LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

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

October 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…… 3

"Equal lock" on warrant authorisations…….5

Cross-party criticism……..6

The Government's amendment……...7

Case law ……...7

The Watson case……8

Reasonable suspicion threshold…….9

No general warrants……...12

In breach of human rights law……13

Unique identifiers……...14

Government's response……...14

Cross-party concern……..15

Surveillance for serious crime and national security purposes only……....17

Serious crime……...18

***Stalking and harassment*……..18**

***Missing persons*……19**

Improve error reporting……20

***A breach of a person's human rights must be reported as an error*……...20**

***Obstructing the right to redress*……....20**

Fettering the IPC's discretion…….21

***A breach of the Human Rights Act does constitute 'harm'*……...21**

Establish the Privacy and Civil Liberties Board……22

Protections for legally privileged information…….……..24

Protections for journalists and sources……..26

INTRODUCTION

Liberty welcomes the opportunity to provide briefing and amendments for Report Stage of the Investigatory Powers Bill in the House of Lords.

The Government published 46 pages of amendments to the Bill on Tuesday 5th October, notably on provisions for surveillance of journalistic material and legally privileged communications. Whilst some of the amendments are welcomed, it remains that the Bill fails

to uphold fundamental democratic rights; extends police powers without attendant safeguards; puts the internet histories of the population at officer's fingertips in £170m+ plans; and disturbingly, extends the suspicionless surveillance powers that have been the subject of great public controversy,

At this vital juncture for civil liberties in the digital era, we urge Parliamentarians to consider the following amendments:

- An 'equal lock' for warrant authorisation, removing the 'judicial review' restriction
- Requiring that a reasonable suspicion threshold is met before surveillance warrants can be authorised
- Rejecting general warrantry for limitless numbers of persons or groups within the UK
- Requiring that surveillance is authorised only for national security and serious crime purposes; removing the power to access communications data for trivial purposes
- Uphold protections for clients' privileged communications with their lawyers
- Uphold journalistic protections and source confidentiality
- Remove the restriction on the Investigatory Powers Commissioner's reporting, that specifically prevents breaches of human rights being reported as serious errors
- Establish the Privacy and Civil Liberties Board to provide expert oversight, as provided for the in Counter-Terrorism and Security Act 2015
- Reject proposals for 'internet connection records' (see separate briefing).

Liberty currently has litigation pending both before the European Court of Human Rights & the Court of Justice of the European Union challenging key aspects of the current legislation, which is replicated and extended in this Bill. Awaiting further judgement in both cases, we do not address the bulk powers provided for in this Bill – but it should be noted that recent judgements are instructive on the many ways in which corresponding areas of the Bill fall woefully short of ECHR standards.

“EQUAL LOCK” ON WARRANT AUTHORISATIONS

Amendments to remove the ‘judicial review’ standard for Judicial Commissioners’ authorisations

Targeted interception

Clause 23, page 18, line 34, leave out “review the person’s conclusions as to” and insert “determine”

Clause 23, page 18, line 41, leave out paragraph (a)

Targeted equipment interference

Clause 103, page 80, line 26, leave out “review the person’s conclusions as to” and insert “determine”

Clause 103, page 80, line 33, leave out paragraph (a)

National security and technical capability notices

Clause 230, page 182, line 7, leave out “review the Secretary of State’s conclusions as to” and insert “determine”

Clause 230, page 182, line 14, leave out paragraph (a)

Clause 234, page 185, line 24, leave out “review the Secretary of State’s conclusions as to” and insert “determine”

Clause 234, page 185, line 33, leave out paragraph (a)

Effect

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

Briefing

The Government has claimed that judges would be able to go further than a narrow procedural review of a Minister’s decision - yet this is impossible to reconcile with its opposition to removing references to judicial review. To avoid uncertainty and ensure that Judicial Commissioners are not limited to reviewing only procedural aspects of the Secretary

of State's decision, but instead are able to determine the necessity and proportionality of warrants on the merits of their contents, all references to 'judicial review' should be removed.

Cross party criticism

The judicial review standard in the Bill has drawn criticism across all parties, from pre-legislative scrutiny to Committee scrutiny in the Commons and the Lords.

