to shield our cars and airplanes from being taken over by malicious hacks, and to*

[194] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye* – UN Human Rights Council, 22 May 2015, paragraph 1
[195] Ibid, paragraph 56
[196] Ibid, paragraph 60. Note: a key escrow is an arrangement in which cryptographic keys are entrusted to a third party (in this context, the state).
[197] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248

otherwise preserve our security and safety. We deeply appreciate law enforcement's and the national security community's work to protect us, but weakening encryption or creating backdoors to encrypted devices and data for use by the good guys would actually create vulnerabilities to be exploited by the bad guys, which would almost certainly cause serious physical and financial harm across our society and our economy.[198]

140. In a recent research paper by world leading technologists, it was concluded that US and UK governments' proposals to achieve "exceptional access" to encrypted communications would "*raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm"*[199]. Security experts agree. In a recent op-ed for the Washington Post Mike McConnell, the former Director of the NSA, Michael Chertoff, former Secretary of Homeland Security and William Lynn, the former Deputy Secretary of Defence argued that, in order to protect economic and national security, encryption should not be undermined for Government surveillance. They concluded, "*(w)e believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring*"[200].

141. There is increasing awareness in the US of the dangers of undermining encryption for mass surveillance purposes. A recent draft opinion paper on strategic approaches to encryption from the National Security Council argued that "*(o)verall, the benefits to privacy, civil liberties and cybersecurity gained from encryption outweigh the broader risks that would have been created by weakening encryption*". The NSC concluded, "*the Administration will not seek legislation that compels providers to enable government access to encrypted information, even pursuant to lawful process*"[201]. Apple's Chief Executive Tim Cook has argued against government attempts to 'backdoor' (i.e. seek or create vulnerabilities in software to achieve unauthorised access) encryption, explaining, *"(t)o protect people who use any products, you have to encrypt (…) Any backdoor is a backdoor for everyone (…) Opening a backdoor can have very dire consequences*"[202]. The UK's national cybersecurity, is an increasingly critical element of our national security. As stated by the Information Technology Council, "*weakening security with the aim of advancing security simply does not make sense"*[203].

142. In addition, the Software and Information Industry Association (SIIA) submitted written evidence to the Science and Technology Select Committee regarding the Draft Bill, seeking

[198] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015
[199] *Keys Under Doormats* – H. Abelson, R. Anderson, S. M. Bellovin, et al., MIT, 7 July 2015
[200] *Why the fear over ubiquitous data encryption is overblown* – Mike McConnell, Michael Chertoff & William Lynn, The Washington Post, 28 July 2015
[201] *Review of Strategic Approaches* – National Security Council; cited in *Obama faces growing momentum to support widespread encryption* - Ellen Nakashima & Andrea Peterson, The Washington Post, 16 Sept 2015
[202] *Apple's Tim Cook declares the end of the PC and hints at new medical product* – Allister Heath, The Telegraph, 10 Nov 2015
[203] *Tech Responds to Calls to Weaken Encryption* – Information Technology Council, 19 Nov 2015

clarification on provisions relating to encryption, and expressing concerns about the pressure to respond to similar requests from multiple governments:

> *Should Western democracies require "backdoors," companies will not have a credible reason not to provide backdoors to other countries. This increases the exposure of critical infrastructure and individuals to attacks and spying from nation state actors, as well as from terrorists and criminals.* [204]

143. The free software community Mozilla, whose web browser 'Firefox' encrypts 100 billion individual web data transfers every day, also submitted written evidence expressing the same concern.[205]

144. "*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) has expressed concern that "*attempts to undermine encryption could damage user trust in online services*".[206] Indeed, if the provision to force removal of encryption is passed it is very likely that users – particularly those in sensitive sectors such as law, journalism and health - will move away from UK technologies and towards providers based in countries that do not undermine security, thus damaging the UK's digital economy. Furthermore, some UK providers may have to discontinue services if they do not wish to mislead customers as to the security features, or indeed if their product design does not include a mechanism by which to remove users' encryption.

145. Anyone intent on evading surveillance need not rely on a telecommunications service to provide encryption, but can easily use open source encryption software with personally generated and managed keys. This type of client-side encryption, typically used to encrypt files and email communications, is independent of third party providers, and as such would remain unaffected by this legislation. The proposal to force telecommunications services to allow government access to masses of encrypted communications, by an offline analogy, is akin to forcing every locksmith to retain duplicates or a master key to thousands of houses to enable suspicionless property searches. By any usual test, this would not be considered a necessary or proportionate measure.

