LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on the Investigatory Powers Bill for Committee Stage in the House of Lords

July 2016

About Liberty

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

Liberty Policy

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

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

Contact

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

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

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

Silkie Carlo
Policy Officer (Technology & Surveillance)
Direct Line: 020 7378 5255
Email: silkiec@liberty-human-rights.org.uk

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

CONTENTS

INTRODUCTION

Liberty welcomes the opportunity to provide briefing and amendments to the Investigatory Powers Bill for Committee Stage in the House of Lords. Peers may wish to consult this briefing in conjunction with Liberty's Briefing on the Investigatory Powers Bill for Second Reading in the House of Lords.

This briefing sets out the following proposals:

- To **improve the quality of investigatory powers warrants** by
    - Providing for single-stage judicial authorisation for law enforcement warrants, and a double lock for national security warrants
    - Providing for merits-based judicial authorisation rather than judicial review
    - Requiring reasonable suspicion of a crime
    - Requiring that the subject of a warrant is identified, to prevent 'thematic' warrants
    - Defining 'national security' to ensure warrants are properly issued for this purpose.
    - Amend the privacy clause so to clarify that abiding by the Human Rights Act is not an optional consideration
- To protect **confidential and sensitive communications**, by
    - Protecting legal professional privilege
    - Protecting the confidentiality of MPs' correspondence
- To **remove or amend overly broad powers** by
    - Deleting provisions for internet connection records
    - Deleting provisions for a request filter
    - Deleting provisions to force companies to remove encryption
- To allow the appropriate **transparency** of investigatory powers by
    - Notifying subjects of investigatory powers after the intrusion and investigation has ceased
    - Providing a public interest defence for whistle-blowers.
    - Providing for an Investigatory Powers Commission
    - Provide Treasury funding for oversight arrangements
    - Establishing the Privacy and Civil Liberties Board

We welcome the Home Secretary's agreement to commission a review of the operational necessity of the bulk powers proposed in Parts 6 and 7 of the Bill. As the review is in progress, bulk powers are not discussed further in this briefing.

IMPROVING WARRANTS

Judicial authorisation

Single stage judicial authorisation for law enforcement warrants

Amendments

Targeted Interception

Clause 19, Page 14, line 29, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 30, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 33, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 35, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 38, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 41, leave out paragraph (d)

Clause 19, Page 15, line 1, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 3, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 5, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 8, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 12, leave out paragraph (d)

Clause 19, Page 15, line 16, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 18, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 20, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 23, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 15, line 26, leave out paragraph (d)

Clause 19, Page 15, line 30, leave out subsection (4)

Clause 20, Page 15, line 41, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 20, Page 16, line 9, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 20, Page 16, line 10, leave out “Secretary of State” and insert “Judicial Commissioners”

Page 16, line 21, leave out Clause 21

Page 17, line 32, leave out Clause 22

Page 18, line 25, leave out Clause 23

Targeted equipment interference

Clause 96, page 72, line 16, after ‘Power’ insert ‘of Judicial Commissioners’; leave out ‘: the Secretary of State’

Clause 96, page 72, line 17, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners.

Clause 96, page 72, line 19, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 21, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 24, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 27, leave out paragraph (d).

Clause 96, page 72, line 30, leave out ‘the Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 32, leave out ‘the Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 35, leave out paragraph (b).

Clause 96, page 72, line 41, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 43, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 72, line 45, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’.

Clause 96, page 73, line 1, leave out ‘The Secretary of State’ and insert ‘Judicial Commissioners’

Clause 96, page 73, line 6, leave out paragraph (d).

Clause 96, page 73, line 9, leave out subsection (4).

Clause 96, page 73, line 30, leave out subsection (8).

Page 73, line 33, leave out Clause 97.

Clause 98, page 74, line 26, leave out ‘Secretary of State’ and insert ‘Judicial Commissioner’

Clause 98, page 74, line 28, leave out ‘Secretary of State’ and insert ‘Judicial Commissioner’

Clause 98, page 74, line 30, leave out ‘Secretary of State’ and insert ‘Judicial Commissioner’

Clause 98, page 74, line 33, leave out ‘Secretary of State’ and insert ‘Judicial Commissioner’

Clause 98, page 74, line 36, leave out paragraph (d).

Page 74, line 42, leave out clause 99.

Page 78, line 11, leave out clause 102.

New clause

'Double lock' for warrants pertaining to national security and foreign policy

"Power of Secretary of State to certify warrants

(1) The Secretary of State may certify an application for a warrant in those cases where the Secretary of State has reasonable grounds to believe that an application is necessary pursuant to section 18(2)(a) (national security) and involves—

(a) the defence of the United Kingdom by Armed Forces; or

(b) the foreign policy of the United Kingdom.

(2) A warrant may be certified by the Secretary of State if—

(a) the Secretary of State considers that the warrant is necessary on grounds falling within section 18; and

(b) the Secretary of State considers that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(3) Any warrant certified by the Secretary of State subject to subsection (1) is subject to approval by a Judicial Commissioner.

(4) In deciding to approve a warrant pursuant to this section, the Judicial Commissioner must determine whether—

(a) the warrant is capable of certification by the Secretary of State subject to subsection (1);

(b) the warrant is necessary on relevant grounds subject to section 18(2)(a)and subsection (1)(a) or (b); and

(c) the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

(5) Where a Judicial Commissioner refuses to approve the person's decision to approve a warrant under this section, the Judicial Commissioner must produce written reasons for the refusal.

(6) Where a Judicial Commissioner, other than the Investigatory Powers Commissioner, approves or refuses to approve a warrant under this Section, the person, or any Special Advocate appointed, may ask the Investigatory Powers Commissioner to decide whether to approve the decision to issue the warrant."

Effect

These amendments would give the power to issue targeted interception and targeted equipment interference and examination warrants to Judicial Commissioners rather than the Secretary of State.

As such, these amendments would also remove the responsibility of Scottish ministers to issue warrants within Scotland, replacing the dual political authorisation processes with a single judicial authorisation process for warrants within the UK.

The new clause would give the Secretary of State the power to authorise warrants relating to national security and foreign policy matters in a 'double lock' process.

Briefing

Independent authorisation is required by human rights law

The European Court of Human Rights has stressed the importance of effective supervision of State surveillance by an independent judiciary. In *Klass v Germany* the Court made clear that 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".*[1]

Most recently and pertinently, the ECtHR ruled in *Szabo and Vissy v Hungary* that the Hungarian system of interception violated Article 8 of the Convention. The court commented extensively on the fact that:

[1] *Klass and others v Federal Republic of Germany*, European Court of Human Rights, 2 EHRR 214, 6 September 1978.

"*The measures are authorised by the Minister in charge of justice upon a proposal from the executives of the relevant security services…For the Court this supervision, eminently political,,,. is incapable of ensuring the requisite assessment of strict necessity with regard to the aims and means at stake*".