In Public Bill Committee, Keir Starmer QC MP tabled an amendment to provide for a "*true and equal lock",* concluding that the procedure in the Bill,

> *"(…) is not, therefore, truly a double lock. A double lock denotes a decision by the Secretary of State, which survives in clause 17, and a decision by a judge—a judicial commissioner—under clause 21, but this is not that sort of double lock."*

The Shadow Home Secretary, Andy Burnham MP, wrote to then Home Secretary Theresa May on this issue:

> "*If the 'double-lock' is to command trust, it needs to be an 'equal-lock'. That means* ***a judicial commissioner having the same ability to look at the merits of the case*** *and not just the process.* ***Removal of the JR test*** *would clear up any potential for confusion*." [1]

The issue has continued to draw criticism, even from the Government's own benches. During Committee stage in the Lords, Viscount Hailsham told the House:

> *"I should like to see some* ***review of the merits****—more particularly, addressing whether the issue of the warrant is properly supported by the material advanced in support of its issue and whether it is truly within the scope of the statutory criteria".*[2]

The Government has at times sought to argue that judges are not equipped to make a merits-based decision to authorise warrants and that it would be inappropriate for them to do so. Liberty finds this view concerning. Under our constitutional system, independent judges are well placed and experienced in assessing applications for intrusive powers and reaching impartial determinations on the facts and strengths of the application.

[1] *Letter to the Home Secretary on the Investigatory Powers Bill* – Andy Burnham MP, 4th April 2016, (emphasis added) http://andyburnhammp.blogspot.co.uk/2016/04/letter-to-home-secretary-on.html
[2] Committee Stage of the Investigatory Powers Bill in the House of Lords, July 13th 2016

The Government's amendment

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

Case law

In determining whether authorisation procedures comply with Article 8 of the ECHR, the Court will take into account the authority competent to authorise the surveillance, its scope of review and the content of the interception authorisation.

While in *Kennedy v UK* the Court upheld the existing model of authorisation for section 8(1) warrants under RIPA, Strasbourg case law has since evolved significantly. In both *Zakharov v Russia* and *Szabo and Vissy v Hungary* the Court found Article 8 violations and significantly tightened its jurisprudence on the independence of the authorising authority.

In *Roman Zakharov* v *Russia,* the European Court of Human Rights approved the fact that authorisations were issued by Russian courts but nevertheless found that this didn't meet necessary standards because "*Russian judicial scrutiny is limited in scope*" and Russian judges were not provided with necessary material "*to assess whether there is a sufficient factual basis to suspect the person in respect of whom measures are requested of a criminal offence."*[3]

In *Szabo & Vissy v Hungary*, the Court's commented extensively on the fact that

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

The Court rejected the Government's argument that a Government minister is better positioned than a judge to authorise measures of secret surveillance and instead held that "*the political nature of the authorisation and supervision increases the risk of abusive measures*" concluding that,

[3] *Roman Zakharov v Russia* (47143/06) 4 December 2015, para.261.

"*For the Court supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees*".[4]

The Watson Case

The Advocate General's opinion on Tom Watson MP's case at the CJEU emphasises the importance of substantive independent authorisation for access to communications data:

> *"(…) access to the data retained must be made* ***dependent on a prior review carried out by a court or by an independent administrative body*** *whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued."*[5]

Discussing routes to access communications data, the AG continued:

> *"Competent law enforcement authorities have every interest in requesting the broadest possible access. Service providers, who will be ignorant of the content of any investigation file, are incapable of checking that requests for access are limited to what is strictly necessary and persons whose data are consulted have no way of knowing that they are under investigation, even if their data is used abusively or unlawfully (…) Given the nature of the various interests involved,* ***the intervention of an independent body prior to the consultation of retained data, with a view to protecting persons whose data are retained from abusive access by the competent authorities, is to my mind imperative****."*[6]

We are strongly of the view that the current model for Secretary of State or Chief Constable authorisation of all types of warrants, supplemented only by a narrow judicial review of their decision by a Judicial Commissioner, will not meet the criteria recently elucidated by the Court. This would be remedied by the amendments above to make clear that Judicial Commissioners should engage in substantive, merits-based assessments of the necessity and proportionality of applications.

