LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's briefing on the Investigatory Powers Bill for Report Stage in the House of Commons

June 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 for Report Stage of the Investigatory Powers Bill.

This briefing sets out the following proposals:

- To improve the quality of investigatory powers warrants by
    - Providing for merits-based judicial authorisation of all powers
    - Providing for single-stage judicial authorisation
    - 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.
- To protect the confidentiality of MPs' correspondence
- To remove or amend overly broad powers by
    - Deleting provisions for internet connection records
    - Adding safeguards to equipment interference (hacking) powers
    - Deleting provisions that allow blanket interception of immigration detention facilities
    - Deleting provisions for broad "national security" and "technical capability" notices
- 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 whistleblowers.

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. Additionally, whilst David Davis MP and Tom Watson MP's legal challenge to DRIPA is ongoing, amendments to the substance of the communications data retention regime proposed in the Bill are not presented here – the European Court of Justice will hand down further judgment on this issue in due course. The Advocate General's Opinion is due on 19 July 2016.

A review of the necessity of bulk powers

Liberty gives cautious welcome to the review, but believes it is vital that it is conducted by an independent assessor with adequate time, resources, and legal and technical expertise if the report is to provide a valuable contribution to the debate. Our recommendations for the review are as follows:

1. The review must answer a two-part question:

(a) whether information gathered through the use of bulk powers was the critical factor in preventing or detecting a specific serious crime; and
(b) whether that information could have been obtained via other, targeted, investigative and police powers.
Only answering 'yes' for (a) and 'no' for (b) can show the practical necessity of these mass-snooping powers to detecting and preventing serious crime.
In answering (a), the Agencies should be required to point to a successful conviction – while (b) can only be suitably answered by considering every other non-bulk or targeted power available to the Agencies and police.

2. The review must be completely independent, and reviewers should harbour no pre-existing bias on the necessity of bulk powers. In answering the principle question above, the review will need to request all available evidence and examine it from both a technical and legal perspective.

Although David Anderson's review A Question of Trust was not tasked with investigating the effectiveness and necessity of bulk powers per se, Liberty was concerned at the way in which it appeared to accept several vague and contradictory case studies proffered by the Agencies as evidence of the claimed necessity of the bulk powers. It would be woefully inadequate for this review to accept case studies at face value. The technical necessity of bulk powers must be interrogated alongside an inspection of more proportional alternatives.

3. A thorough review cannot focus only on the claimed successes of bulk power use, but must inspect evidence of their failures – such as producing intelligence of little value, or inadequate processing of the algorithms used to acquire information.

4. A rigorous inquiry needs to pick apart the breadth of what "bulk interception" currently entails, and which, if any, of those aspects are strictly "necessary".

5. The review must verify the necessity of all bulk powers contained in the Bill – bulk hacking, bulk personal datasets, bulk interception and bulk acquisition of communications data. This will clearly not be possible in the suggested time frame.

6. The reviewers should also have diverse expertise in the relevant fields. The review can only be credible if they are capable of challenging and examining highly complex, technical evidence.

7. Any review will be insufficient unless those conducting it are able to access all the relevant classified information or systems in order to independently investigate and inform their findings.

8. The reviewers must be given adequate time to complete their report – and should explicitly note its limitations if they are not.

9. The reviewers would do well to draw on the methodology of the Privacy and Civil Liberties Oversight Board's report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act in the United States.
The Board examined classified evidence and were given demonstrations of the programs and capabilities in operation, while also engaging with public forums and expert panels on technological, policy and legal issues.

Liberty has shared these recommendations with David Anderson and we sincerely hope this opportunity to properly challenge the evidence and produce a thorough, comprehensive and unbiased examination of the necessity of all bulk powers in the Investigatory Powers Bill is used to its greatest potential. The stakes are extremely high.

IMPROVING WARRANTS

Judicial authorisation

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

Amendments 208, 209, 210, 211

Tabled by Mr David Davis, Andy Burnham, Keir Starmer, Lyn Brown, Jack Dromey, Sarah Champion, Sue Hayman, Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Targeted Interception

> Clause 21, page 17, line 4, leave out "review the person's conclusions as to the following matters" and insert "determine" (**amendment 208**)
>
> Clause 21, page 17, line 10, leave out subsection (2) (**amendment 209**)

Targeted equipment interference

> Clause 97, page 74, line 40, leave out "review the person's conclusions as to the following matters" and insert "determine" (**amendment 210**)
>
> Clause 97, page 75, line 1, leave out subsection (2) (**amendment 211**)

Effect

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

Briefing

The Government has sought to portray the authorisation process as a "double lock" implying that both the Minister and the judge have a substantive role in issuing warrants. This is highly misleading. The Bill sets out that the judicial review standard should be applied when Judicial Commissioners consider warrants issued by the Secretary of State. In conducting judicial review of Executive decisions the courts apply a varying standard of review that is highly dependent on the context of the matter before it. At one end of the spectrum is a strict "Wednesbury" standard of review which will only interfere with an Executive decision that is manifestly unreasonable. At the other end of the spectrum is a more intense standard of review that will substantively assess the proportionality of the Executive decision.

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.[1] Strasbourg case law is clear on the need for a fully independent body, with sufficient expertise and agency to engage in a review of the evidence put forward to justify a surveillance warrant.

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.

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

Single stage judicial authorisation

Amendments 218-259; New Clause 20

Tabled by Alistair Carmichael

Effect

These amendments would remove the role of the Secretary of State in formally issuing interception warrants and instead require Judicial Commissioners to issue warrants. The New Clause 20 would give the Secretary of State the power to certify warrants relating to defence or foreign policy.

Briefing

The Bill's authorisation process for interception warrants, retains the role of the Secretary of State in issuing warrants and gives Judicial Commissioners a limited role judicially reviewing the Secretary of State's decision to issue. This is inadequate to allow the UK to fulfil its human rights obligations and to provide a 'world leading oversight regime'. The JC powers are so circumscribed that the Bill risks creating the illusion of judicial control over surveillance while achieving little change from the status quo. Parliamentarians who would like to see a substantive role for the judiciary in authorising surveillance warrants should support a straightforward one-stage process that gives the task to a JC and removes Ministers' involvement. Indeed, this was the recommendation of the Government's own Reviewer of Terrorism Legislation, David Anderson, in his report *A Question of Trust*.

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."* He further reported, *"Most intercepting authorities did not mind whether their warrants were issued by the Secretary of State or by a judge, so long as a quick turnaround could be achieved and urgency procedures were in place*".[2]

In recognition of concerns that have been expressed regarding warrants that may have international relations ramifications, Liberty advocates proposed New Clause 20, which would allow the Secretary of State to certify such warrants; or indeed for an amendment to the internal processes in place for MI6 which could require a certain category of warrants to receive internal approval by the Foreign Secretary before the formal authorisation process is

[2] David Anderson QC, A Question of Trust, paragraph 14.54

triggered. However, this should be entirely separate from the system of independent authorisation.

The sheer volume of surveillance 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."*[3] In 2014, the Home Secretary personally authorised 2345 interception and property warrants and renewals i.e. about 10 per working day. Liberty shares the Reviewer's concerns that this may not be the best use of the Home Secretary's time given her responsibility for a huge department of State. Removing primary responsibility from one individual who already bears huge responsibility for policing, immigration and other services, is supported by the reflections of a former Home Secretary, David Blunkett, who has written of his time as Home Secretary *"my whole world was collapsing around me. I was under the most horrendous pressure. I was barely sleeping, and yet I was being asked to sign Government warrants in the middle of the night. My physical and emotional health had cracked."*[4]

Arguments concerning Ministers' democratic or political accountability for surveillance warrants 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 49 and similar provisions in the Bill.[6]

A corollary to this argument is that ministers are politically accountable for the Agencies and will be required to resign if things ever go wrong. This is also incorrect. While the Home Secretary is responsible for setting the strategic direction of the Government's counter-terrorism policy and the Cabinet Minister responsible for MI5, MI5 - like the police - is operationally independent. MI5's Director General retains operational independence for day-

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

[5] Paragraph 203GG.
[6] Clauses 49 & 51 of the Bill criminalise the disclosure of the existence of an interception warrant without authorisation to do so.

to-day decision-making. Historically, when terrorist attacks have tragically succeeded, this has not led to political resignations. Despite inquests and inquiries following the 7/7 attacks and the murder of Fusilier Lee Rigby uncovering internal errors in the Agencies' handling of information relating to those responsible for the attacks, this has not resulted in the 'political accountability' now being claimed. In reality, oversight and accountability for Agency activities is instead provided by a patchwork of mechanisms – including public inquiries, the ISC, and legal challenges brought against the Government. Liberty believes there are many ways in which this oversight and accountability could and should be enhanced but it is not correct to argue that political accountability is provided by the ministerial sign off on warrants.

