

# LIBERTY

PROTECTING CIVIL LIBERTIES  
PROMOTING HUMAN RIGHTS

## **Liberty's briefing on Part 2 of the Investigatory Powers Bill for Committee Stage in the House of Commons**

**April 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](mailto:bellas@liberty-human-rights.org.uk)

Rachel Robinson

Policy Officer

Direct Line: 020 7378 3659

Email: [rachelr@liberty-human-rights.org.uk](mailto:rachelr@liberty-human-rights.org.uk)

Sara Ogilvie

Policy Officer

Direct Line: 020 7378 3654

Email: [sarao@liberty-human-rights.org.uk](mailto:sarao@liberty-human-rights.org.uk)

Silkie Carlo

Policy Officer (Technology & Surveillance)

Direct Line: 020 7378 5255

Email: [silkiec@liberty-human-rights.org.uk](mailto:silkiec@liberty-human-rights.org.uk)

Sam Hawke

Policy Assistant

Direct Line

Email: [samuelh@liberty-human-rights.org.uk](mailto:samuelh@liberty-human-rights.org.uk)

## Introduction

1. Liberty welcomes the opportunity to provide briefing and amendments in relation to Part 2 of the Investigatory Powers Bill.
2. This briefing sets out the following proposals for reform:
  - A single-step process of judicial authorisation to replace the proposed “double lock” system and ensure that decisions to issue warrants are taken by judicial commissioners rather than the Secretary of State
  - Clarifying the standard for review by a judicial commissioner as a substantive merits review rather than a limited judicial review
  - Ensuring that warrants contain an identifiable subject matter rather than permitting warrants to be granted on the basis of broad themes which could effectively subject hundreds of thousands of individuals to surveillance powers
  - Remove “the economic well-being of the UK” as a separate ground for the authorisation of interception
  - Require that the grounds for authorisation are tied to a threshold of reasonable suspicion that a criminal offence has been or will be committed
  - Delete provisions to allow for modification of warrants without judicial authorisation
  - Limit the circumstances in which urgent warrants can be issued, reduce the length of time in which a judicial commissioner must then decide whether or not to approve the warrant, and require the deletion of any material gathered under an urgent warrant that is not approved unless there are exceptional circumstances.
  - Delete provisions seeking to permit the extension by rules and regulations of interception powers in prisons, psychiatric hospitals and immigration detention centres.
  - Remove provisions seeking to extend the reach of warrants in this part extraterritorially.
  - Additional protections for confidential and privileged correspondence.

## **Judicial Authorisation**

### **Amendments**

Clause 17, Page 13, line 4, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 5, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 8, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 10, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 13, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 16, leave out paragraph (d)

Clause 17, Page 13, line 20, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 22, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 24, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 27, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 31, leave out paragraph (d)

Clause 17, Page 13, line 35, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 37, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 39, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 42, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 13, line 45, leave out paragraph (d)

Clause 17, Page 14, line 5, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 14, line 8, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 17, Page 14, line 13, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 18, Page 14, line 16, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 18, Page 14, line 30, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 18, Page 14, line 31, leave out “Secretary of State” and insert “Judicial Commissioners”

Clause 19, Page 14, line 39, leave out Clause 19

Clause 21, page 17, line 2, delete clause 21

### **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.

### **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.

*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*".<sup>1</sup>

In recognition of concerns that have been expressed regarding warrants that may have international relations ramifications, Liberty advocates for an amendment to the internal processes in place for MI6 which could require a certain category of warrants to receive internal approval by the Foreign Secretary before the formal authorisation process is triggered. However, this should be entirely separate from the system of independent authorisation and does not need to be provided for in legislation.