[4] *Szabo and Vissy v Hungary*, paras. 75-77
[5] OPINION OF ADVOCATE GENERAL SAUGMANDSGAARD 0E, Joined Cases *C·203/15* and *C·698/15* - 19 July 2016, para. 232
[6] Ibid. para. 236

REASONABLE SUSPICION THRESHOLD

Amendments to require reasonable suspicion of a serious crime

Targeted interception and examination

Clause 20, page 16, line 11, at end insert –

"( ) A warrant may be considered necessary on the ground falling within subsection (2)(b) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed and it is reasonably believed that the communications sought for interception will contain information relevant to the criminal investigation.."

Targeted communications data acquisition

Clause 58, page 48, line 9, at end insert –

"( ) An authorisation may be considered necessary on the grounds falling within subsections (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 and it is reasonably believed that the communications data sought will be relevant to the criminal investigation."

Targeted equipment interference and examination

Clause 97, page 75, line 21, at end insert –

"( ) A warrant may be considered necessary on the ground falling within subsection (5)(b) only where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed and it is reasonably believed that the equipment sought for interference will contain information relevant to the criminal investigation."

Effect

These amendments would require the authorities to demonstrate a reasonable suspicion of serious crime and a nexus between the communications sought and the crime suspected in order for a targeted surveillance warrant to be authorised.

Briefing

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

Intrusive powers can be authorised in order to 'prevent and detect serious crime', but this general purpose is left wide open to broad interpretation and abuse without requiring the authorising authority to verify the existence of reasonable suspicion of criminality. A requirement of reasonable suspicion, when the purpose of preventing and detecting serious crime is invoked, would prevent the potential of abusive surveillance of law-abiding citizens that we have seen in the past without unduly limiting legitimate use of surveillance powers.

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

In *Zhakarov v Russia* the European Court of Human Rights found Russian interception law to be in violation of Article 8 of the ECHR and emphasised that importance of a reasonable suspicion for compliance. It said:

> *"Turning now to the authorisation authority's scope of review, the Court reiterates that it must be capable of verifying the existence of reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures."*[7]

Opposition parties have proposed amendments on this point throughout the passage of the Bill.

In Public Bill Committee, Home Office Minister John Hayes MP described the Government's position:

> *"Not every individual involved in an investigation would themselves be suspected of committing a serious criminal offence, but their relationship with wider associates and potential facilitators of a crime might be crucial to identifying the extent of the organised crime gang and its international links and bringing the ringleaders to justice".*[8]

[7] Roman Zhakarov v Russia (Application No 47143/06), paragraph 260.
[8] Public Bill Committee on the Investigatory Powers Bill, 21st April 2016

The amendments suggested above would provide for this. They simply require (a) a threshold of reasonable suspicion that a serious crime had been planned or committed and (b) a factual basis for believing that the targeted communications would contain information relevant to the criminal investigation.

We urge the Government to accept the amendments and reassure the public that intrusive targeted surveillance powers can only be used where there is reasonable suspicion of a serious crime.

NO GENERAL WARRANTS

Amendments to require targets of surveillance are identified in warrants

Targeted interception and examination

Clause 29, page 23, line 20, leave out 'Where' and insert 'A targeted interception warrant, a mutual assistance warrant and a targeted examination warrant'

Clause 29, page 23, line 21, leave out paragraph (a)

Clause 29, page 23, line 24, leave out paragraph (b)

Clasue 29, page 23, line 26, leave out 'the warrant'

Clause 29, page 23, line 28, after 'communications' insert 'sought under the warrant'.

Targeted equipment interference and examination

Clause 108, page 86, line 35, at end insert –

( ) A targeted equipment interference warrant and a targeted examination warrant must specify the addresses, numbers, apparatus, or other factors, or combination of factors, that are to be used for identifying the material sought under the warrant.

Effect

These amendments clarify the 'requirements that must be met by warrants' under clause 29 and clause 108 in relation to targeted interception and targeted equipment interference warrants respectively. The requirements are that warrants must specify the identifiers (addresses, numbers, etc.) that will be subject to interference.

The amendments to clause 29 clarify that such requirements apply to all warrants issued under Part 2 (interception), and not only the warrants which merely 'describe' the target of interception/examination.