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 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.

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

---

[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 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*.

Require judicial authorisation to obtain communications data

Amendments 320-322, 327

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley and Margaret Ferrier

Clause 53, page 42, leave out lines 14 and 15 and insert –

"(1) A Judicial Commissioner may, on an application made by a designated senior officer at a relevant public authority, issue a communications data access authorisation where the Judicial Commissioner considers – " (**amendment 320**)

Clause 53, page 42, line 21, leave out paragraph (b)(ii) (**amendment 321**)

Clause 53, page 42, line 26, leave out 'The designated senior officer may authorise any officer of the authority to' and insert 'A communications data access authorisation may authorise the designated senior officer or a telecommunications operator to' (**amendment 322**)

Clause 55, page 45, line 16, leave out paragraph (a) (**amendment 327**)

Amendment 323

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 53, page 42, line 39, leave out "authorised officer" and insert "designated senior officer" (**amendment 323**)

Effect

These amendments provide that in order to access communications data, a relevant public authority must seek a warrant from a Judicial Commissioner rather than undertake a system of internal authorisation.

Briefing

Case law is clear that access to communications data must be authorised by a truly independent administrative or judicial body, and the current provisions do not provide for this.

It is entirely unacceptable for public authorities to be able to self-authorise access to revealing personal data. A series of police surveillance scandals, from the unlawful

surveillance of journalists' communications data to extremely disproportionate undercover policing of victims and campaigners, demonstrates the fatal problems of internal authorisation as currently permitted for number of investigatory powers. Judicial authorisation for access to this highly revealing information is a vital safeguard, and one clearly required by the relevant case law.

Require judicial authorisation for retention of communications data

Amendments 328-330, 332-348, 350, 470-1

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 78, page 61, line 5, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 328**)

Clause 78, page 61, line 5, after second "notice" insert "on an application made by a designated senior officer at a relevant public authority" (**amendment 329**)

Clause 78, page 61, line 7, leave out "Secretary of State" and insert "Judicial Commissioner" (**amendment 330**)

Clause 78, page 61, line 38, leave out 'Secretary of State' and insert 'Judicial Commissioner'. (**amendment 332**)

Clause 79, page 62, line 26, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 333**)

Clause 79, page 62, line 35, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 334**)

Clause 80, page 62, line 37, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 335**)

Clause 80, page 62, line 40, leave out "Secretary of State' and insert 'Judicial Commissioner' on both occasions (**amendment 336)**

Clause 80, page 63, line 7, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 337**)

Clause 80, page 63, line 8, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 338**)

Clause 80, page 63, line 9, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 339**

Clause 80, page 63, line 10, leave out 'Secretary of State' and insert 'Judicial Commissioner' (**amendment 340**)

Clause 80, page 63, line 19, leave out ‘Secretary of State’ and insert “designated senior officer at a relevant public authority” (**amendment 341**)

Clause 80, page 63, line 24, leave out ‘Secretary of State’ and insert “designated senior officer at a relevant public authority” (**amendment 342**)

Clause, 80, page 63, line 25, leave out ‘Secretary of State and insert “Judicial Commissioner” (**amendment 343**)

Clause 83, page 64, line 13, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 344**)

Clause 83, page 64, line 14, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 345**)

Clause 83, page 64, line 15, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 346**)

Clause 83, page 64, line 23, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 347**)

Clause 83, page 64, line 38, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 348**)

Clause 83, page 64, line 40, leave out “Secretary of State” and insert ‘Judicial Commissioner’ (**amendment 350**)

Clause, 80, page 63, line 31, leave out ‘Secretary of State and insert “Judicial Commissioner” (**amendment 470**)

Clause, 80, page 63, line 33, leave out ‘Secretary of State and insert “Judicial Commissioner” (**amendment 471**)

Effect

These amendments provide that in order to access communications data, a relevant public authority must apply for an authorisation from a Judicial Commissioner rather than undertake a system of internal authorisation.

Briefing

Communications data is currently retained by telecommunications operators for business purposes and in addition where they are required to do so under a data retention notice

issued by the Secretary of State. The Secretary of State currently serves bulk communications data retention notices to telecommunications operators. We believe that communications data retention should be targeted and initiated only as part of a criminal investigation, and that retention notices for those individuals' data should be authorised by a Judicial Commissioner. A similar system of targeted data retention is used in the U.S., and judicial authorisation of such notices is clearly required by the relevant case law.

Remove power for numerous public officials to request hacking warrants and limit the power to senior law enforcement officials subject to judicial authorisation.

Amendments 364-376, 378-9, 381, 383

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 96, page 72, line 37, leave out 'law enforcement chief described in Part 1 or 2 of the table in Schedule 6' and insert 'Judicial Commissioner' (**amendment 364**)

Clause 96, page 72, line 38, leave out 'person who is an appropriate law enforcement officer in relation to the chief' and insert 'law enforcement chief described in Part 1 of the table in Schedule 6' (**amendment 365**)

Clause 96, page 72, line 41, leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 366**)

Clause 96, page 73, line 1, leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 367**)

Clause 96, page 73, line 4, leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 368**)

Clause 96, page 73, line 7, leave out paragraph (d) (**amendment 369**)

Clause 96, page 73, line 10, leave out 'law enforcement chief described in Part 1 of the table in Schedule 6' and insert 'Judicial Commissioner' (**amendment 370**)

Clause 96, page 73, line 11 leave out 'person who is an appropriate law enforcement officer in relation to the chief' and insert 'law enforcement chief described in Part 1 of the table in Schedule 6' (**amendment 371**)

Clause 96, page 73, line 13 leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 372**)

Clause 96, page 73, line 17, leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 373**)

Clause 96, page 73, line 20, leave out 'law enforcement chief' and insert 'Judicial Commissioner' (**amendment 374**)

Clause 96, page 73, line 23, leave out paragraph (d) (**amendment 375**)

Clause 96, page 73, line 26, leave out subsection (3) (**amendment 376**)

Clause 96, page 73, line 38, after 'Where' insert 'an application for an equipment interference warrant is made by a law enforcement chief and' (**amendment 378**)

Clause 96, page 73, line 42, leave out subsections (6) – (10) (**amendment 379**)

Clause 96, page 74, line 18, leave out subsections (12) and (13) (**amendment 381**)

Schedule 6, page 214, line 7, leave out Part 2 (consequential amendment) (**amendment 383**)

Amendment 377

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier.

Clause 96, page 73, line 32, leave out paragraphs (b) and (c) (**amendment 377)**

Effect

This set of amendments would remove the new and anomalous power for law enforcement chiefs to issue equipment interference warrants on application from law enforcement officers. It would replace this power with the power for Judicial Commissioners to issue equipment interference warrants on application from law enforcement chiefs e.g. chief constables and other senior police as listed in Part 1, Schedule 6 of the Bill. It would remove altogether the power to issue equipment interference warrants from other officers listed in Part 2, Schedule 6, such as immigration officers, officers of Revenue and Customs, Customs officials the Chair of the Competition and Markets Authority and the Police Investigations & Review Commissioner.