*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.*”<sup>2</sup> 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.*”<sup>3</sup> Liberty also questions whether Ministers are best placed to decide the legality of warrants. During an oral evidence session with the Intelligence and Security Committee in 2014, Phillip Hammond MP, the Secretary of State for Foreign and Commonwealth Affairs, appeared to misunderstand a number of key RIPA terms – in particular the distinction between internal and external communications – and appeared confused about how the warrant system for surveillance operates.<sup>4</sup> This is a cause for concern, given his huge, current, responsibility for authorising 8(4) RIPA warrants.

---

<sup>1</sup> David Anderson QC, A Question of Trust, paragraph 14.54

<sup>2</sup> David Anderson QC, A Question of Trust, paragraph 14.49.

<sup>3</sup> 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>.

<sup>4</sup> See, for example: <http://www.theguardian.com/politics/2014/dec/11/philip-hammond-powers-warrants-understanding>

*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*”.<sup>5</sup> The Reviewer responded to this argument in his report in June by rightly 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.<sup>6</sup>

A corollary to this argument is that ministers are politically accountable for the Agencies and will be required to resign if things ever go wrong. This is also incorrect. While the Home Secretary is responsible for setting the strategic direction of the Government's counter-terrorism policy and the Cabinet Minister responsible for MI5, MI5 - like the police - is operationally independent. MI5's Director General retains operational independence for day-to-day decision-making. Historically, when terrorist attacks have tragically succeeded, this has not led to political resignations. Despite inquests and inquiries following the 7/7 attacks and the murder of Fusilier Lee Rigby uncovering internal errors in the Agencies' handling of information relating to those responsible for the attacks, this has not resulted in the 'political accountability' now being claimed. 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,<sup>7</sup> 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.<sup>8</sup> In Canada it is unlawful to intercept

---

<sup>5</sup> Paragraph 203GG.

<sup>6</sup> Clauses 49 & 51 of the Bill criminalise the disclosure of the existence of an interception warrant without authorisation to do so.

<sup>7</sup> 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.

<sup>8</sup> *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

private communications unless the interception is in accordance with an authorisation issued by a judge,<sup>9</sup> 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.<sup>10</sup> 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.

## **Standard of Review**

### **Amendment**

Clause 21, Page 17, line 10, leave out subsection (2)

### **Effect**

This amendment would remove reference to the standard of review to be conducted by a Judicial Commissioner as that of judicial review rather than a substantive merits review.

### **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 JCs consider warrants issued by the Secretary of State. In conducting judicial review of Executive decisions the courts apply a varying standard of review that is highly dependent on the context of the matter before it. At one end of the spectrum is a strict “Wednesbury” standard of review which will only interfere with an Executive decision that is manifestly unreasonable. At the other end of the spectrum is a more intense standard of review that will substantively assess the proportionality of the Executive decision.

---

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).

<sup>9</sup> Canada *Criminal Code*, Part VI, section 186.

<sup>10</sup> Part 11A of the *Crimes Act*, and under the *Misuse of Drugs Amendment Act 1978*.

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

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

A merits review is also made practically impossible by the two-stage model in the Bill. The issuing authority will be the body with the practical ability to probe and test the requesting

---

<sup>11</sup> *Home Office v Tariq*, [2011] UKSC 35.

<sup>12</sup> *Home Office v Tariq*, paragraph 27.

<sup>13</sup> *Home Office v Rehman* [2001] UKHL 47.

agency or law enforcement body as to the necessity and proportionality of a warrant. The secondary role given to JCs under the model in the Bill will mean that JCs are restricted to considering ministerial decisions to issue warrants on the papers, in secret, with no opportunity to question the requesting agency, nor to probe as to whether less intrusive methods or capabilities could be deployed or ask for further material to justify the request. It should also be noted that Judicial Commissioners will make their decisions *ex partes* and therefore without the benefit of substantive legal argument. In order to ensure that JCs have a substantive role in issuing warrants, they must receive applications directly from requesting bodies and be provided with expert technical support to ensure a substantive assessment of warrants.<sup>14</sup>