The Court rejected the Government's argument that a Government minister is better positioned than a judge to authorise measures of secret surveillance and instead held that:

"*the political nature of the authorisation and supervision increases the risk of abusive measures*" concluding that "*For the Court supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees*".[2]

A two-stage authorisation is unnecessary and risks delay.

This apparently and understandably concerns the Agencies. David Anderson reported:

"*There was some resistance on the part of intercepting authorities to the idea of double authorisation, which was perceived as unnecessarily time-consuming."*.[3]

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

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."*[4]

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.

In Second Reading of the Bill in the House of Lords, Lord Lester commented:

[2] Szabo and Vissy v Hungary, paras 75-77.
[3] David Anderson QC, A Question of Trust, paragraph 14.54
[4] David Anderson QC, A Question of Trust, paragraph 14.49.

"'The independent reviewer has said that he knows of no other country in which the Secretary of State holds responsibility for authorising police warrants; judicial authorisation is sufficient. The Home Secretary signs some 1,600 warrants each year, not including national security warrants. If the requirement of her direct approval for police warrants were removed from the Bill, she would have 70% fewer warrants to approve, giving her more time to focus on vital national security interests. That makes good sense."

In addition, Lord Strasburger commented:

"I have sat through endless evidence and debates on the Joint Scrutiny Committee and I have yet to hear a single convincing reason as to why a Minister needs to be involved in day-to-day police warrantry, as the Bill currently provides".

Arguments concerning Ministers' democratic or political accountability for investigatory powers are misconceived and misplaced.

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 public*".[5] 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 54 and similar provisions in the Bill.[6]

This misconception arose again in the Second Reading debate in the House of Lords. Lord Keen asserted that, "*In the end the Secretary of State must be answerable to Parliament for the warrants for these intrusive powers, and that is allowed for".* However, Baroness Hamwee correctly advised peers that "*the Executive's own proposals gag the Secretary of State with regard to that accountability".*

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

In America,[7] federal investigative or law enforcement officers are generally required to obtain judicial authorisation for intercepting 'wire, oral and electronic' communications, and a court

[5] Paragraph 203GG.
[6] Clauses 54 & 56 of the Bill criminalise the disclosure of the existence of an interception warrant without authorisation to do so.
[7] 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*

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.[8] In Canada it is unlawful to intercept private communications unless the interception is in accordance with an authorisation issued by a judge,[9] 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.[10] 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 for law enforcement warrants.

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.

[8] *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).

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

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

Remove the 'judicial review' standard for Judicial Commissioners' authorisations

Amendments

Targeted Interception

Clause 23, page 18, line 28, leave out "review the person's conclusions as to the following matters" and insert "determine"

Clause 23, page 18, line 35, leave out paragraph (a)

Targeted equipment interference

Clause 102, page 78, line 13, leave out "review the person's conclusions as to the following matters" and insert "determine"

Clause 102, page 78, line 17, leave out subsection (2)

Effect

These amendments would remove reference to 'judicial review' standards and allow Judicial Commissioners to make a fresh, merits-based, decision as to the necessity and proportionality of warrants.

Briefing

Whilst Liberty believes that a single stage judicial authorisation process is important for compliance with human rights case law, we can see a role for a double lock process for national security warrants. In either case, to avoid uncertainty and ensure that Judicial Commissioners are not limited to reviewing the Secretary of State's decision, but instead able to determine the necessity and proportionality of warrants on the merits of their contents, all references to 'judicial review' should be removed. The Government has claimed that judges would be able to go further than a narrow procedural review of a Minister's decision yet this is impossible to reconcile with its opposition to removing references to judicial review.

The Government attempted to allay concerns about the limited role of judges with the introduction of a privacy clause, which Judicial Commissioners must now 'consider' when reviewing a Minister's targeted interception warrant (but not an equipment interference warrant). However, this addition has not materially changed the judicial review standard that restricts the role of Judicial Commissioners.

Recently, the ECtHR ruled in *Roman Zakharov v Russia* that the Russian regime for interception violated Article 8. The Court highlighted that while Russian law requires prior judicial authorisation for interception measures, Russian judges in practice only apply purely formal criteria in deciding whether to grant an authorisation, rather than verifying the necessity and proportionality of imposing such measures.[11] Strasbourg case law has evolved since Kennedy v UK and is clear on the need for a fully independent body, with sufficient expertise and agency, to engage in a substantive review of the evidence put forward to justify a surveillance warrant. British judges can only meet that standard with the clear ability to authorise, rather than simply review, warrants.

[11] Roman Zakharov v Russia (47143/06) 4 December 2015, paragraph 263.

Reasonable suspicion

Amendments to require reasonable suspicion of a serious crime

Targeted interception

Clause 20, page 16, line 3, at end insert –

"( ) A warrant may be considered necessary in relation to the grounds falling within (2)(b) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed."

Communications data acquisition

Clause 58, page 47, line 33, at end insert –

"( ) An authorisation may be considered necessary in relation to the grounds falling within (7)(b) or (7)(f) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed."

Communications data retention

Clause 83, page 64, line 15, at end insert –

"( ) A notice may be considered necessary committed in relation to the grounds falling within section 58(7)(b) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed"

Equipment interference

Clause 96, page 73, line 21, at end insert –

"( ) A warrant may be considered necessary committed in relation to the grounds falling within section 96(5)(b) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed"

Effect

These amendments would require that there is reasonable suspicion of serious crime for a warrant authorising interception, communications data acquisition or retention, or equipment interference to be issued, when it is issued for the purpose of preventing or detecting serious crime.

Briefing

One of the greatest problems, recurrent in every power in the Bill, is the lack of a reasonable suspicion threshold for surveillance powers to be authorised for the purpose of preventing and detecting crime.

Intrusive powers can be authorised in order to ‘prevent and detect serious crime’, or even (in the case of communications data’) to collect tax, prevent disorder, or in the interests of public safety. However, these general purposes are left wide open to broad interpretation and abuse without requiring a threshold of proof. A requirement of reasonable suspicion, when the purpose of preventing and detecting serious crime is invoked, would prevent the potential of abusive surveillance of law-abiding citizens that we have seen in the past.

The threshold of reasonable suspicion has long been an important safeguard for both citizens and law enforcers against the risk of arbitrary use of police powers. The ‘necessary and proportionate’ standard invokes an important assessment of the extent of the intrusion, but it does not require a burden of proof. Whilst one would expect that, in practice, targets of surveillance would indeed meet this modest burden of proof, it is negligent not to include the reasonable suspicion threshold on the face of the Bill and leaves these serious powers ripe for abuse.

Identifying subjects of warrants

The Bill, as currently drafted, allows for warrants to be issued in relation to persons, premises, locations, organisations, or 'a group of persons who share a common purpose or who carry on, or may carry on, a particular activity', or for 'testing or training activities'. Warrants need not identify subjects but rather can, for example, 'describe as many of those persons as is reasonably practicable'. This unacceptable standard allows for intrusive powers to be authorised against potentially unknown subjects. Whilst the name of a suspect may not always be known, it should be a bare minimum that a unique identifier (e.g. an IP address) is known to ensure the surveillance is being applied to the intended target, and the warrant is sufficiently specific in its assessment of necessity and proportionality in relation to the subject to be compliant with human rights law.