Briefing

It is a disturbing anomaly that this Bill proposes that (a) junior ranking officers in a range of public bodies should have the power to apply for authorisation to conduct the most intrusive form of surveillance and (b) that warrants should be authorised by officers at the same public body with only limited oversight provided by judicial review of judicial commissioners. This process would allow thousands of public authority workers to apply for hacking warrants and put a range of actors from chief constables to immigration officers in charge of issuing hacking warrants giving them greater powers of intrusion than the security services who are at least required to apply to the Secretary of State for the issuing of hacking warrants. For countless obvious reasons it is important that the process for authorisation is much more

tightly ring-fenced and made independent. In the wake of the Hillsborough inquests, it would be absurd for Parliament to grant the police such unchecked and potentially abusive powers. The best model for ensuring that equipment interference warrants are only sought where strictly necessary is to restrict applications to law enforcement officers of appropriate seniority and to put the issuing (or rejection) of applications firmly in the hands of the Judicial Commissioner.

Reasonable suspicion

Amendments 313, 325, 331, and 360 to require reasonable suspicion of a serious crime

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael.

Targeted interception

Clause 18, page 14, line 24, insert new clause 2A –

"3A - A warrant may be considered necessary as mentioned in subsection (2)(b) and (3) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed." (**amendment 313**)

Communications data acquisition

Clause 53, page 44, line 13, at end insert –

"(7A) An authorisation may be considered necessary as mentioned in subsection (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." (**amendment 325**)

Communications data retention

Clause 78, page 61, line 10, at end insert –

"(1A) A notice may be considered necessary only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed in relation to the grounds falling within section 53(7)" (**amendment 331**)

Equipment interference

Clause 91, page 70, line 11,at end insert–

"(5A) A warrant may be considered necessary only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed in relation to the grounds falling within this section." (**amendment 360**)

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.

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.

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 suspicion. A requirement of reasonable suspicion, when the purpose of preventing and detecting serious crime is invoked, would prevent the abusive surveillance of campaigners, unionists and victims by undercover police; police surveillance of journalists' lawful activity; and the Agencies' surveillance of law-abiding NGOs and MPs that we have seen in the recent past. However, the threshold would allow for authorisation of powers for serious and violent crimes.

We can envisage careful extensions to amendments 325 and 331 to widen the ability to retain and access communications data – for example, where there is reasonable suspicion that an offence has been committed under Section 111 of the Protection of Freedoms Act 2012 or the Protection from Harassment Act 1997, or where the material sought is necessary on the grounds in 53(7)(g).This would enable communications data to be sought in relation to stalkers, until stalking is classified as a serious crime, and missing persons/where there is a risk of death or injury.

The current framework is inferior to the 'probable cause' standard in the U.S., which is set to frustrate efforts for improved international data sharing arrangements. The U.S. Department of Justice recently recognised that a threshold of reasonable suspicion would be necessary for productive government-to-government engagement on cross-border data sharing[11]. For 'world-leading' legislation resistant to abuse, a reasonable suspicion threshold must be required for the powers in the Bill.

The 'reasonable suspicion' threshold was recently held to be necessary by the European Court of Human Rights in a case concerning the Russian interception regime. In *Roman Zakharov v Russia* the Court said:

> *Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of a reasonable suspicion against the*

[11] Rep. Lofgren expressed concern in a House Judiciary Committee hearing (*International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests* on 25 Feb 2016) about the UK not having a judicial authorisation or a "probable cause" standard. David Bitkower, the Principal Deputy Assistant Attorney General, stated the DoJ does not consider the UK standards acceptable and said the DoJ was still working with the UK on this.

person concerned, in particular whether there are factual indications for suspecting that person of planning, committing, or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security.[12]

We urge parliamentarians to support this amendment to ensure that the UK's investigatory powers regime meets international human rights standards.

[12] At paragraph 260.

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.

The creation of thematic warrants in the Bill provides for open-ended warrants that could encompass many hundreds or thousands of people, and represents a huge departure from the position at common law which has long banned "general warrants". The expansive scope of these warrants, combined with the broad grounds for which they can be authorised, do not impose sufficient limits on the authorities' interception powers.

The ISC reported that the Interception of Communications Commissioner has "*made some strong recommendations about the management of thematic warrants*" and has in some cases recommended that they are cancelled.[13] The ISC has expressed further *"concerns as to the extent that this capability is used and the associated safeguards. Thematic warrants must be used sparingly and should be authorised for a shorter timescale than a standard 8(1) warrant".*[14] Reporting on the draft Investigatory Powers Bill, the ISC noted that "*unfortunately",* its previous recommendation *"has not been reflected in the draft Bill"*;[15] nor has it been reflected in the revised Bill, in which the scope for thematic warrants remains unchanged. The Joint Committee also 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".*[16]

[13] *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 45.
[14] Ibid, page 24 recommendation D
[15] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J(vii).
[16] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, recommendation 38, para. 468

Targeted Interception

Amendments 131 and 132

Tabled by Harriet Harman, Fiona Bruce, Karen Buck, Jeremy Lefroy, Amanda Solloway, Joanna Cherry and Gavin Newlands:

> Clause 15, Page 12, line 8, insert after activity 'where each person is named or specifically identified using a unique identifier' (**amendment 131**)
>
> Clause 15, page 12, line 11, insert after 'operation' 'where each person is named or specifically identified using a unique identifier' (**amendment 132**)

Amendments 267, 268, 307-311

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

> Clause 15, page 12, line 3, after 'person' leave out 'or organisation' (**amendment 267**)
>
> Clause 15, Page 12, line 9, after 'person' leave out 'or organisation' (**amendment 268**)
>
> Clause 27, page 21, line 7, leave out 'or organisation' (**amendment 307**)
>
> Clause 27, page 21, line 8, leave out 'or organisation' (**amendment 308**)
>
> Clause 27, page 21, line 13, leave out 'or describe as many of those persons as is reasonably practicable to name or describe' and insert 'or specifically identify all of those persons using unique identifiers' (**amendment 309**)
>
> Clause 27, page 21, line 15, after 'person' leave out 'or organisation' (**amendment 310**)
>
> Clause 27, page 21, line 19, 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 'all of those persons or sets of premises.' (**amendment 311**)

Amendments 272 and 306

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley and Margaret Ferrier

Clause 15, page 12, line 12, leave out paragraph (c) (**amendment 272**)

Clause 15, page 12, line 13, leave out subsection (3) (**amendment 306**)

Effect

As drafted, clause 15 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 27 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[17] where the ECtHR found Russia's interception scheme in violation of Article 8 of the Convention, the Court cited the fact that Russian "*courts sometimes grant interception authorisations which do not mention a specific person or telephone number to be tapped, but authorise interception of all telephone communications in the area where a criminal offence has been committed."* [18] Thematic warrants are sufficiently broad to violate Article 8 and need considerable amendment on the face of the Bill.

Equipment Interference

Amendments 178, 180, 183, 184 and 187

Tabled by Stephen McPartland, Joanna Cherry, Gavin Newlands, Alistair Carmichael and Steve Baker:

Clause 90, page 68, line 24, leave out subsection (1)(b) (**amendment 178**)

Clause 90, page 68, line 33, leave out subsection (1)(f) (**amendment 180**)

[17] (47143/06) 4 December 2015.
[18] Paragraph 265.

Clause 101, page 78, leave out lines 21 to 27 (**amendment 183**)

Clause 101, page 79, leave out lines 3 to 7 (**amendment 184**)

Clause 90, page 68, line 41, 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." (**amendment 187**)

Amendments 181, 182, 185 and 186

Tabled by Stephen McPartland, Joanna Cherry, Gavin Newlands and Steve Baker:

Clause 90, page 68, line 35, leave out subsection (1)(g) (**amendment 181**)

Clause 90, page 68, line 38, leave out subsection (1)(h) (**amendment 182**)

Clause 101, page 79, leave out lines 8-12 (**amendment 185**)

Clause 101, page 79, leave out lines 13-18 (**amendment 186 –** *tabling error lists lines as 14-9*)

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 90 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 that, "*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'".[19]

In addition, the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest".[20] 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. IMSI catchers can for example pick up stored content of all mobile phones in a particular area. If use of the capability is to stand a chance of meeting the UK's human rights obligations, it is even more imperative that the legal framework for hacking requires specificity of targets.