The amendment to clause 108 broadly replicates the requirements that must be met by interception warrants (cl. 29, subsections (8) and (9)) in the requirements that must be met by equipment interference and examination warrants.

Briefing

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, or even 'describe' *all* subjects, but rather can 'describe as many of those persons as is reasonably practicable'**.

To 'describe' a subject does not necessarily identify a person; to describe 'as many' subjects as practicable means that not all subjects need be described; and the leniency of 'reasonably practicable' could, in some circumstances, mean that no subject need be described at all. This loose drafting has **been criticised by the Intelligence and Security Committee,[9] the Joint Committee on the Draft Investigatory Powers Bill,[10] and the Joint Committee on Human Rights.[11]**

The intention in the Bill is to require that subjects of warrants are described with sufficient flexibility that a warrant can still be issued where the identities of the individual/s concerned are yet to be known. However, the warrant requirements far exceed this necessity and are so broadly drafted as to permit 'general warrants' – long outlawed under common law.

In breach of human rights law

Such broad 'general warrants' are also incompatible with the European Convention on Human Rights.

The Court's approach in this regard was reiterated in Kennedy v UK where the existing targeted interception regime under section 8(1) RIPA was upheld partly on the basis of Government's submissions that warrants only ever related to named individuals and premises. The Court noted with approval that:

> *"in internal communications cases, the warrant itself must clearly specify, either by name or by description, one person as the interception subject or a single set of premises as the premises in respect of which the warrant is ordered (see paragraphs 40 to 41 above). Names, addresses, telephone numbers and other relevant information must be specified in the schedule to the warrant."*[12]

The Court's strict standard in this regard was recently reiterated in its judgment *in Zakharov v Russia* where it held that interception authorisations:

---

[9] *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 45.
[10] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, recommendation 38, para. 468
[11] See Amendments tabled for Report Stage in the House of Commons
[12] Kennedy v UK, 2010, (Application no. 26839/05), paragraph 160.

> "*(…) must **clearly identify a specific person** to be placed under surveillance or a single set of premises as the premises in respect of which the authorisation is ordered. Such identification may be made by names, addresses, telephone numbers or other relevant information*". [13]

However, the unacceptable standard in the Bill allows for the full range of intrusive powers to be authorised against potentially unknown subjects.

Unique identifiers

Clearly, it is important that warrants are sufficiently flexible that they may be issued where the name of the target is not known. This is essential in the modern communications framework, where communications data such as a mobile phone number, an email address or an IP address rather than a name may be the investigative lead, or subject of surveillance. The Bill should be amended to reflect this intention and require that each person is named or specifically identified using a unique identifier to ensure a regime that meets human rights standards and does not permit spurious abuses of general warrantry.

A unique identifier (UID) is a numeric or alphanumeric string that is associated with a single entity – for example, a phone number, email address, a physical address, a Facebook numeric ID or device identifier such as an iPad UDID, MAC address for personal computers, or IMEI for mobile phones. As a minimum, a unique identifier should be required to ensure the surveillance is being applied to the intended target, and the warrant is sufficiently specific in its assessment of necessity and proportionality in relation to the subject to be compliant with human rights law.

Government's response

In evidence to the Joint Committee, Theresa May explained that such 'thematic' warrants are designed for "*circumstances in which perhaps somebody has been kidnapped or there is a threat to life, where only certain information is available, and it is necessary because of the pace at which something is developing to **identify the group of people** who are involved with that particular criminal activity as being within the thematic warrant*."[14]

It is right that warrants, whether affecting one person or multiple people within a group, **identify** the specific phones and computers (for example) that are to be subject to

[13] *Zakharov v Russia* (47143/06) 4 December 2015, paragraph 264.
[14] Theresa May MP in Oral evidence: Draft Investigatory Powers Bill, HC 651, 13 January 2016

surveillance under the warrant – even if the targets are subject to change - rather than only 'describe' the group affected. Identifying targets of surveillance is a practical necessity for deployment, as well as a legal necessity if our warrantry system is to comply with human rights law.