As currently drafted, targeted warrants may drawn so broadly to in fact be 'thematic' warrants that encompass potentially hundreds of people, or more. This represents a departure from the position at common law which has long banned "general warrants". The Intelligence and Security Committee 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.[12] The Joint Committee recommended "*that the language of the Bill be amended so that targeted interception and targeted equipment interference warrants cannot be used as a way to issue thematic warrants".*[13] The Joint Committee on Human Rights also tabled many of the amendments below at Report Stage in the House of Commons in attempt to require the identification of subjects.

The Marquess of Lothian, a member of the ISC, said during Second Reading of the Bill in the House of Lords that targeted warrants:

> *"can be drawn very widely, potentially catching a large number of people in a single warrant. These concerns have still not been completely met by the Government".*

Lord Lester advised that:

> *"the Bill should be amended to circumscribe the possible subject matter of warrants in the way recommended by the Independent Reviewer of Terrorism Legislation. That will ensure that the description in the warrant is sufficiently specific to enable the*

[12] *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 45.
[13] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, recommendation 38, para. 468

person unknown, but who is the subject of it, to be identified and to prevent the possibility of large numbers of people being potentially within the scope of a vaguely worded warrant".

The amendments recommended below would serve that purpose.

Amendments to require subjects are identified: Targeted Interception

Clause 17, page 13, line 31, after 'person' leave out 'or organisation'

Clause 17, Page 13, line 36, insert after activity 'where each person is named or specifically identified using a unique identifier'

Clause 17, Page 13, line 37, after 'person' leave out 'or organisation'

Clause 17, page 13, line 39, insert after 'operation' 'where each person is named or specifically identified using a unique identifier'

Clause 17, page 13, line 40, leave out paragraph (c)

Clause 17, page 13, line 41, leave out subsection (3)

Clause 29, page 22, line 36, after 'person' leave out 'or organisation'

Clause 29, page 22, line 37, leave out 'or describe that person or organisation' and insert 'or specifically identify that person using a unique identifier'

Clause 29, page 22, line 43, leave out 'or describe as many of those persons as it is reasonably practicable to name or describe' and insert 'or specifically identify all of those persons using unique identifiers'

Clause 29, page 23, line 1, after 'person' leave out 'or organisation'

Clause 29, page 23, line 5, leave out 'or describe as many of those persons or organisations, or as many of those sets of premises, as it is reasonably practicable to name or describe' and insert 'or specifically identify all of those persons using unique identifiers'

Clause 29, page 23, line 8, leave out subsection (6)

Effect

As drafted, clause 17 permits 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 29 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.

These amendments would retain the capacity of a single warrant to permit the interception of multiple individuals but would require an identifiable subject matter or premises to be provided. This narrows the current provisions which would effectively permit a limitless number of unidentified individuals to have their communications intercepted.

Briefing

Liberty believes the scope of warrants permitted fails to comply with both common law and ECHR standards. In *Zakharov v Russia*[14] where the ECtHR found Russia's interception scheme in violation of Article 8 of the Convention, the Court complained that:

> "*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."* [15]

Thematic warrants are sufficiently broad to violate Article 8 and need considerable amendment on the face of the Bill.

Amendments to require targets are identified: Equipment Interference

> Clause 95, page 71, line 31, leave out paragraph (b)
>
> Clause 95, page 71, line 40, leave out paragraph (f)
>
> Clause 95, page 71, line 42, leave out subsection (1)(g)
>
> Clause 95, page 72, line 1, leave out subsection (1)(h)
>
> Clause 107, page 82, leave out lines 35 to 41
>
> Clause 107, page 83, leave out lines 19 to 23
>
> Clause 107, page 83, leave out lines 24 to 28

[14] (47143/06) 4 December 2015.
[15] Paragraph 265.

Clause 107, page 83, leave out lines 29 to 34

Clause 95, page 72, line 3, at end insert -

"(1A) A targeted equipment interference warrant may only be issued in relation to any of the matters that fall under subsection (1) if the persons, equipment, or location to which the warrant relates are named or specifically identified using a unique identifier."

Effect

These amendments would ensure that all targets of hacking are properly named or otherwise identified, removing overly broad and vague subject categories. Warrants may still be granted where the equipment in question belongs to or is in the possession of an individual or more than one person where the warrant is for the purpose of a single investigation or operation; or for equipment in a particular location or equipment in more than one location where for the purpose of a single investigation or operation.

Briefing

Clause 95 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 person or organisation*" or "*a group of persons who share a common purpose or who carry on, or may carry on, a particular activity*" or more than one person or organisation "*where the interference is for the purpose of a single 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 used, for the purposes of a particular activity or activities of a particular description*" as well as testing, developing or maintaining capabilities.

The ISC reported:

> "*the Director of GCHQ suggested that, hypothetically, a Targeted EI warrant could cover a target as broad as an entire hostile foreign intelligence service".*

The breadth of targeted hacking warrants was "*a concern recognised by the Director of GCHQ who noted that* 'the dividing line between a large-scale targeted EI and bulk is not an exact one'".[16]

In addition, the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest".[17] 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. Hacking equipment such as 'IMSI catchers' can, for example, collect the 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.

<u>Amendments to require subjects are identified: Equipment Interference Examination Warrants</u>

Clause 95, page 72, line 6, leave out 'or organisation'

Clause 95, page 72, line 7, leave out paragraph (b)

Clause 95, page 72, line 9, leave out 'or organisation'

Clause 95, page 72, line 11, leave out paragraph (d)

Clause 95, page 72, line 13, leave out paragraph (e)

Clause 95, page 72, line 14, at end insert –

"(2A) A targeted examination warrant may only be issued in relation to any of the matters that fall under subsection (2) if the persons, equipment, or location to which the warrant relates are named or specifically identified using a unique identifier."

Clause 107, page 84, line 3, leave out 'or organisation' on both occasions

Clause 107, page 84, line 4, leave out 'or a description of' and insert 'or a unique identifier for'

Clause 107, page 84, line 5, leave out 'or organisation'

[16] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; para. 14.
[17] *Draft Code of Practice on Equipment Interference* (Spring 2016) - Home Office, p.21, p.29; see also Draft Code of Practice on Equipment Interference (February 2014), Home Office.

Clause 107, page 84, leave out lines 6 to 11

Clause 107, page 84, line 12, leave out ‘or organisation’

Clause 107, page 84, line 15, leave out ‘or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe’ and insert ‘or a unique identifier for each of the persons’

Clause 107, page 84, leave out lines 20 to 29.