Equipment Interference Examination Warrants

Amendment 188

Tabled by Stephen McPartland, Joanna Cherry, Gavin Newlands, Alistair Carmichael and Steve Baker:

> Clause 90, page 69, line 4, 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." (**amendment 188**)

Amendments 352, 356 and 357

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael:

> Clause 90, page 68, line 44, leave out paragraph (b) (**amendment 352**)

[19] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; para. 14.
[20] *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 101, page 79, line 37, leave out lines 37-44 (**amendment 356**)

Clause 101, page 80, line 11, leave out lines 8-12 (**amendment 357**)

Amendments 353 and 354

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley and Margaret Ferrier:

Clause 90, page 69, line 1, leave out paragraph (d) (**amendment 353**)

Clause 90, page 69, line 3, leave out paragraph (e) (**amendment 354**)

Effect

These amendments would ensure that all targets of hacking are properly named or specifically identified, and refine the matters to which targeted examination warrants may relate 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 496

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley and Margaret Ferrier

Page 177, clause 225, line 27, at end 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 (**amendment 496**)

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 a discretion so broad as to be arbitrary. Furthermore, the Courts have responded with considerable deference to Government claims of 'national security', viewing them not as a matter of law, but as executive led policy judgements.[21] National security as a legal test is therefore meaningless if left without a statutory definition.

The Joint Committee on the draft Bill recommended that the Bill should include definitions of national security[22] and economic well-being[23]; the ISC further recommended that economic well-being should be subsumed within a national security definition, finding it "*unnecessarily*

[21] 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".
[22] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 82
[23] Ibid. Recommendation 83

confusing and complicated".[24] The ISC queried both the Agencies and the Home Office on this point but reported that '*neither have provided any sensible explanation'*.[25] 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 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.*"[26]

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

The definition provided in this amendment is based on the UN's Siracusa Principles.[27] 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.

Again in Roman Zakharov, 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 discretion in determining which events or acts constitute such a threat and whether*

[24] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J (i)
[25] Ibid.
[26] See Hansard, 15 March 2016, http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0002.htm
[27] 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)

that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse".[28]

[28] At paragraph 248.

PROTECT MP's CORRESPONDENCE

Targeted Interception

Amendment 314

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

> Clause 24, page 18, line 39, leave out "Secretary of State' and insert 'Judicial Commissioner' (**amendment 314**)

Amendments 315 and 316

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, and Margaret Ferrier

> Clause 24, page 18, line 41, leave out subsection (b) and insert - "(b) the warrant involves a member of a relevant legislature." (**amendment 315**)
>
> Clause 24, page 19, line 7, 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 indictable offence has been committed
> (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)
> (c) Other proportionate methods of obtaining the material have been tried without success or have not been tried because it appeared that they were bound to fail
> (d) It is in the public interest having regard to the democratic interest in the confidentiality of correspondence with members of a relevant legislature. (**amendment 316**)

Effect

These amendments would ensure that applications for warrants to intercept the communications of elected politicians 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.

Targeted Equipment Interference

Amendments 363 and New Clause 23

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, and Margaret Ferrier

Page 71, line 40, leave out Clause 94 (**amendment 363**)

Clause 94, page 71, leave out clause 94 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 an indictable 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:

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

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

iii. the democratic interest in the confidentiality of correspondence with members of a relevant legislature. (**New Clause 23**)

Effect

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

These amendments would also apply additional safeguards to the correspondence of MPs when a warrant for hacking is sought.

Briefing

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

> *"As Mr Macmillan once said, there can only be complete security with a police state, and perhaps not even then, and there is always a difficult balance between the requirements of democracy in a free society and the requirements of security. With my right hon. Friends, I reviewed the practice when we came to office and decided – on balance – and the arguments were very fine – that the balance should be tipped the other way and that I should give this instruction that there*

was to be no tapping of telephones of Members of Parliament. That was our decision and that is our policy. But if there was any development of a kind which required a change in the general policy, I would, at such moment as seemed compatible with the security of the country, on my own initiative make a statement in the House about it. I am aware of all the considerations which I had to take into account and I felt that it was right to lay down the policy of no tapping of telephones of Members of Parliament."[29]

This protection, extended to correspondence of members of the House of Lords in 1966, was repeated in unequivocal terms by successive Prime Ministers. Tony Blair clarified in 1997 that the policy *"applies in relation to telephone interception and to the use of electronic surveillance by any of the three Security and Intelligence Agencies."*[30]

Despite this clear and unambiguous statement that MPs and Peers would not be placed under electronic surveillance, a recent decision by the Investigatory Powers Tribunal in a case brought by Caroline Lucas MP and Baroness Jenny Jones held that the doctrine had been unilaterally rescinded by the Executive.[31] Liberty disputes the IPT's decision. We believe the unequivocal statement made by Prime Minister Wilson back in 1966 was a constitutional convention protecting vital discourse between the people and their ultimate representatives, creating a legitimate expectation on the part of parliamentarians and their constituents that their correspondence was protected until and unless the Prime Minister informed the House otherwise. However, as there is currently no right of appeal against decisions of the IPT, the only recourse left to parliamentarians seeking to protect their constituent's correspondence is to support amendment to the Bill.

It is inherent to our democracy that elected representatives can correspond in private. As stated by Keir Starmer MP QC during Committee Stage debate of the Bill, *"On the general principles, the first thing to say about journalistic material and communications sent by or*

[29] HC Deb 17 November 1966 Vol 736, columns 634-641.
[30] HC Deb 4 December 1997 Vol 302, Col 321.

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

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."[32]

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. It is difficult to see why Members of Parliament and other elected representatives should have confidence that "consultation" with the Prime Minister can act as a bulwark against unjustified surveillance of constituency communications. 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 only be rebutted in 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 discussion concerning the protection of correspondence with elected representatives in 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 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."*[33]

[32] IP Bill Committee, 12 April 2016, at column 190.
[33] IP Bill Committee Hansard, 21 April 2016, John Hayes MP, at column 402

REMOVING AND AMENDING OVERLY BROAD POWERS

Internet Connection Records

Amendment 3

Tabled by Alistair Carmichael, Joanna Cherry and Gavin Newlands:

> Clause 78, page 62, line 22, leave out "therefore includes, in particular" and insert "does not include" (**amendment 3**)

Effect

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

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. Under current legislation in DRIPA 2014, public telecommunications operators may be required to retain "*relevant communications data"* for up to 12 months[34], including data that may be used to identify the internet protocol (IP) addresses of senders and recipients of communications. However, this specifically excluded the obligation to retain the most revealing data, previously described as 'web logs' but presented here as ICRs, that would explicitly identify the websites or internet communications services users have accessed.[35]

ICRs are described in the Bill as communications data which "*may be used to identify, or assist in identifying, a telecommunications service".*[36] In explanatory notes accompanying the draft Bill, ICRs are described as "*a record of the internet services that a specific device connects to – such as a website or instant messaging application – captured by the company providing access to the internet".*[37] However, the exact fields of information that would constitute an ICR have not been defined.

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

[34] *Data Retention and Investigatory Powers Act 2014,* section 1

[35] *Counter Terrorism and Security Act 2015,* section 21(3)(c)
[36] *Investigatory Powers Bill 2016,* clause 54, subsection (6)(a)
[37] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.29

Gambling Commission, the Food Standards Agency, and several ambulance services.[38] The scale of public authority access to ICRs mirrors that for communications data, barring local authorities who will not be granted access.

Public authorities will not need a warrant to obtain an individual's detailed internet connection records. Applications by law enforcement and public authorities to acquire ICRs relating to suspects will mirror existing provisions for access to communications data and instead be authorised by a 'designated person'[39] within the public authority, and then by a 'single point of contact.'[40]Provisions in the Bill would permit law enforcement and public authorities to gain access to ICRs for four purposes: to identify who or what device has sent a communication or used an internet service; to identify what internet communications services have been used, when and how; to identify when and where a person has accessed or made available illegal material; and now in the revised Bill, the additional power to reveal all internet connections of an identified person.[41]

Defining ICRs

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.