Facing consistent criticism on this point, Lord Keen attempted to justify the broad drafting during Committee Stage in the House of Lords:

> *"(…) it is not always possible at the outset of an investigation to know or have identified all of the individuals who may be subject to a warrant over the course of that investigation. (…) When a warrant is granted against a gang, the person applying for the warrant may not know that there are four members of the gang rather than three."*[15]

However, the ability to add a new subject to a warrant is specifically provided for by 'major modifications'. In fact, Lord Keen made this point himself when justifying the provision for major modifications in a separate debate during Committee Stage.[16] A major modification permits the Secretary of State (or in urgent cases, the person to whom the warrant is addressed) "adding, varying or removing the name or description of a person, organisation or set of premises to which the warrant relates",[17] without prior notification to a Judicial Commissioner. Therefore, the requirement that the subjects of warrants are identified – a bare minimum for human rights compliance – would clearly not obstruct the addition of further subjects to a warrant, which is carried out by a major modification.

Cross-party concern

In Public Bill Committee, Keir Starmer QC MP tabled a series of amendments to require identification in warrants. Debating the potential breadth of targeted hacking warrants, he said:

> *"It is called a targeted equipment interference warrant, but it is so wide as to be tantamount to a bulk power. (…) It is an extremely wide and permissive thematic warrant that allows interference with equipment in a very wide range of circumstances, which of course includes monitoring, observing, listening to and so on.* ***It is far too wide****".*[18]

[15] Lord Keen, Investigatory Powers Bill Committee Stage in the House of Lords, 19th July 2016
[16] Lord Keen, Investigatory Powers Bill Committee Stage in the House of Lords, cl.253, 13th July 2016
[17] Investigatory Powers Bill, 2016, cl.32(2)(a)
[18] Keir Starmer QC MP in Public Bill Committee on the Investigatory Powers Bill, 19th April 2016, cl. 381

In the same Committee, Joanna Cherry QC MP tabled amendments to require identification in warrants, commenting that the drafting of targeted interception warrants:

> *"(…) effectively permit a limitless number of unidentified individuals to have their communications intercepted.(…) Many lawyers believe that the scope of warrants permitted under clause 15 as drafted would fail to comply with both the common law and European Court of Human Rights standards, as expounded in a very recent decision in Zakharov v. Russia from 4 December 2015."*[19]

Both Keir Starmer MP and Joanna Cherry MP referenced the concerns that David Anderson QC has also expressed about the drafting of thematic warrants, which he describes as "***extremely broad***" and "*considerably more permissive than I had envisaged*".[20]

Similarly, in Second Reading of the Bill in the House of Lords, Lord Lester QC advised that:

> *"(…) the Bill should be amended to circumscribe the possible subject matter of warrants in the way recommended by the Independent Reviewer of Terrorism Legislation. That will ensure that the description in the warrant is sufficiently specific to enable the person unknown, but who is the subject of it, to be identified and to prevent the possibility of large numbers of people being potentially within the scope of a vaguely worded warrant".*[21]

In his Report on the Review of Bulk Powers, Mr Anderson described the drafting of thematic equipment interference as "strikingly broad", and as effectively an alternative power to bulk hacking, only with fewer safeguards.[22] He wrote:

> "*To the Government's answer that targeted thematic EI warrants will only be used in cases where the proposed interferences with privacy are adequately foreseeable, such that 'the additional access controls under the bulk EI warrantry regime are not required', I responded that (…)* ***it should be possible to 'reduce the scope of [targeted thematic warrants]*** *(…)'"*[23]

[19] Joanna Cherry QC MP in Public Bill Committee on the Investigatory Powers Bill, 12th April 2016, cl. 135
[20] Ibid, cl. 138
[21] Lord Lester QC in Second Reading of the Investigatory Powers Bill in the House of Lords, 27th June 2016
[22] *Report of the Bulk Powers Review* – David Anderson Q.C., 19 August 2016, para 2.12, p.22
[23] Ibid., emphasis added

SURVEILLANCE FOR SERIOUS CRIME AND NATIONAL SECURITY PURPOSES ONLY

Amendments to prevent communications data acquisition in relation to non-serious offences

> Clause 58, page 47, line 36, leave out 'or of preventing disorder' and insert 'or an offence under the Protection of Harassment Act 1997'
>
> Clause 58, page 47, line 36, after 'detecting' insert 'serious'.
>
> Clause 58, page 47, line 41, leave out subsection (d).
>
> Clause 58, page 47, line 42, leave out subsection (e).
>
> Clause 58, page 47, line 43, leave out subsection (f).
>
> Clause 58, page 47, line 49, leave out subsection (h).