Effect

These amendments would refine the matters that targeted examination warrants may relate to by removing vague and overly broad categories and training purposes. Warrants may still be granted where the equipment in question belongs to or is in the possession of an individual or more than one person where the warrant is for the purpose of a single investigation or operation; or for equipment in a particular location or equipment in more than one location where for the purpose of a single investigation or operation.

National Security Definition

Amendment

Clause 235, page 184, line 37, insert –

"national security" means the protection of the existence of the nation and its territorial integrity, or political independence against force or threat of force.

Effect

This amendment would provide for a definition of national security under 'General definitions', to apply throughout the Bill.

Briefing

A principal statutory ground for authorising surveillance is 'in the interests of national security'; another is 'economic wellbeing' as far as it relates to 'national security'. Left undefined, 'national security' is unnecessarily open to broad and vague interpretation. 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 discretion so broad as to be arbitrary. Furthermore, domestic 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.[18] National security as a legal test is therefore meaningless if left without a statutory definition.

Strasbourg case law on this issue has progressed in the past year. In *Zakharov v Russia*, the Court disapproved the open-ended discretion granted to the Russian Executive under its domestic law to undertake interception with the aim of "*obtaining information about events or activities endangering the national, military, economic or ecological security of the Russian Federation*". The Court said -

> *"It is significant that [Russia's domestic interception law] does not give any indication of the circumstances under which an individual's communications may be intercepted on account of events or activities endangering Russia's national, military, economic or ecological security. It leaves the authorities an almost unlimited degree of*

[18] 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".

> *discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse".*[19]

In *Szabo & Vissy v Hungary* the Court similarly observed:

> *"in a matter affecting fundamental rights it would be contrary to the rule of law, one of the basic principles enshrined in the Convention, for a discretion granted to the Executive in the sphere of national security to be expressed in terms of an unfettered power."*[20]

The Joint Committee on the draft Bill recommended that the Bill should include definitions of national security[21] and economic well-being[22]; the ISC further recommended that economic well-being should be subsumed within a national security definition, finding it "*unnecessarily confusing and complicated"*.[23] The ISC queried both the Agencies and the Home Office on this point but reported that '*neither have provided any sensible explanation'*.[24] Their report recommendations were dismissed, and the core purposes for which extraordinary powers can be used remain undefined, and dangerously flexible, in the Bill.

Ken Clarke MP remarked, in the House of Commons' Second Reading of the Bill:

> "*It is true that there is a vast amount of activity under the general title of economic wellbeing. I have known some very odd things to happen under that heading. National security can easily be conflated with the policy of the Government of the day. I do not know quite how we get the definition right, but it is no good just dismissing that point.*"[25]

Baroness Kennedy, in the House of Lords' Second Reading of the Bill, said national security:

> *"can be an elastic notion, capable of being harnessed for questionable ends".*

Clearly, it is time that our legal framework benefitted from a statutory definition of national security. The undefined tests of 'national security' and 'economic well-being' risk interference

[19] At paragraph 248.
[20] Szabo and Vissy v Hungary, para 65.
[21] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 82
[22] Ibid. Recommendation 83
[23] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J (i)
[24] Ibid.
[25] See Hansard, 15 March 2016, http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0002.htm

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.

The definition provided in this amendment is based on the UN's Siracusa Principles.[26] The amendment may be considered a probing amendment to stimulate debate on defining national security, which is an essential task for the passage of this Bill.

[26] Siracusa Principles on the Limitation and Derogation of Provisions in the International Covenant on Civil and Political Rights. Annex, UN Doc E/CN.4/1984/4 (1984)

Amend the privacy clause to require regard to the Human Rights Act

Amendment

Clause 2, page 3, line 6, insert new paragraph (d) –

(d) the requirements of the Human Rights Act 1998

Effect

This amendment would require that a public authority *must* have regard to the Human Rights Act 1998 when making decisions relating to warrants and notices, rather than the current provision that the authority 'may' consider it.

Briefing

The current wording of the provision to optionally consider the Human Rights Act 1998 in the new privacy clause undermines the standing of the Act and the rights within, which are at the heart of constitutional law and British democracy. In doing so, the privacy clause is self-defeating. We urge parliamentarians to correct this drafting error, by making clear that the Human Rights Act *must* be regarded – of course, it is not an optional consideration.

It should also be noted that clause 23 (2)(b), whereby a Judicial Commissioner must comply with the privacy clause (section 2) when authorising interception warrants, has not been applied to clause 102 (2) on equipment interference warrants. We expect that this is a further drafting error.

PROTECTING CONFIDENTIAL AND SENSITIVE COMMUNICATIONS

Legal professional privilege

An amendment prepared by the Law Society and Bar Council addresses some of the defects with the current regime for interception of communications. However, to properly protect LPP the Government needs to adopt a different approach to the one currently contained in the Bill. There should be an **outright prohibition on the targeting of legally privileged material**, with material only targeted where a Judicial Commissioner is satisfied that there is **reasonable suspicion** that the communications in question are intended to further a criminal purpose. Where legally privileged material is inadvertently captured (as it is material which does not further a criminal purpose), it must be **destroyed immediately**. Any additional rules for the handling of material in these circumstances must be on the face of the Bill and written in explicit terms. The Government should also **ensure that protections extend to other forms of interference**, including communications data.

Parliamentarians' correspondence

Amendment

Clause 26 page 20, line 23, leave out "Secretary of State' and insert 'Judicial Commissioner'

Clause 26, page 20, line 32, leave out subsection (2) and insert –

(-) Further to the requirements set out elsewhere in this part, the Judicial Commissioner may only issue a warrant if –

(a) there are reasonable grounds for believing that an serious criminal offence has been committed, and

(b) there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation in connection to the offence at (a), and

(c) other proportionate methods of obtaining the material have been tried without success or have not been tried because they were assessed to be bound to fail, and

(d) it is in the public interest, having regard to the democratic interest in the confidentiality of correspondence with members of a relevant legislature.

Effect

This amendment would ensure that applicantions to intercept the communications of parliamentarians would be made to the judicial commissioner rather than to the Secretary of State via the Prime Minister. It would also set out additional requirements that the judicial commissioner must take into account before granting a warrant.

Amendment

Page 80, line 12, leave out Clause 105 and insert –

(1) This section applies where –

(a) an application is made to the Judicial Commissioner for a targeted equipment interference warrant, and

(b) the warrant relates to a member of a relevant legislature.

(2) This section also applies where –

(a) an application is made to the Judicial Commissioner for a targeted examination warrant, and

(b) the warrant relates to a member of a relevant legislature.

(3) Where any conduct under this Part is likely to cover material described above, the application must contain –

(a) A statement that the conduct will cover or is likely to cover such material

(b) An assessment of how likely it is that the material is likely to cover such material

(4) Further to the requirements set out elsewhere in this part, the Judicial Commissioner may only issue a warrant if –

(a) there are reasonable grounds for believing that a serious criminal offence has been committed, and

(b) there are reasonable grounds for believing that the material is likely to be of substantial value to the investigation in connection to the offence at (a), and

(c) other proportionate methods of obtaining the material have been tried without success or have not been tried because they were assessed to be bound to fail, and

(d) It is in the public interest having regard to:

a. the public interest in the protection of privacy and the integrity of personal data, and

b. the public interest in the integrity of communications systems and computer networks, and,

c. democratic interest in the confidentiality of correspondence with members of a relevant legislature.