The Bill and accompanying documents have consistently failed to define the exact fields of information that would constitute an 'internet connection record' – indeed, there is nothing on the face of the Bill to limit the potential data fields within ICRs. Rather, the Home Office describes the definition of ICRs as 'flexible'[42], and the draft Code of Practice confirms that 'there is no single set of data that constitutes an internet connection record'.[43] The Home Office's accompanying ICR factsheet says that ICRs "*will involve retention of a destination IP address but can also include a service name (e.g. Facebook or Google) or a web address*

[38] *Investigatory Powers Bill 2016,* schedule 4, part 1
[39] *Investigatory Powers Bill 2016,* clause 53
[40] *Investigatory Powers Bill 2016,* clause 67. A SPoC is an "*accredited*", "*trained*" individual. *Investigatory Powers Bill: Explanatory Notes,* 4 Nov 2015, p. 27
[41] *Investigatory Powers Bill 2016,* clause 54, subsection (4)
[42] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.1
[43] *Communications Data: Draft Code of Practice* – Home Office, 1 March 2016, p.18

(e.g. www.facebook.com or www.google.com) along with a time/date".[44] 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 not only web addresses and IP addresses are included, but the names, addresses, email addresses, phone numbers and billing data of customers; usernames and passwords; locations of internet access and each internet communication; and device identifiers (MAC address, IMSI, IMEI).[45].

"*The voice of the internet industry"*, the Internet Service Providers Association (ISPA) expressed concern that ICRs have not been properly defined.[46] The Joint Committee reported, "*We have concerns about the definitions and feasibility of the existing proposal, which the Home Office must address".*[47] 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.*"[48] The Science and Technology Committee's press release stated, "*The Bill was intended to provide clarity to the industry, but the current draft contains very broad and ambiguous definitions of ICRs, which are confusing communications providers."*[49] However, no further clarity or definition has been provided in the revised Bill or accompanying documents.

In practice, ICRs would provide a detailed record of internet connections for every person in the UK and comprise a 12 month log of websites visited, communications software used, system updates downloaded, desktop widgets used (e.g. calendars, notes), every mobile app used (e.g. Whatsapp, Signal, Google Maps), and logs of any other device connecting to the internet, such as games consoles, baby monitors, digital cameras and e-book readers.

Law enforcement bodies can currently obtain similarly extensive internet connection data for specific surveillance targets in several ways. First, they can request telecommunications operators to retain the data of specific targets on a forward-looking basis[50], 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

[44] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015
[45] *Annex A: Terminology and Definitions* – Home Office, in evidence to the Joint Committee on the draft Investigatory Powers Bill, (IP0146), January 2016, p.6
[46] *Internet industry has major concerns on the Investigatory Powers Bill,* ISPA Conference press release, 19 Nov 2015
[47] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 106
[48] Ibid. Recommendation 7, para. 122
[49] *Press Release: Cost of Investigatory Powers Bill Could Undermine UK Tech Sector* – Science and Technology Committee, 1 February 2016
[50] *Draft Investigatory Powers Bill 2015: Explanatory Notes,* p.25

own business purposes.[51] 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.[52] 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[53]. 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 they have a range of other capabilities which enable them to obtain equivalent data."*[54] The ISC recommended that this be amended in the Bill "*in the interests of transparency*"; yet no such transparency has been provided.

Liberty believes the case supporting this expanded data collection by ISPs, including its claimed benefit to law enforcement, is deeply flawed, contradicted by the available evidence, and has been accurately described as "*overstated and misunderstood*".[55] Further, there is no other known Five Eyes country in which operators have been or are being forced to retain similar internet connection data[56]. 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.[57] As the CJEU ruled in 2014,[58] 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.

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

---

[51] *Operational Case for the Retention of Internet Connection Records,* 2015, p.25
[52] *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
[53] *GCHQ and NCA join forced to ensure no hiding place online for criminals* – NCA, 6 Nov 2015
[54] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation I.
[55] *Written evidence regarding Investigatory Powers Bill* – Adrian Kennard (Andrews & Arnold Ltd.), 25 Nov 2015, http://www.me.uk/IPBill-evidence1.pdf
[56] *A Question of Trust: Report of the Investigatory Powers Review* – David Anderson Q.C., June 2015, p.265
[57] Ibid
[58] *Digital Rights Ireland* (C-293/12) *and Seitlinger and Others* (C-594/12), 8 April 2014

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

The Metropolitan Police and National Crime Agency (NCA) have suggested that without ICRs, they cannot resolve IP addresses (that is, identify web users) and continue investigations in a minority of cases (approximately 14%[59]).

In the *Operational Case for the Retention of Internet Records*, published with the draft Bill, three case studies of discontinued investigations relating to child sexual exploitation and three relating to fraud are presented to support the argument for retaining ICRs. It is claimed that ICR retention would be required in order to progress those investigations and increase chances of accurately identifying a web user.[60] However, the likelihood of bulk ICRs to prove vital in accurately identifying otherwise anonymous suspects of serious crime has been questioned by ISPs and technologists.[61] The justification relies on the assumption that online criminals offend using a regular browser or public file sharing service on their own device, using personal internet connections, without employing the most basic of the widely available anonymity tools to avoid detection. The use of privacy-enhancing and anonymising tools such as Virtual Private Networks (VPNs), which securely 'tunnel' internet connections; Tor, a secure browser that anonymises users' location and identity; and proxy web browsers that bypass filters and anonymise web browsing, is widespread and increasing exponentially. ICRs will be unusable and in fact misleading where such privacy tools have been used. Furthermore, the retention of ICRs will push internet traffic, both legitimate and otherwise, into more protected spaces. This inevitable digital shift will render ICRs an invasive database of, almost exclusively, innocent citizen's digital lives, and forced retention of them a costly, out-dated, ineffective strategy.

In the limited cases where the ICRs might assist in resolving an IP address they will provide limited assistance in identification of suspects as they can only help to identify a device, such as a laptop or PC – not an individual user. Identifying a specific user requires a context of information that would typically be gathered in a targeted surveillance operation. Devices such as laptops, PCs, tablets and even smart phones are commonly shared within families,

[59] It is argued that the retention of ICRs would improve the chances of being able to resolve an IP address in 14% of cases in a sample from the US based National Centre for Missing and Exploited Children, NCMEC - as cited in the ICR evidence base: *Operational Case for the Retention of Internet Connection Records,* 2015, p.14

[60] *Operational Case for the Retention of Internet Connection Records,* 2015, p.20

[61] *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

workplaces and public institutions, further diminishing the value of bulk ICRs in identifying an individual suspect. Indeed, ICR data is "inexact and error-prone".[62]

In evaluating the efficacy of ICRs in serving the purpose of IP resolution and identification of a suspect, we are informed by the case study of Denmark's Data Retention Law (*Logningsbekendtgørelsen*), effective 2007-2014, which required communication service providers to retain internet session logs. Denmark's data retention law compelled telecommunications operators to store internet session data for 12 months including client and server IP addresses, port numbers, transmission protocols and timestamps.[63] The data retention excluded DNS logs (i.e. the names of the websites the server IP addresses corresponded to). **A self-evaluation report published by the Danish Ministry of Justice in December 2012 found that several years of collecting internet session data had not yielded any significant benefits for law enforcement - session data had played a minimal role in only one case.**[64] In fact, Ministry staffers reported that session logging "*caused serious practical problems"* due to the volume and complexity of the data hoarded.[65] In 2013, approximately 3,500 billion telecommunication records were retained in Denmark, averaging 620,000 records per citizen.[66] 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*".[67]

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.[68] Despite the rhetoric of "*important differences"*, there are two differences in substance. Firstly, the UK Government promises (although will not make a statutory commitment) to meet CSPs' costs upfront to cover the necessary infrastructural change, drain on resources, and

---

[62] *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

[63] *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

[64] *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).

[65] Ibid.

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

[67] *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

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

generation and storage of data – whereas in Denmark, CSPs were paid for the generation and storage of data after they implemented infrastructural change. It does not follow that this different mode of reimbursement will affect the usability of data. 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.[69]

Rebuttal to Purpose 2 - identify what ISPs an identified suspect has used, when and how[70], in order to inform law enforcement as to which communications service providers to request further information from.