Effect

This would limit the grounds for which access to communications data may be granted to the prevention and detection of serious crime or a stalking or harassment offence, the interests of national security, and preventing death or injury. These are the grounds for which interception warrants may be issued. Serious instances relating to the deleted subsections would rather fall under cl. 58 (7)(b).

Briefing

Currently, the Bill would allow access to communications data for eleven broad purposes including economic wellbeing, protecting public health, in the interests of public safety, collecting any taxes or duties, and mitigating damage to a person's mental health.[24]

Article 8 of the HRA and Articles 7 & 8 of the Charter of Fundamental Rights requires access to communications data to be strictly restricted to circumstances where precisely defined serious crime is being investigated. In the Advocate General's opinion in the Watson case, delivered on 19th July 2016, Henrik Saugmandsgaard Øe made clear that communications data must only be used for the purpose of preventing and detecting precisely defined serious crime. His opinion said:

> *"(…) the requirement of proportionality within a democratic society* ***prevents the combating of ordinary offences and the smooth conduct of proceedings other than criminal proceedings from constituting justifications for a general data***

[24] Investigatory Powers Bill 2016, clause 58

> ***retention obligation**. The considerable risks that such obligations entail outweigh the benefits they offer in combating ordinary offences (…) Article 52(1) of the Charter must be interpreted as meaning that the fight against serious crime is an objective in the general interest that is capable of justifying a general data retention obligation, whereas **combating ordinary offences and the smooth conduct of proceedings other than criminal proceedings are not**."*[25]

Similarly, elsewhere in the Bill targeted interception and other powers are restricted to use where it is necessary and proportionate for the prevention and detection of serious crime or in the interests of national security. Given the incredibly intrusive nature of communications data, and the rights implications set out in the *Watson* case, it is right that the threshold for access is streamlined across the powers and that a "serious crime" threshold applies to the surveillance of communications data.

Serious crime

Serious crime is defined in the Bill as an offence carrying a sentence of three years imprisonment or more, or a crime where the conduct involved the "use of violence", results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose.[26]

"Violence" is not consistently defined in UK law, and it is unclear precisely which offences are included and excluded within the definition. However, "violence" predominantly refers to physical violence in UK law, and several parliamentarians have expressed concern that the serious crime definition in the Bill would not include stalking offences and serious online harassment, even though many such cases involve threats of physical and sexual violence.

Stalking and harassment

To allow for communications data to be used in relation to stalking and harassment offences, Liberty recommends amending paragraph 58(7)(b) so that communications data can be accessed "for the purpose of preventing or detecting **serious** crime or **an offence under the**

[25] OPINION OF ADVOCATE GENERAL SAUGMANDSGAARD 0E, Joined Cases *C·203/15* and *C·698/15* - 19 July 2016, paragraphs 172-3
http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=80465
[26] Investigatory Powers Bill 2016, clause 239

Protection from Harassment Act 1997" (additions in bold). This would raise the threshold for accessing communications data to serious crime, as per our obligations under human rights law, whilst explicitly including stalking and harassment offences – offences which cause serious harm and fear and for which communication is the primary tool of perpetrators.

Missing persons

It is Liberty's view that this amendment, combined with the deletion of non-serious purposes listed in paragraphs 58(7)(d), (e), (f) and (h), would improve the Bill's compliance with human rights case law. The retention of paragraph 58(7)(g), "the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health", would permit communications data to continue to be used in missing person inquiries.

IMPROVE ERROR REPORTING

Amendments to remove the restriction on reporting errors that breach a person's Convention rights

Page 165, clause 20, line 41, leave out 'must' and insert 'may'

Page 165, clause 209, leave out line 44

Page 166, clause 209, line 1, leave out subsection (2)

Page 166, clause 209, line 5, leave out subsection (3)

Effect

This amendment would give the Investigatory Powers Commissioner discretion to inform a person of an error relating to them, if doing so is deemed to be in the public interest, and not prejudicial to national security or the prevention and detection of crime.