<u>Effect</u>

This amendment would ensure that applications for a targeted equipment interference warrant or targeted examination warrant are granted on application only to a Judicial Commissioner, removing the role of Secretary of State.

This amendment would also apply additional safeguards to the correspondence of parliamentarians when a warrant for hacking is sought.

Briefing

It is inherent to our democracy that members of the public can correspond with their representatives in private. As stated by Keir Starmer MP QC during Committee Stage debate of the Bill in the House of Commons:

> *"On the general principles, the first thing to say about journalistic material and communications sent by or intended for Members of this Parliament and other relevant legislatures is that the protection is not for the benefit of the journalist or the Member of Parliament but for the wider public good."*[27]

In the House of Lords, Baroness Hayter added:

> *"We will want to test the current wording on these sensitive professions, as the Bill perhaps has not yet achieved the right balance in protecting the privacy of those who need it most."*[28]

Liberty believes it is illogical to suggest that an adequate replacement to the previous complete prohibition on surveillance of politicians is expressly allow it, only requiring the Secretary of State to consult with the Prime Minister prior to authorising interception or hacking. Instead of securing an independent authorisation process, involving two politicians rather than one would make the process more political rather than less.

While Liberty believes that a single process of judicial authorisation ought to exist across the Bill, in relation to the power to surveil politicians it is absolutely imperative to remove any political involvement from the process. 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 be rebutted only in clear and specific circumstances overseen only by Judicial Commissioners, without political involvement. It is also essential that the protections granted to elected representatives are consistent across the different methods of surveillance.

As part of the discussion concerning the protection of correspondence with elected representatives in the House of Commons Committee Stage of the Bill, Government Minister John Hayes stated:

> *"I think that the hon. and learned Gentleman is right that close examination of consistency in the Bill, in terms of how we deal with Members, is important. To that*

[27] IP Bill Committee, 12 April 2016, at column 190.
[28] IP Bill Second Reading in the House of Commons, 27 June 2016, Hansard, column 1458.

end, I hear what he says and will look at this again. The conversation on this, in the Committee and more widely, needs to take full account of the proper assumption on the part of those who contact their Members of Parliament that any material they provide will be handled with appropriate confidentiality and sensitivity. The hon. and learned Gentleman makes that point well. It is a point that I have heard and will consider further."[29]

[29] IP Bill Committee Hansard, 21 April 2016, John Hayes MP, at column 402

REMOVING AND AMENDING OVERLY BROAD POWERS

Internet Connection Records

Amendment

Clause 83, page 65, line 30, leave out “therefore includes, in particular” and insert “does not include”

Effect

This amendment would remove the requirement for ‘internet connection records’ to be retained by ISPs.

New Clause

Tabled by Baroness Hamwee and Lord Paddick.

Internet Connection Records

(1) Nothing in this Act shall permit the retaining by a public authority of internet connection records.

(2) In this Act “internet connection record” means communications data which –

a. may be used to identify, or assist in identifying, a telecommunications service to which a communication is transmitted by means of a telecommunication system for the purpose of obtaining access to, or running, a computer file or computer program, and

b. comprises data generated or processed by a telecommunications operator in the process of supplying the telecommunications service to the sender of the communication (whether or not a person).

Effect

This new clause would explicitly prohibit public authorities retaining internet connection records.

Briefing

The Bill describes a new category of information – an internet connection record – and provides significant new powers (a) for the Home Secretary to require telecommunications operators to generate and retain ‘internet connection records’ (ICRs) for up to 12 months

and (b) for a multitude of public authorities to gain access to ICRs. The Data Retention and Investigatory Powers Act, 2014 allows for communications data to be retained that identifies the senders and recipients of communications online but 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.[30]

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.[31] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access. In 2014, there were 517, 236 authorisations for public authorities' access to communications data.[32] Making the population's internet histories also available to police for any investigative purpose will lead to unprecedented covert intrusion into potentially hundreds of thousands of peoples' private lives.

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 will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[33] within the public authority, and then by a 'single point of contact.'[34]Provisions in the Bill would permit law enforcement and public authorities to gain access to ICRs to reveal all the internet connections of a subject or subjects.[35]

ICRs are not the equivalent of a telephone call record

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.

The Government compares internet connection records to telephone records and asserts that expansion into internet records is merely filling a gap left by technological innovation.

---

[30] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[31] *Investigatory Powers Bill 2016,* schedule 4, part 1
[32] *Statistics: Communications Data* – IOCCO, http://www.iocco-uk.info/sections.asp?sectionID=12&type=top, retrieved 10 March 2016
[33] *Investigatory Powers Bill 2016,* clause 53
[34] *Investigatory Powers Bill 2016,* clause 67. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[35] *Investigatory Powers Bill 2016,* clause 54, subsection (4)

Similarly Baroness Harding, CEO of TalkTalk (one of the major ISPs to be reimbursed by the Home Office for generating ICRs), supported the policy during Second Reading of the Bill in the House of Lords claiming that "*Knowing what website someone visits is just the modern equivalent of knowing who they called*". However, such comparisons are deeply misleading. Call records show who telephoned who, where and when; internet connection records, by offline analogy, are more comparable to a compilation of call records, postal records, library records, study and research records, film and TV records, political and religious records, shopping records, leisure records, location records, and additionally capture concerns about health, sexual and family issues.

ICRs do not naturally exist

ICRs do not naturally exist within the technical infrastructure of a telecommunications operator. Under this Bill, telecommunications operators would be forced to make considerable infrastructural changes to generate and retain ICRs in bulk. Although there are a variety of ways in which authorities can obtain comparable data on a targeted basis, **there is no targeted method by which to generate "ICRs" – this is inherently a bulk power.** Correspondingly, the Agencies would be able to acquire this intrusive, population-level data in bulk under the terms in this Bill.

There is nothing on the face of the Bill to limit the potential data fields within ICRs. Rather, the Home Office describes the definition of ICRs as 'flexible'[36], and the draft Code of Practice confirms that 'there is no single set of data that constitutes an internet connection record'.[37] The Home Office was pressed to release further evidence to define what would be collected as 'communications data' including ICRs to the Joint Committee. It released an annex of 'examples' which revealed that the following fields of information are included in an internet connection record: [38]

- Websites visited
- Timestamp of each internet connection
- IP addresses
- Names
- Addresses
- Email addresses

[36] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.1
[37] *Communications Data: Draft Code of Practice* – Home Office, 1 March 2016, p.18
[38] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.6

- Telephone numbers
- Billing data
- Usernames
- Passwords
- Location data
- Unique device identifiers (MAC address, IMSI, IMEI)

Widespread concerns from major tech companies in response to the Home Office's incompetent ICRs proposals led the Committee to recommended that "*more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level.*"[39]

Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways.