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

The argument in favour of this new, invasive category of bulk data retention rests, in part, upon the claim that there is an "*extremely high threshold"*[71] and "*very limited circumstances in which the interception of communications content can be authorised*", and therefore targeted interception "*cannot be used in most law enforcement cases".*[72] This is a peculiar argument, as interception is used for three broad statutory purposes: the prevention and detection of serious crime (which accounts for 68% of interception warrants[73]), the interests of national security and for the economic well-being of the UK.[74] The case studies provided

[69] See written and oral evidence to the Joint Committee and the Science and Technology Committee.
[70] *Draft Investigatory Powers Bill 2015,* clause 47 (4)(b)
[71] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[72] *Operational Case for the Retention of Internet Connection Records,* 2015, p.16
[73] *HM Government Transparency Report 2015: Disruptive and Investigatory Powers,* p.34
[74] *Draft Investigatory Powers Bill 2015,* clause 14 (3)

to support the case for ICR retention all qualify as serious crimes[75] for which interception can be used, as they relate to child sex abuse, fraud and human trafficking.

Additionally, it is claimed that law enforcement bodies cannot request data from popular online service providers who store communications data for their own purposes, such as Facebook, without ICR evidence proving that the individual or device in question definitely accessed their service.[76] Without this data, they argue that such a request "*is unlikely to be necessary and proportionate*".[77] Liberty does not recognise this explanation. If the authorities have objective and reasonable grounds for suspecting serious criminality and further believe that the suspect's use of a telecommunications platform may provide evidence of the offence, a request for communications data will be necessary and proportionate.[78] If the suspect did not use the communications service, the data would simply not be there to obtain.

As a third argument for ICR retention, law enforcement bodies say it is "*thanks to seizure of devices*" that it has thus far been possible to identify communications services used by suspects, but that seizure of a device "*will not always be the preferred course of action in an investigation, as it is an overt action that will normally involve an arrest*".[79] Investigators would rather "*develop intelligence on the group covertly*" and establish any possible "*previous linkages"* between group members. However, links between group members can be covertly discovered through a targeted communications data retention order; through requests for retrospective data from the operators who store it for their own purposes; or through interception.

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".*[80] In response,

[75] Serious crimes are those that incur a sentence of 3 years or more; violent crimes; crimes involving substantial financial gain, or conduct by a large number of persons in pursuit of a common purpose. *Draft Investigatory Powers Bill 2015,* clause 195 (1),
[76] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4; p.25
[77] *Operational Case for the Retention of Internet Connection Records,* 2015, p.4
[78] Many online public services are co-operative with law enforcement: Facebook, for example, co-operates with the NCMEC and has an established system for law enforcement data requests[78]. In the period January 2015 – June 2015, UK law enforcement made 3,384 requests to Facebook alone for various types of data, relating to 4,489 accounts; Facebook found legal basis to comply with 78.04% of these requests[78].
[79] *Operational Case for the Retention of Internet Connection Records,* 2015, p.17
[80] *Factsheet*: *Internet Connection Records,* Home Office, 4 Nov 2015

ISPA (Internet Service Providers Association) members *"pointed out the huge flaw in this argument*".[81] 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) often stays connected in the background whether in current use or not, remaining connected for a period of days, weeks or months.[82] Connection records show connection timestamps rather than access timestamps, and one such 'internet connection' could exceed the 12 month retention period by the time it is logged. ISPs and technologists have expressed serious concern that the Home Office has based an extensive, invasive data collection policy on a fundamental misunderstanding, or worse misguidance, as to how internet connections work, and that it has provided misleading descriptions of what purposes ICRs would serve accordingly.

Rebuttal to Purpose 3 - to "identify the accessing of illegal online services or websites"[83].

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

[81] *Home Office Meeting re IPBill* by Adrian Kennard, 25 Nov 2015 – http://www.revk.uk/2015/11/home-office-ipbill.html
[82] 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.
[83] Draft Investigatory Powers Bill 2015, clause 47 (4)(c).

Rebuttal to Purpose 4 – to view any "internet services (websites, apps, etc.) *an individual is using"*

The three purposes described above, provided as the original justification for the collection of ICRs, are now largely unnecessary, as the revised Bill has expanded the police and public authorities' power to access all of an individuals' ICRs[84] – not just those relating to "*internet communication services*" or "*illegal online services"* . This is not only unnecessary, but alarmingly disproportionate. In 2014, there were 517, 236 authorisations for public authorities' access to communications data.[85] 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.

Threat to privacy and 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*".[86]** In their final report, the Joint Committee noted that *"storing web log data, however securely, carries the possible risk that it may be hacked into or may fall accidentally into the wrong hands, and that, if this were to happen, potentially damaging inferences about people's interests or activities could be drawn*".[87] The Joint Committee on the draft Investigatory Powers Bill noted that "*data theft remains an ongoing challenge".*[88] 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,[89] it is extraordinarily irresponsible to coerce private companies with the burden of generating, storing and securing vast swathes of revealing data on the general

[84] Investigatory Powers Bill 2016, clause 54, subsection (4)(d)
[85] *Statistics: Communications Data* – IOCCO, http://www.iocco-uk.info/sections.asp?sectionID=12&type=top, retrieved 10 March 2016
[86] MPs call communications data bill 'honeypot for hackers and criminals' – Alan Travis, The Guardian, 31 Oct 2012.
[87] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, pp.28-29
[88] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Para. 174
[89] 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.

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.[90] 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.[91]

The difficulty of tracking some online criminals is a real problem. However, it is not a problem that mass surveillance programs – least of all this one - can solve. Bulk ICR retention will not be able to meet these three investigative purposes with greater efficacy than the targeted surveillance methods available for investigations; in fact, it could easily cause false suspicion. Arguably, the £175 million budgeted to fund reluctant telecommunications operators to spy on their customers would be better spent on hiring more officers to conduct targeted, warranted surveillance on suspects of serious crime.

[90] Investigatory Powers Bill 2016, clause 86
[91] A Question of Trust: Report of the Investigatory Powers Review – David Anderson Q.C., June 2015, p.207

Adding safeguards to Equipment Interference powers

Powers to conduct equipment interference – or to hack – are new and have not previously existed in legislation. They therefore require significant scrutiny by parliamentarians before they are added to the statute books. By its very nature hacking is an extremely intrusive power, granting authorities the power to see all past and future information and activity on a computer or other device. Beyond the implications for privacy, the potential ramifications for cyber-security of the whole country and fair trials require that hacking is used only as a tool of last resort and stronger protections must be added to the Bill.

Part 5 of the Bill makes provision for targeted hacking, euphemistically termed "*equipment interference*". There are two types of warrant: "targeted equipment interference warrants" and "targeted examination warrants", the latter of which can be issued in relation to material obtained via the bulk hacking powers in Part 6. Secretaries of State (and in certain circumstances Scottish Ministers[92]) can issue both types of warrants to the intelligence agencies and the Chief of Defence Intelligence where he or she considers it necessary and proportionate on the three main grounds. In contrast to the scheme for interception, the power to issue hacking warrants is also extended to chief constables, deputy chief constables, assistant chief constables and senior HMRC officers on application from junior HMRC and police officers 'for the purpose of preventing and detecting serious crime".[93]

A hacking warrant authorises a person to interfere with any equipment for the purpose of obtaining "communications", "equipment data", or "any other information".[94] There are no limits as to what information could be obtained. Information can be obtained by *"monitoring, observing or listening to a person's communications or other activities and recording anything that is monitored, observed or listened to*".[95]

Warrants last for six months and can be renewed potentially indefinitely. Warrant applications will be subject to the weak system of judicial review. Warrants can be modified by ministers without the approval of a JC and modification can include changing the name, descriptions and scope of the warrant.[96] Chief constables are required to have their

[92] Clause 92.

[93] The majority of police forces can only hack devices and networks with a "British Isles connection" (although NCA has global powers) and this requirement is made out if any of the conduct, equipment interfered with or private info sought is in the British Islands.

[94]Equipment data is defined at clause 89.

[95] Clause 88(4).