Briefing

The Bill provides for the Investigatory Powers Commissioner to inform someone subjected to a surveillance error by a public authority (but not a CSP) only if it is 'serious', which the Bill defines as causing "significant prejudice or harm to the person concerned" (terms which are left undefined). The Government makes a startling assertion that a breach of a person's Human Rights is *not* necessarily a serious error (cl. 209(3)) – i.e. a breach of one's rights does not constitute harm. Furthermore, the Bill imposes a restriction that the IPC may not inform someone that their rights have been breached in a serious error *unless* an additional test of significant prejudice or harm is met (cl. 209(7)).

A breach of a person's human rights must be reported as an error

There is no doubt that a breach of a person's human rights must constitute a serious error. If public authorities' conduct is not in accordance with the law, and a person's rights are subsequently breached, this is undoubtedly a serious error and must be reported.

Obstructing the right to redress

If a person is not informed that their rights have been breached, they will be denied the right to exercise their right to remedy and bring proceedings against the authority in breach, as

provided for by s.7(1) of the HRA. The demonstration of ‘harm’, however defined, is irrelevant to this right.

Fettering the IPC’s discretion

The restriction imposed by cl. 209 (3) and (7) obstructs the IPC from informing a person that their Convention rights have been breached (unless an additional test is met), despite the fact that they are aware of the breach. As such, the IPC would further be complicit in obstructing the affected person’s right to redress. It is wholly inappropriate and unconstitutional to require that the IPC, of high judicial office, is forced to actively deny people their fundamental rights in this way.

A breach of the Human Rights Act does constitute ‘harm’

A breach of a person’s Convention rights necessarily constitutes harm to a person. It is sufficient if an individual’s Article 8 rights are breached, for example, for the person affected to be awarded damages. It is clearly recognised by ECtHR and UK courts that such a breach is significant and deserving of remedy without an arbitrary and superfluous threshold of ‘harm’ being enforced. Evidently, harm is inherent to human rights breaches.

ESTABLISH THE PRIVACY AND CIVIL LIBERTIES BOARD

New Clause

"**Privacy and Civil Liberties Board**

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

Effect

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

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

In July 2014, over two years ago, then Home Secretary Theresa May MP promised:

> *"We are going to ensure that we have more transparency from Government (…) We will also reduce the number of bodies that are able to have access to the communications data,* ***establish a privacy and civil liberties board based on the US model****, have a review of the capabilities and powers that are necessary against the threats we face and the ways in which those are regulated, and lead discussions with other Governments on how we deal with these matters of sharing data across borders."*[27]

In February 2015, months before the publication of the Draft Investigatory Powers Bill, Theresa May MP maintained her pledge to establish a Privacy and Civil Liberties Board under the Counter Terrorism and Security Act. She said:

> *"(…) it is worth reflecting on David Anderson's most recent comments on these matters:*
>
> > *'if skilled and practical people are appointed to the Board, content to work under the Reviewer's direction, the capacity for independent review will be improved.'*

[27] Theresa May MP in Communications Data and Interception debate in Commons Chamber, 10 July 2014, cl. 472

I should also draw the attention of hon. Members to his acknowledgement published on his website and dated 31 January that

> *'the Government has listened to what I have been saying, and put forward changes which should significantly improve the ability of the Independent Reviewer to do an effective job.'"*[28]

The existing provision for a Privacy and Civil Liberties Board does not alter or amend the existing statutory duties of the Independent Reviewer of Terrorism Legislation, but could significantly enhance his/her work. The addition of expert scrutiny, particularly focused on safeguarding civil liberties, would be a welcome addition and would especially appropriate for the review of the functioning of the duties in relation to privacy (as required under clause 2) and the General Privacy Protections (Part 1) more widely.

[28] Theresa May MP in Counter-Terrorism and Security Bill debate in Commons Chamber, 10th February 2015, cl. 733

PROTECTING LEGALLY PRIVILEGED INFORMATION

The Government published amendments on 5th October 2016 which amend the circumstances in which public authorities can surveil legally privileged communications.

If the Bill is amended in this way, public authorities will be authorised to intercept or hack devices to obtain legally privileged communications if there are no other reasonable means to obtain the information, and the information is sought in the interests of national security, or for the prevention or detection of crime where the purpose is to prevent significant injury or death. Legally privileged communications may also be obtained under bulk powers, and examined if the conditions above are similarly met.