As noted by Lord Paddick:

> *"The security services MI5, MI6, and GCHQ say that they do not need internet connection records because they can get the information they need by other means".*

Police can also obtain this information by several means. First, they can request telecommunications operators to retain the data of specific targets on a forward-looking basis[40], or they can conduct targeted interception.

Secondly, they can request retrospective 'internet connection' data on specific targets from operators who temporarily store it for their own business purposes.[41]

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.[42] 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[43]. The ISC noted that the delivery of ICR proposals:

> *"could be interpreted as being the only way in which Internet Connection records may be obtained. However, this is misleading: the Agencies have told the Committee that*

[39] Ibid. Recommendation 7, para. 122
[40] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25
[41] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[42] *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
[43] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015

they have a range of other capabilities which enable them to obtain equivalent data."[44]

The ISC recommended that this be amended in the Bill "*in the interests of transparency*"; yet no such transparency has been provided.

It is far more preferable, with regard to human rights, law enforcement, and public spending, to employ robust targeted powers on identified suspects than intrude on the rights of the entire population. Some unconvincing attempts have been made to explain why existing powers, including using targeted interception, making targeted requests for communications data from service providers, and seizing and forensically examining a device, may sometimes be deemed less desirable than mass ICRs.

For example, it is claimed[45] that services such as Facebook may not hand over stored data unless police provide evidence that the individual in question definitely accessed their service.[46] This is entirely at odds with common practice – Facebook and other providers assist with law enforcement extensively. Additionally, it has been said that an alternative highly insightful method, seizure and examination 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*".[47] Investigators would rather "*develop intelligence on the group covertly*" and establish any possible "*previous linkages"* between group members. However, this is also an unrecognisable argument - 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. The arguments against using existing methods are wholly unconvincing and are far from justifying this mass surveillance regime of unprecedented intrusion and extremely limited effectiveness.

Lord Oates remarked:

"That is not evidence-based policy-making; it is policy-based evidence making".

[44] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation I.
[45] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4
[46] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25
[47] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17

Liberty believes the case supporting this expanded data collection is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[48]

There is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[49].

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.[50] As the CJEU ruled in 2014,[51] 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.

ICRs do not and cannot meet the stated policy aims

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 was 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".*[52] In response, ISPA (Internet Service Providers Association) members *"pointed out the huge flaw in this argument*".[53] Often, ICRs would not accurately show *when* communications services have been used, and therefore would not be helpful for informing an accurate time frame for further communications data requests. This is because communications software (particularly on smartphones) makes frequent internet connections whether in use or not, remaining connected for a period of days, weeks or months.[54] Connection records show

[48] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[49] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[50] Ibid
[51] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014
[52] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[53] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html
[54] 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.

connection timestamps rather than access timestamps. ISPs and technologists have expressed serious concern that the Home Office has based an extensive, invasive data collection policy on misleading descriptions of what purposes ICRs could serve.

Even without using widely available privacy software, ICR data is "inexact and error-prone".[55] But the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of serious crime is vanishingly slim, as pointed out by ISPs and technologists.[56] Many online criminals do not, and certainly will not, offend using the internet under the conditions for which an internet connection record would need to be meaningful – that is, using a regular browser or public file sharing service on their own device, using personal internet connections, and 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 misleading where such privacy tools have been used. In addition, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This digital shift renders ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

ICRs can be dangerously misleading and falsely incriminating

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.

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 generates a separate 'internet connection', which may relate to a server (or 'site') 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

[55] *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

[56] *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

and a pop-up. Therefore, an ICR could show repeated access to a website hosting indecent images, which could in fact represent an unwanted pop-up during innocent web browsing. Bulk ICR retention could be exploited by hackers for nefarious purposes – for example, by embedding 'suspicious' scripts into webpages (e.g. linking to ISIS or jihadist websites), 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. This also regularly creates involuntary, misleading internet connections. Clearly, bulk ICRs collected on a population-wide scale will lead to misleading, inaccurate and potentially suspicious information being generated on many innocent internet users.

ICRs have failed, at enormous public cost, where practiced before

In evaluating the efficacy of ICRs, 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.[57] **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.**[58] In fact, Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[59] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[60] In June 2014, the Danish government repealed the obligation on operators to retain session data on the basis that it was "*questionable whether the rules on session logging can be considered suitable for achieving their purpose*".[61]

[57] *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

[58] *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).

[59] Ibid.

[60] *Written evidence on Investigatory Powers Bill: Technology Issues* - IT-Political Association of Denmark, 2 Dec 2015, p.2

[61] *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

In response to widely expressed concerns about the UK adopting this failed model, the Home Office published a document comparing the Dutch case study with current UK plans.[62] Despite the rhetoric of "*important differences"*, there are only two minor differences in substance. Firstly, the UK Government promises (although will not make a statutory commitment) to meet communication service providers' costs *upfront* to cover the necessary infrastructural change, drain on resources, and generation and storage of data – whereas in Denmark, CSPs were remunerated *after* they implemented infrastructural change. It does not follow that this different mode of reimbursement will affect the usability of data, and if anything, gives rise to concerns about huge bills from internet companies to be footed by the taxpayer. Secondly, the Home Office makes much of the "*flexibility to tailor the design of ICR retention models*", referring to the lack of definition of ICRs and the intention to 'negotiate' with CSPs as to what data is generated and how. However, the Danish model also employed flexible regulation. The proclaimed difference is largely one of intent – the Home Office intends to exert an unprecedented level of control over CSPs through 'negotiations' which it anticipates will provide for never-before-seen modes of tailored data collection at the population level. These proposals have proved deeply unconvincing, unpopular, and even alarming to CSPs.[63]

Threat to security posed by bulk retention of ICRs

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*".[64]**

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*

[62] *Comparison of internet connection records in the Investigatory Powers Bill with Danish Internet Session Logging legislation* – Home Office, 1 March 2016

[63] See written and oral evidence to the Joint Committee and the Science and Technology Committee.
[64] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.

happen, potentially damaging inferences about people's interests or activities could be drawn".[65]

The Joint Committee on the draft Investigatory Powers Bill noted that "*data theft remains an ongoing challenge".*[66]

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 hacked in the world,[67] 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 – burdening 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 Bill places a duty on overseas operators to collect and retain ICRs on UK citizens.[68] 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.[69]

ICR retention will not be able to meet its stated purposes, and certainly not with any greater efficacy than the targeted surveillance methods available for investigations; in fact, it could easily cause false suspicion. Arguably, the £175+ million budgeted to fund telecommunications operators to spy on their customers would be better spent on frontline staff or community policing.