---

<sup>14</sup> The explanatory notes say that Government will make tech expertise available to the IPC but there are no details and no particular obligations are provided on the face of the Bill. Explanatory Notes, p. 8, para. 13: The Investigatory Powers Commissioner will be able to draw on extensive legal and technical expertise. Guide to powers, p.31, para. 75: The IPC will oversee how the agencies use bulk personal datasets: “Supported by a team of Judicial Commissioners and technical and legal experts, the Commissioner will audit how the agencies use them and they will report publicly on what they find”. 176: On how the JCs will be funded, and the Sec of State will provide staff, accommodation, equipment and ‘other facilities’ as necessary, after consultation with the IPC. In the explanatory notes on 176 (p. 54, para 409): “It is intended that the resources afforded to the Investigatory Powers Commissioner will ensure that the office is fully staffed with judicial, official, legal and technical support to ensure that the Commissioners are fully able to perform their oversight and authorisation functions and to hold those that use investigatory powers to account”.

## **Subject matter of warrants**

### **Amendments**

Clause 15, page 12, line 3, after or delete 'organisation'

Clause 15, Page 12, line 8, insert after activity 'where each person is named or otherwise identified'

Clause 15, Page 12, line 9, delete 'organisation'

Clause 15, page 12, line 11, insert after 'operation' 'where each person is named or otherwise identified'

Clause 15, page 12, line 12, delete subclause (c)

Clause 15, page 12, line 13, delete subclause (3)

Clause 27, page 21, line 7, delete 'organisation'

Clause 27, page 21, line 8, delete 'organisation'

Clause 27, page 21, line 13, delete 'or describe as many of those persons as is reasonably practicable to name or describe' and insert 'or otherwise identify all of those persons'

Clause 27, page 21, line 15, delete 'or organisation'.

Clause 27, page 21, line 19, delete '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.'

### **Effect**

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**

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. The creation of thematic warrants in the Bill means that communications intercepted in their billions under Part 6 could be trawled thematically for groups sharing a common purpose or carrying on a particular activity. It provides for an open-ended warrant that could encompass many hundreds or thousands of people. The expansive scope of these warrants, combined with the broad grounds for which they can be authorised, do not impose sufficient limits on the authorities' interception powers.

This change follows the dramatic disclosure in March 2015 that the Secretary of State is already issuing "thematic" interception warrants. The ISC reported that the significant majority of 8(1) warrants relate to one specific individual, but that some do not apply to named individuals or specific premises but rather groups of people. The current Home Secretary has apparently derived the authority to do so from the broad definition given to "person" found elsewhere in RIPA, despite the unequivocal reference to "one person" in section 8(1). Liberty does not recognise this unorthodox statutory construction and any thematic warrants that have been issued under this power are likely to be *ultra vires*. Like much surveillance practice in recent years, this appears to be a case of the Agencies and Executive claiming powers well beyond those provided on the face of RIPA and other enabling statutes. The existence of "thematic" warrants also represents a huge departure from the position at common law which has long banned "general warrants".

The ISC reported that the Interception of Communications Commissioner has "*made some strong recommendations about the management of thematic warrants*" and has in some cases recommended that they are cancelled.<sup>15</sup> 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*".<sup>16</sup> Reporting on the draft Investigatory Powers Bill, the ISC noted that "*unfortunately*", its previous recommendation "*has not been reflected in the draft Bill*";<sup>17</sup> 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*

---

<sup>15</sup> *Privacy and Security: a modern and transparent legal framework* - Intelligence and Security Committee, March 2015, paragraph 45.

<sup>16</sup> *Ibid*, page 24 recommendation D

<sup>17</sup> *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J(vii).

*amended so that targeted interception and targeted equipment interference warrants cannot be used as a way to issue thematic warrants”.*<sup>18</sup>

Liberty believes the scope of warrants permitted under clause 15 fails to comply with both common law and ECHR standards. In *Zakharov v Russia*<sup>19</sup> 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.*”<sup>20</sup> While thematic warrants do not relate to geographical location, they are sufficiently broad to violate Article 8 and need considerable amendment on the face of the Bill.