Recommendations

- Liberty believes the power to remove or in any way undermine encryption over entire communication services indiscriminately denies millions of people the right to privacy, and jeopardises freedom of expression. Therefore, Liberty believes that the requirement to remove encryption should be removed from clause 189.

---

[204] *Written evidence regarding Investigatory Powers Bill* - Software & Information Industry Association, 1 Dec 2015
[205] *Written evidence regarding Investigatory Powers Bill* - Mozilla, 1 Dec 2015
[206] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015

- We concur with David Anderson's view that *"(f)ar preferable, on any view, is a law-based system in which encryption keys are handed over (by service providers* [if they have them] *or by the users themselves) only after properly authorised requests*".[207] This should be a tightly regulated power subject to judicial authorisation, and exercised only in the interests of investigating serious crimes. Anderson argued that the best way to set an example to other nations, thus protecting international cybersecurity, is "*by demonstrating an ability to patrol those spaces in tightly defined circumstances, and with sufficient safeguards against abuse*".[208]

[207] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, paragraph 13.12, p.248
[208] Ibid. Paragraph 13.14, p.248

Intelligence Sharing

146. 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 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 explains 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 concludes that *"in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State."*[209] The report also states 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.[210]

147. 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 actions in various statutes.[211] 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..

148. David Anderson's report recommends that information sharing with foreign countries be subject to strict, clearly defined and published safeguards.[212] The report adds 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".*[213] Such safeguards and guarantees are notably absent from the Draft Bill.

[209] Paragraph 6.87.
[210] Paragraph 6.88.
[211] Paragraph 6.89.
[212] Recommendations 76 and 77.
[213] Recommendation 78.

Oversight

149. The Draft 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[214] 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

150. Liberty supports the creation of a single body to undertake the duties and functions currently covered by a range of different surveillance commissioners. 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 169 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.

Recommendation

- Liberty supports the consolidation of the byzantine model of surveillance oversight currently provided by several commissioners. However we are deeply concerned the Draft Bill hands these functions to the newly created body of JCs. **JCs independence and perceived independence will be wholly undermined by the clear conflicts of interest that will likely arise on a regular basis.** We believe that oversight of intrusive powers should be vested and consolidated in a new body independent from the IPC, IPT and Executive.

Post surveillance notification

151. 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.

[214] Draft Investigatory Powers Bill, Clause 170.

152. 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).[215]

153. 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.

154. The Draft Bill provides a new power for the JCs to inform someone subjected to a surveillance error if the JC is made is aware of it; considers it sufficiently serious and the IPT agrees that it is a serious error and that it is in the public interest for the person concerned to be informed.[216] For it to be serious it must have caused '*significant prejudice or harm to the person concerned'*. The Draft Bill states that a breach of the HRA is not sufficient for an error to be considered a serious error. Before making its decision the Tribunal must ask the public authority responsible for the error to make submissions to the Tribunal about the seriousness of the error and the public interest in disclosure. 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 JC's 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.

Recommendation

- **Liberty believes that in order to ensure accountability for surveillance, JCs should be required to notify those subjected to surveillance after an investigation or operation has ended unless there is an objectively justifiable reason for maintaining secrecy.**

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

Reform of the Investigatory Powers Tribunal

155. 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.

Recommendation

- 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.

- 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.

Appeals

156. Liberty welcomes the granting of a right of appeal from the IPT in the Draft Bill which inserts new clause 67A RIPA. This creates a right of appeal and specifies that the appeal only lies against the final determination of a claim / complaint and 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 who would hear the appeal.

Recommendation

- Liberty believes that the right of appeal should be extended to cover any IPT ruling on a point of law, including in the *course* of proceedings, as was the case in Liberty's recent claim in the IPT.
- Liberty believes that the Draft Bill should specify which court the appeal would lie to, rather than the Court of Appeal in England and Wales and equivalent courts in Scotland and NI *unless the Secretary of State provides otherwise*. This is important for costs purposes as CPR 52.9A gives the Court of Appeal the power to limit costs liability when a case comes to it from a non-costs jurisdiction. This would not be the case if the appeal were to a different court.

- Liberty further advocates that the IPT 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