---

[65] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29
[66] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Para. 174
[67] 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.
[68] Investigatory Powers Bill 2016, clause 86
[69] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207

The chilling effect of ICRs

Evidently, the proposal to store the internet records of every UK web user, with unwarranted access by police and bulk access by the Agencies, is an unprecedented breach of the right to privacy.

Lord Paddick described a powerful example of the ways in which people might use the internet for deeply private matters, for example concerning sexuality, and considered whether people will refrain from seeking confidential advice on the internet in the knowledge that their every online move is being recorded. Privacy is a prerequisite for free personal development, and is essential online where many people now socialise, learn, research and create. The sense of being watched online is certain to have a chilling effect on individuals' freedom, denying not only the personal rights of every citizen but hampering the freedom, education and growth of our society as a whole.

We urge parliamentarians to reject the unnecessary power to generate and retain internet connection records.

Request filter

Amendments

Page 50, line 14, leave out Clause 63

Page 51, line 7, leave out Clause 64

Page 51, line 34, leave out Clause 65

Effect

These amendments would remove provisions for the establishment and use of a filter to gather communications data.

Briefing

The Bill contains provisions for a communications data 'Request Filter'[70] – 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 currently required to build and hold. However, the legality of bulk communications data storage is contested and is currently being challenged in the CJEU by David Davis MP and Tom Watson MP.

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*",[71] which significantly positions the Government at the centre of the data retention and disclosure regime.

Access to the Filter, and the data it produces, would be subject to the same self-authorisation process as all communications data. In practice, the 'Request Filter' would be a search engine over a "*federated database*"[72] 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.

The Government is keen to portray the Request Filter as a 'safeguard' that "*will minimise the interference with the right to privacy".*[73] However, the processing of personal data represents

[70] Investigatory Powers Bill 2016, clause 58
[71] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[72] Ibid.
[73] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23

a significant privacy intrusion. The Joint Committee on the draft Investigatory Powers Bill noted "*the privacy risks inherent in any system which facilitates access to large amounts of data in this manner".*[74] Whilst a useful tool for complex data searches, the 'Request Filter' cannot be viewed as a straightforward safeguard; Lord Strasburger has described it as "*a classic wolf in sheep's clothing".* Rather it is a portal with power to easily assemble a comprehensive picture of each of our lives. In the House of Lords' Second Reading of the Bill, Lord Lucas remarked:

> "*We are producing a resource there that Francis Urquhart would have loved to have his fingers on: absolute knowledge of everyone's private life".*

It raises many of the same concerns as a large and centralised store, with added security concerns of protecting multiple distributed databases. Lord Paddick said that the Filter,

> *"conjures up the spectre of a virtual national database, where government can bring together every piece of available personal data held on an individual into one place".*

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.[75] The ability to conduct complex queries over bulk data is a remarkable extension of power and capability at a time when the necessity and lawfulness of bulk data storage is in question. We urge peers to reject the provision for a Request Filter – a tool which in any view is not 'necessary', and which unacceptably widens the profiling capabilities of the police and other public authorities.

[74] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 247
[75] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin).

Protecting encryption

Amendments

Clause 226, page 175, line 8, leave out paragraph (c)

Clause 228, page 176, line 20, leave out subsection (4)

Clause 228, page 176, line 20, insert new subsection (4A) –

(4A) A notice under section 225 or 226 may not impose obligations on a relevant operator relating to the removal of electronic protection.

Effect

These amendments would delete reference to 'obligations relating to the removal by a relevant operator of electronic protection', thereby removing the explicit provision to force operators to remove encryption from their services.

Briefing

Clauses 225 and 226 have proved to be among the most controversial clauses in the Bill, and some of the most concerning for telecommunications companies and the tech sector both within the UK and abroad. The Intelligence and Security Committee acknowledged communications service providers':

"*serious concern as to this seemingly open-ended and unconstrained power*".

Technical capability notices provide the Government with a blank-cheque power to force telecommunications operators to comply with 'any applicable obligations specified in the notice'. The recipient of such a notice must comply with it but must not disclose the existence or contents of it. It is understood that the main purpose of this clause is to require telecommunications providers to remove encryption from their services. Thus, were an Apple v FBI scenario to occur in the UK, Apple would not be able to disclose even the fact that it had been served with a notice, let alone challenge it in court.

The proposal to force telecommunications operators 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. With use of these notices, communications providers can be prevented from offering services that genuinely offer users a private conversation – although the product may claim to do so. By any rational assessment, this cannot be considered a necessary or proportionate measure. Nor does it achieve any legitimate ends that cannot be achieved

through the array of targeted surveillance methods at the hands of the security and intelligence agencies. 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 (…) only after properly authorised requests".*

This should be a tightly regulated power subject to judicial authorisation, and exercised only in the interests of investigating serious crimes.

The power to force a company to remove encryption from a whole service is especially disproportionate given the security implications. When encryption is removed, communications are much more easily accessed and by third parties – not only domestic authorities, but hostile States and criminal elements. Given the security and economic reliance placed on encryption in our society, Liberty believes that this clause should be removed altogether and that alternative, targeted powers should be used.

In the House of Commons the Solicitor General stated that *""Following further engagement with industry, we have taken steps to address further concerns, and so amendment 86 will make it clear that national security notices cannot require companies to remove encryption"*. However, that amendment does not in fact have that effect and NSN can still require operators to take "to take such specified steps as the Secretary of State considers necessary in the interests of national security." Moreover, obligations to remove electronic protection can explicitly be issued in a 'technical capability notice' from the Secretary of State.[76]

We concur with Baroness Chalker's assessment in the Second Reading of the Bill in the House of Lords:

> *"We should not state in the Bill anything which might be construed as requiring a company to weaken or to defeat its security measures, which are a critical component of efforts to protect users from hackers and from other threats".*

Since the Solicitor General wishes to make clear that notices cannot require companies to remove encryption, the amendments we have suggested above should be adopted to fulfil the promise that amendment 86 failed to.

[76] Investigatory Powers Bill 2016, clause 226, subsection (5)

IMPROVE TRANSPARENCY

Post-notification following surveillance

New Clause.

Notification

(1) The Investigatory Powers Commissioner is to notify the subject or subjects of investigatory powers relating to the statutory functions identified in section 196, subsections (1), (2) and (3), including –

a. the interception or examination of communications,

b. the retention, accessing or examination of communications data or secondary data,

c. equipment interference,

d. access or examination of data retrieved from a bulk personal dataset,

e. covert human intelligence sources,

f. entry or interference with property.

(2) The Investigatory Powers Commissioner must only notify subjects of investigatory powers under subsection (1) upon completion of the relevant conduct or the cancellation of the authorisation or warrant.

(3) The notification under subsection (1) must be sent by writing within thirty days of the completion of the relevant conduct or cancellation of the authorisation or warrant.

(4) The Investigatory Powers Commissioner must issue the notification under subsection (1) in writing, including details of –

a. the conduct that has taken place, and

b. the provisions under which the conduct has taken place, and

c. any known errors that took place within the course of the conduct.