[96] Investigatory Powers Bill 2016, clause 104

decisions to modify warrants reviewed by a JC, unless they consider the modification to be urgent.[97]

Hacking is potentially much more intrusive and damaging than any other forms of traditional surveillance such as bugging, interception and acquisition of communications data. Hacking can grant access to a large amount of highly sensitive data that has never been communicated or transmitted and can give the hacker access to all historical and future data stored on a device. Uniquely, it also grants the hacker total control over a device – phones and computers can be turned on or off, have their cameras or microphones activated, and files added or deleted. Furthermore, all this can be done without the fact of the hack being known or knowable to the target.

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

[97] Investigatory Powers Bill 2016, clause 106 subsection (3)(b)

Proportionality and technical assessment

Amendments 362, 380, and 386

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 93, page 71, line 35, leave out from "include" to the end of line 36 and insert –

(a) the requirement that 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

(b) the requirement that a "Cyber-Security Impact Assessment" has been conducted by the Investigatory Powers Commissioner's technical advisors with regard to the specific equipment interference proposed, accounting for –

i. the risk of collateral interference and intrusion, and

ii. the risk to the integrity of communications systems and computer networks, and

the risk to public cybersecurity (**amendment 362**)

Clause 96, page 74, line 15, leave out 'whether what is sought to be achieved by the warrant could reasonably be achieved by other means' and insert–

(a) the requirement that 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

(b) the requirement that a "Cyber-Security Impact Assessment" has been conducted by the Investigatory Powers Commissioner's technical advisors with regard to the specific equipment interference proposed, accounting for –

i. the risk of collateral interference and intrusion, and

ii. the risk to the integrity of communications systems and computer networks, and

the risk to public cybersecurity (**amendment 380**)

Clause 101, page 79, line 21, leave out paragraph (b) and insert–

(b) precisely and explicitly the method and extent of the proposed intrusion and measures taken to minimise access to irrelevant and immaterial information, and

(a) in a separate "Cyber-Security Impact Assessment",

i. the risk of collateral interference and intrusion, and

ii. the risk to the integrity of communications systems and computer networks, and

iii. the risk to public cybersecurity,

and how those risks and damage will be eliminated or corrected (**amendment 386**)

Effect

These amendments explicitly require that less intrusive methods have been used or considered, and require a technical assessment of proportionality accounting for the risks of the conduct proposed (amendment 386). These requirements would apply when applications from the the Chief of Defence Intelligence (amendment 362) and law enforcement (amendment 380) are considered.

Briefing

In order to consider whether a warrant is necessary and proportionate, not only will the intrusion need to be assessed but the methods. This requires the Judicial Commissioner, supported by independent technical expertise, to assess the proportionality of the conduct proposed in targeted equipment interference applications.

For example, when malware is deployed, there is often a risk of contagion, both overseas and at home. This was dramatically demonstrated by the Stuxnet virus, believed to be an American-Israeli cyberweapon, which intended to hack a single Iranian uranium enrichment facility but infected energy giant Chevron among many other companies as well as Microsoft PCs around the world. The risks of hacks spreading 'in the wild' cannot be overstated: Professor of Security Engineering at Cambridge University, Ross Anderson wrote to the Science and Technology Select Committee, "*it is only a matter of time before interference with a safety-critical system kills someone"*. The practice of equipment interference leads to the controversial stockpiling of software vulnerabilities which puts millions of users at risk. Practices such as subverting software to deploy malware in fake 'software updates' were once reserved to criminals and fraudsters, but are now practiced by intelligence agencies. It

is vital that the Judicial Commissioner understands and accounts for the proportionality of proposed interference methods before authorising them.

There is also the risk that hacks can malfunction, with severe consequences for critical infrastructures and even international relations. For example, Snowden revealed that NSA hacking malfunctions were responsible for the outage of Syria's internet in 2012, which may have caused simultaneous flight-tracking issues, and led government and opposition forces to erroneously blame each other for the incident. There is a high degree of public interest in the proportionality of hacking methods. For example, the debate surrounding the *Apple v FBI* case centred on whether the methods required to hack one particular device were proportionate given the security consequences for all iPhone owners. In the US, this decision was rightly entrusted to an independent judge. Given the potential damage to computer security and corresponding vulnerability to criminal elements that results from hacking, the use of various hacking technologies poses clear risks to those it is used against and the wider public, requiring the addition of a technical proportionality test.

Duration of EI warrants

Amendment 388

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 102, page 80, line 23, leave out '6' and insert '1' (**amendment 388**)

Effect

This specifies that hacking warrants may only last for one month rather than six.

Briefing

Hacking is a highly intrusive power with great potential to damage cyber security. It should only be used where strictly necessary, where the security and law enforcement agencies are unable to access information in another manner. Granting warrants that last half a year does not create the appropriate environment of robust scrutiny that is required in order to ensure that hacking does not become a routine form of surveillance. Given the rate at which technology changes, assessments by the JC's technological experts (see above) risk being out of date during the course of a long warrant. To protect cyber-security and ensure that the proportionality of hacking is fully understood in each case, warrants must be issued for a shorter period of time.

EI audit trail

New Clause 24

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley and Margaret Ferrier.

> "**Audit trail of equipment interference**
>
> Any conduct authorised under a warrant issued under this Part must be conducted in a verifiable manner, so as to produce a chronological record of documentary evidence detailing the sequence of activities (referred to hereafter as "the audit trail")." (**NC24**)

Effect

This amendment would introduce a requirement that all equipment interference produces a verifiable audit trail. This will be particularly vital to the success and legitimacy of prosecutions. It is recommended that further provision for the independent verification of audit trails is included in Part 8 (Oversight Arrangements).

Briefing

Equipment interference can include any number of methods, many of which empower the hacker to add, delete and alter files and software. Unlike traditional searches, the very practice of equipment interference necessitates interference with items that may later be used as evidence. To protect the integrity of potential evidence and the success of prosecutions, it is vital that all interference produces an independently verifiable audit trail. Furthermore, an audit trail provides a helpful way to oversee the conduct that has taken place and ensure good practice. Similarly, police must keep a log of activity undertaken when conducting traditional property searches. A verifiable audit trail will be particularly vital should certain practices be conducted by telecommunications operators or outsourced to private contractors (as in *Apple v FBI*).

Purposes for which EI warrant granted

Amendments 358, 359, 387, 361

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 91, page 69, line 17, leave out paragraph (d) and insert –

(b) the Judicial Commissioner has reasonable grounds for believing that the material sought is likely to be of substantial value to the investigation or operation to which the warrant relates. (**amendment 358**)

Clause 91, page 70, line 8, after 'crime' insert 'where there is reasonable suspicion that a serious criminal offence has been or is likely to be committed' (**amendment 359**)

Clause 101, page 79, line 23, at end insert –

(c) the basis for the suspicion that the target is connected to a serious crime or a specific threat to national security, and

(d) in declaration with supporting evidence,

(i) the high probability that evidence of the serious crime or specific threat to national security will be obtained by the operation authorised, and

(ii) how all less intrusive methods of obtaining the information sought have been exhausted or would be futile (**amendment 387**)

Clause 91, page 70, line 25, at end insert –

(10) A warrant may only authorise targeted equipment interference or targeted examination as far as the conduct authorised relates –

(a) to the offence as specified under (5)(b), or

(b) to some other indictable offence which is connected with or similar to the offence as specified under (5)(b) (**amendment 361**)

Amendment 382 to ensure warrants are only granted to seek relevant material

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Clause 93, page 71, line 31, leave out subsection (d) and insert –

(d) the Judicial Commissioner has reasonable grounds for believing that the material sought is likely to be of substantial value to the investigation or operation to which the warrant relates (**amendment 382**)

Effect

These amendments would introduce a requirement that warrants are only granted where there are reasonable grounds for believing material to be obtained will be of substantial value to the investigation or operation (amendments 358, 382); that authorised conduct is limited to these ends (amendment 361); and the requirement of a threshold of reasonable suspicion that a serious criminal offence has been committed in order for a warrant to be granted (amendments 359, 387).

Briefing

Hacking can result in a significant amount of information being taken from a device – perhaps all the stored emails; perhaps all the information on an entire server. To prevent fishing expeditions and to reflect current legislative requirements in the *Police and Criminal Evidence Act 1984* for when police searches are conducted under warrants, this amendment would introduce a safeguard that conduct taken under a warrant must relate to the offence on which the warrant was sought.