There are no protections afforded to communications data relating to legally privileged material.

Liberty is concerned that the 'national security' exemption for legally privileged communications is a significant and dangerous policy shift. Legal professional privilege is a cornerstone of our democratic tradition and an essential component of a free society under the Rule of Law. Any exception to this principle is only conceivably justified in circumstances where legally privileged material may contain information necessary for the purposes of preventing death or serious injury. However, the Bill, as amended, would provide a wide catch-all national security exemption, that would render legal privilege obsolete.

The only known example of GCHQ targeting interception of legally privileged material relates to Libyan politician, Mr Sami Al Saadi, who alleges he was a victim of a joint CIA-SIS rendition operation in which he and his wife and four children were kidnapped and rendered to Gaddafi's Libya in 2004. He launched civil proceedings to attempt to hold the UK Government to account for this and during the course of the proceedings, in the wake of the Snowden revelations, his lawyers came to fear that they were under surveillance. He brought proceedings in the Investigatory Powers Tribunal to ascertain whether he had been targeted by the Agencies and over the course of the proceedings the Government conceded that "since January 2010 the policies and procedures for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material have not been in accordance with human rights legislation specifically Article 8(2) of the ECHR." The Tribunal agreed and also made a further determination that two documents containing material subject to Mr Al Saadi's LPP were held by GCHQ. The Tribunal ordered GCHQ to give an undertaking that these documents would be destroyed or deleted. It is unacceptable that the Government could have used its surveillance powers to undermine attempts to hold it to account for its complicity in torture, but given the absence of a national security definition and the circular

and subjective definition frequently adopted by the Executive, it is possible that similar interception of LPP material would continue under the terms of the Bill.

As Ken Clarke MP remarked in the debate in the House of Commons: *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."* [29] In *Szabo and Vissy* the Court similarly observed *"in a matter affecting fundamental rights it would be contrary to the rule of law, one of the basic principles enshrined in the Convention, for a discretion granted to the Executive in the sphere of national security to be expressed in terms of an unfettered power."*[30] The Joint Committee on the draft Bill recommended that the Bill should include definitions of national security but to date this advice has been ignored by the Executive.[31]

In absence of such a definition, we recommend that:

- Legally privileged material should only be sought or examined for the purpose of national security where the material is necessary for the prevention of death or significant injury.

In addition, we support the insertion of an identical amendment to provide equivalent protection to legally privileged communications data.

[29] See Hansard, 15 March 2016, http://www.publications.parliament.uk/pa/cm201516/cmhansrd/cm160315/debtext/160315-0002.htm
[30] Szabo and Vissy v Hungary, para 65.
[31] *Report of the Joint Committee on the Draft Investigatory Powers Bill,* 11 February 2016, Recommendation 82

PROTECTIONS FOR JOURNALISTS AND SOURCES

The Government published amendments on 5th October 2016 which specify the circumstances in which public authorities can surveil confidential journalistic material and identify journalists' sources.

As it stands the Bill provides procedural protection only where communications data is sought with the purpose of identifying a source. The new amendments pertain to 'protections' for journalists and sources in relation to targeted interception and equipment interference powers. However, that 'protection' is merely that handling arrangements are in place for dealing with the material sought. There are no procedural protections regarding targeted access to journalistic material/source identities and similarly no procedural protections for the examination of journalistic material/source identities obtained through bulk powers.

These amendments are a missed opportunity to meet our obligations under Article 10, and fall dismally short of upholding the fundamental democratic principles put so at risk by these powers.

Liberty strongly recommends that further amendments are urgently sought to ensure the following:

- Communications data sought or examined to identify a journalist's source should only be authorised in the interests or national security or the prevention and detection of serious crime, if the public interest in obtaining the identity *outweighs* the public interest in a free press and source protection, and there are no other reasonable means by which to identify the suspect

- Any journalistic material, or source identity, sought or examined under an interception or equipment interference warrant should only be authorised in the interests or national security or the prevention and detection of serious crime, if the public interest in obtaining the material/identity *outweighs* the public interest in a free press and source protection, there are no other reasonable means by which to obtain the material or identify the suspect, and where there are reasonable grounds to believe that the material sought is likely to be of substantial value to the investigation.