(5) The Investigatory Powers Commissioner may postpone the notification under subsection (1) beyond the time limit under subsection (3) if the Commissioner assesses that notification may defeat the purposes of an on-going serious crime or national

security operation or investigation, or where there is reasonable suspicion that the subject or subjects have committed or are likely to commit a serious criminal offence.

(6) The Investigatory Powers Commissioner must consult with the person to whom the warrant is addressed in order to fulfil an assessment under subsection (5).

Effect

These amendments would provide for a process of post-notification following an investigatory powers operation.

Briefing

In order to ensure accountability for investigatory powers, Liberty believes that the body charged with oversight of investigatory powers should be under a mandatory statutory duty to notify those subjected to surveillance once a particular operation or investigation has ended or once reasonable suspicion of the subject/s has subsided. At present, unlawful surveillance only comes to light as a result of a chance leak, whistleblowing or public interest litigation. This is deeply unsatisfactory.

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

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

In *Zakharov v Russia* the EctHR found 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.

Post-notification is particularly important and urgent given the recent judgment handed down by Investigatory Powers Tribunal in the Human Rights Watch and Others case in which the

[77] Weber and Saravia v Germany, 2006, application 54934/2000, paragraph 135.

Tribunal introduced a new hurdle for IPT applicants.[78] Those wishing to apply to the Tribunal now have to show that "due to their personal situation, [they are] personally at risk of being subject to such [investigatory powers] measures". In this case, the Tribunal found that six NGO claimants could demonstrate that they were at risk of being subject to such measures but that more than 600 private individuals could not.

[78] [2016] UKIPTrib15_165-CH available at - http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

Whistle-blower protections

Amendments

Interception disclosures

Clause 56, page 44, line 33, at end insert –

"(4) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest."

Effect

This amendment would provide a defence to the criminal offence of disclosure in relation to a warrant issued under Part 2. The offence includes disclosure of the existence and content of a warrant as well as disclosure as to steps taken to implement one. The offence is subject to a maximum penalty of five years imprisonment.

Disclosures regarding the obtaining of communications data

Clause 78, page 62, line 3, at end insert –

" (4) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest."

Effect

This amendment would provide a defence to the criminal offence of disclosure in relation to a notice issued under Part 3. The offence includes the disclosure of the existence of a notice. The offence is subject to a maximum penalty of two years imprisonment.

Disclosures regarding the retention of communications data

Clause 89, page 68, line 33, at end insert –

(4A) Subsections (2) and (3) do not apply to a disclosure made in the public interest

Effect

This amendment would balance the duty not to disclose the existence or contents of a retention notice with the responsibility to act in the public interest.

Equipment interference disclosures

Clause 125, page 100, line 6, at end insert –

(4A) In proceedings against any person for an offence under this section in respect of any disclosure, it is a defence for the person to show that the disclosure was in the public interest

Effect

This amendment would provide a defence to the criminal offence of unauthorised disclosure in relation to a warrant issued under Part 5. The offence includes disclosure of the existence and content of a warrant as well as disclosure as to steps taken to implement one. The offence is subject to a maximum penalty of five years imprisonment.

Establish an independent oversight Commission

Amendments

Clause 203, page 155, line 22, insert new clause -

(2A) There shall be a body corporate known as the Investigatory Powers Commission. The Investigatory Powers Commission shall have such powers and duties as shall be specified in this Act.

Clause 203, page 156, line 11, at end insert—

"(c) to the Investigatory Powers Commission are to be read as appropriate to refer to the body corporate, the Investigatory Powers Commission, and in so far as it will refer to the conduct of powers, duties and functions, those shall be conducted by either the Judicial Commissioners or the Inspectors as determined by this Act or by the Investigatory Powers Commissioner, consistent with the provisions of this Act."

Effect

The purpose of these amendments is to replace the proposal to create an Investigatory Powers Commissioner with provisions to create a new Investigatory Powers Commission.

These amendments would provide for the creation of a separate oversight body, the Investigatory Powers Commission, as recommended by the Government's Reviewer of Terrorism Legislation, David Anderson QC in his report *A Question of Trust*. The oversight functions currently residing with Judicial Commissioners, who authorise warrants, should instead be placed with an Investigatory Powers Commission.

Briefing

The Bill proposes that the Investigatory Powers Commissioner (IPC) will replace the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (ISCom). Their roles would be divested in the newly created Investigatory Powers Commissioner and fellow Judicial Commissioners, who would therefore have dual responsibility (a) for reviewing surveillance warrants issued by the Secretary of State and law enforcement chiefs and (b) for post-facto 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 Prime

Minister, and must make an annual report to the PM about the carrying out of the functions of the Judicial Commissioners.

The Home Office has thus far refused to establish an independent Investigatory Powers Commission as a statutory oversight body despite recommendations, based on extensive evidence, from the Joint Committee and the Government's Reviewer of Terrorism Legislation, David Anderson QC. Instead, it has retained its own proposal for a team of Judicial Commissioners, appointed by the Prime Minister, funded by the Home Secretary, to both authorise *and* oversee the use of investigatory powers.

This approach 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 confusion and a conflict of interest.

Liberty supports the consolidation of the byzantine model of surveillance oversight currently provided by several commissioners. However, we believe that a new commission specifically tasked with oversight functions should be established, as per David Anderson's recommendation.

Oversight arrangements: funding

Amendment

Clause 213, page 165, line 25, leave out 'The Secretary of State must' and insert 'The Treasury must'

Clause 213, page 165, line 26, leave out 'and subject to the approval of the Treasury'

Clause 213, page 165, line 27, at end insert 'funds to cover -'

Clause 213, page 165, line 30, leave out 'Secretary of State' and insert 'Treasury'.

Effect

These amendments would remove the role of the Secretary of State in determining the funding, staff and facilities to be afforded to the Judicial Commissioners, leaving this to the Treasury and the IPC.

Briefing

In order for judicial bodies to fulfil their function fully and independently, they must be adequately funded and they must not be dependent on those they purport to scrutinise for this funding. It is therefore inappropriate that, as drafted, the Bill allows the Secretary of State the power to determine funding of the Investigatory Powers Commissioner and Judicial Commissioners. These amendments would remove the power of the Secretary of State to determine the funding, staff and facilities of the Investigatory Powers Commissioner and other Judicial Commissioners. Instead, it will be for the Commissioner to consult with the Treasury to determine funding.

Establish the Privacy and Civil Liberties Board

New Clause

Tabled by Baroness Hamwee and Lord Paddick

"**Privacy and Civil Liberties Board**

The Secretary of State must make and bring into force regulation under section 46 of the Counter-Terrorism and Security Act 2015 (privacy and civil liberties board) prior to the day on which section 2 comes into force."

Effect

This new clause would trigger the establishment of the Privacy and Civil Liberties Board, which was provided for in the Counter-Terrorism and Security Act 2015 but has yet to be established.

This would significantly enhance the oversight of surveillance in the UK, helping to promote human rights compliant practice.