Blanket interception of immigration detention facilities

Amendment 317

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier, and Alistair Carmichael.

Clause 44, page 34, line 21, leave out clause 44 (**amendment 317**)

Effect

This amendment would delete clause 44 which would permit the creation of additional interception powers in immigration detention facilities.

Briefing

Provisions in clause 44 to permit the creation of additional interception rules in immigration detention facilities appear to be a wholly new extension of current provisions. The powers under the clause permit detention centre rules or rules for short-term holding facilities to authorise conduct to intercept. As identified by Joanna Cherry MP QC during the Committee Stage debate of the Bill, there are grave and repeated concerns about the manner in which powers in rules for detention centres which do exist are currently exercised, and those in immigration detention are individuals who have not been detained by the courts nor granted any legal due process. Given these factors, she commented that it would be "fanciful" to assume that powers exercised under this clause would be lawful.[98]

Liberty has grave concerns about provisions which seek to permit for interception regimes to be established outside the IP Bill, which purports to provide a comprehensive basis for the use of investigatory powers by the state. Even more concerning is that this clause permits this additional regime to be determined via rules and regulations rather than in primary legislation. If the Government considers that there are circumstances in which it wishes to grant additional surveillance powers to those operating within certain institutions there can be no justification for failing to set this out on the face of this Bill, along with vital safeguards for their exercise.

It is wholly inappropriate to ask Parliament to grant a blank cheque for separate and additional interception regimes. This is especially so given the highly sensitive and vulnerable nature of many of those who are likely to be subject to these powers, which includes asylum seekers fleeing persecution by their own state.

[98]Investigatory Powers Bill Public Bill Committee, Hansard, Thursday 14 April 2016, Afternoon session, column 240

Request filter

Amendments 4, 5, 6

Tabled by Alistair Carmichael

Page 46, line 40, leave out Clause 58 (**amendment 4**)

Page 47, line 36, leave out Clause 59 (**amendment 5**)

Page 48, line 16, leave out Clause 60 (**amendment 6**)

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'[99] – a feature previously proposed in almost identical terms in the draft Communications Data Bill. The only change is that the Secretary of State must consult the Investigatory Powers Commissioner "*about the principles on the basis of which the Secretary of State intends to establish"* the filter.[100] The Request Filter is a search mechanism, allowing public authorities to conduct simple searches and complex queries of the databases that telecommunications operators are required to build and hold. The Joint Committee on the Draft Communications Data Bill described the 'Request Filter' proposed in that Bill as "*a Government owned and operated data mining device*",[101] 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*"[102] 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".*[103] However, the processing of personal data represents a significant privacy intrusion. The Joint Committee on the draft Investigatory

[99] Investigatory Powers Bill 2016, clause 58
[100] Investigatory Powers Bill 2016, clause 58, subsection (5); see also *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 232
[101] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 113, p.35
[102] Ibid.
[103] Draft Investigatory Powers Bill 2015: Explanatory Notes, p.23

Powers Bill noted "*the privacy risks inherent in any system which facilitates access to large amounts of data in this manner".*[104] Whilst a useful tool for complex data searches, the 'Request Filter' cannot be viewed as a straightforward safeguard. Rather it is a portal with power to put together a comprehensive picture of each of our lives. It raises many of the same concerns as a large and centralised store, with added security concerns of protecting multiple distributed databases.

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.[105] The ability to conduct complex queries could increase the temptation to go on 'fishing expeditions': that is, to sift data in search of 'relationships' and infer that any concurrences are meaningful. This was one of the many concerns about this proposal expressed by the Joint Committee on the Draft Communications Data Bill.[106] For example, given this power, authorities could use communications data to identify attendees at a demonstration and correlate this with attendance at other public or private locations in the 12 month period; or to identify those regularly attending a place of worship, and correlate this with access to online radio websites, inferring risk.[107] Thus, this new ability could risk casting undue suspicion on thousands of innocent citizens.

[104] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, para. 247
[105] Davis and Watson v SS Home Office, 17/7/2015 [2015] EWHC 2092 (Admin).
[106] Joint Committee on the Draft Communications Data Bill: Report, 11 Dec 2012, para. 126, p.37
[107] GCHQ appears to practice similar data mining on the basis of supposed risk factors: *Profiled: From Radio to Porn, British Spies Track Web Users' Online Identities* – Ryan Gallagher, The Intercept, 25 Sept 2015.

National Security and technical capability notices

Amendment 488

Tabled by Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley , Margaret Ferrier and Alistair Carmichael.

Page 167, line 9, leave out clause 216 (**amendment 488**)

Effect

This amendment would remove the provision for national security notices.

Briefing

National security notices provide a blank-cheque power to the State, requiring a telecommunications operator to "take such specified steps as the Secretary of State considers necessary in the interests of national security". National security is left undefined and there is no time limit for their duration, a notice can last indefinitely. National security notices provide powers to force a telecommunications operator to engage in any conduct the Secretary of State demands – that is not otherwise provided for in the Bill. This includes, but is not limited to, the provision of services and facilities for the purpose of 'facilitating anything done by an intelligence service under any enactment other than this Act' and to deal with an emergency as defined under the Civil Contingencies Act 2004. The original draft of the Bill did not provide for any judicial involvement for national security notices but Government has now conceded the unsatisfactory judicial review model of oversight found elsewhere in the Bill for this power. The recipient of such a notice must comply with it but must not disclose the existence or contents of it. Without the ability to foresee the kind of activity and intrusion such obligations could entail – particularly whilst 'national security' remains undefined – it is impossible to condone this power.

Amendment 489

Tabled Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael.

Page 167, line 35, leave out clause 217 (**amendment 489**)

Effect

This amendment would remove the provision for technical capability notices.

Briefing

Clause 217 has proved to be one of the most controversial clauses in the Bill, and one 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'.

Similar to 'national security notices' in clause 216, '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. 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.

It is of further concern that obligations under clause 217 may not necessarily relate to an existing investigatory powers warrant or authorisation. Therefore, a service provider could be compelled with obligations to remove encryption and security measures for communications that are not currently subject to an investigatory powers warrant, perhaps with a view to

seeking a warrant for collection and interception in the future. Therefore, when a warrant for further surveillance is applied for, it is unlikely that the forced removal of encryption or security measures would form part of the proportionality assessment, as it could already have taken place.

Consequential amendments 490, 491, 492 following deletion of national security and technical capability notices.

Tabled Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael.

Page 168, line 2, leave out clause 218 (**amendment 490**)

Page 170, line 10, leave out clause 219 (**amendment 491**)

Page 170, line 38, leave out clause 220 (**amendment 492**)

IMPROVE TRANSPARENCY

Post-notification following surveillance

New Clause 1.

Tabled by Alistair Carmichael, Joanna Cherry and Gavin Newlands:

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).[108]

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

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

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 Tribunal introduced a new hurdle for IPT applicants.[109] 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.

Notification of surveillance is also important to reassure customers. Communications providers in the United States such as Microsoft and Twitter are currently engaged in legal battles on this matter. We believe that notification, in circumstances where it would not jeopardise ongoing investigations and operations, should be an international standard.

[109] [2016] UKIPTrib15_165-CH available at - http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

Whistleblower protections

Amendments 299, 300, 301, 302

Tabled by Andy Burnham, Keir Starmer, Lyn Brown, Jack Dromey, Sarah Champion, Sue Hayman, Joanna Cherry, Gavin Newlands, Stuart C. McDonald, Anne McLaughlin, Richard Arkless, Angela Crawley, Margaret Ferrier and Alistair Carmichael

Interception disclosures

Clause 51, page 41, line 18, 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." (**amendment 299**)

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 73, page 58, 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." (**amendment 300**)

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 84, page 65, line 26, at end insert –

(4A) Subsections (2) and (3) do not apply to a disclosure made in the public interest (**amendment 301**)

Equipment interference disclosures

Clause 116, page 93, line 39, 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 (**amendment 302**)

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.

Bella Sankey

Silkie Carlo

Sara Ogilvie