---

<sup>18</sup> *Report of the Joint Committee on the Draft Investigatory Powers Bill*, 11 February 2016, recommendation 38, para. 468

<sup>19</sup> (47143/06) 4 December 2015.

<sup>20</sup> Paragraph 265.

## **Grounds on which warrants may be issued by Secretary of State**

### **Amendments**

Clause 18, page 14, line 20, after security insert 'or'

Clause 18, page 14, line 21, delete 'or'

Clause 18, page 14, line 22, delete subclause (2)(c)

Clause 18, page 14, line 33, delete subclause (4)

### **Effect**

These amendments would delete the separate ground for interception of "economic well-being" from the face of the Bill.

### **Amendment**

Clause 18, page 14, line 20, insert after 'security', where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed.

Clause 18, page 14, line 21, after 'crime' insert where there is a reasonable suspicion that a serious criminal offence has been or is likely to be committed.

### **Effect**

These amendments would require that the grounds for interception are tied to a threshold of reasonable suspicion of criminal behaviour.

### **Briefing**

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

All three main statutory grounds for authorising surveillance are unnecessarily vague and left dangerously undefined. As the decision will continue to lie with the Secretary of State, the test will be met by whatever he or she subjectively decides is in the interests of national

security or the economic well-being of the UK. This means that individuals are not able to foresee when surveillance powers might be used, and grants the Secretary of State discretion so broad as to be arbitrary. The Joint Committee on the draft Bill recommended that the Bill should include definitions of national security<sup>21</sup> and economic well-being<sup>22</sup>; the ISC further recommended that economic well-being should be subsumed within a national security definition, finding it “*unnecessarily confusing and complicated*”.<sup>23</sup> The ISC queried both the Agencies and the Home Office on this point but reported that ‘*neither have provided any sensible explanation*’.<sup>24</sup> Their report recommendations were dismissed, and the core purposes for which extraordinary powers can be used remain undefined, and dangerously flexible, in the Bill.

In keeping with these recommendations, it is imperative that the Government produces for the Committee an amendment to define national security, which Committee members can then scrutinise. The amendments proposed in this briefing are supplementary to, not a replacement for, such a definition.

The three grounds contain no requirement for reasonable suspicion that an individual has committed or intends to commit a serious criminal offence, nor even suspicion or evidence that a serious crime has been or is going to be committed. This gives licence for speculative surveillance.

The national security ground is particularly problematic, as the Courts have responded with considerable deference to Government claims of ‘national security’, viewing them not as a matter of law, but as executive led policy judgements.<sup>25</sup> National security as a legal test is therefore meaningless. The second ground is similarly broad and open-ended and the Government has not sought to clarify the circumstances in which ‘national security’ as opposed to ‘the prevention and detection of serious crime’ will be in play.

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

---

<sup>21</sup> *Report of the Joint Committee on the Draft Investigatory Powers Bill*, 11 February 2016, Recommendation 82

<sup>22</sup> *Ibid.* Recommendation 83

<sup>23</sup> *Report of the draft Investigatory Powers Bill – The Intelligence and Security Committee*, 9 February 2016; Recommendation J (i)

<sup>24</sup> *Ibid.*

<sup>25</sup> 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”.

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.

## **Modification of warrants**

### **Amendment**

Clause 30, page 23, line 19, delete clause 30 and 31

### **Effect**

This amendment deletes clause 30, which provides for the modification of warrants without judicial authorisation.

### **Briefing**

Surprisingly, the Bill provides for many types of warrant to be retrospectively modified without judicial authorisation. Modifications can relate to the names, premises, organisations etc. to be targeted. While Liberty has serious concerns about the mechanism of judicial sign off provided for by the Bill, the entire purpose of having a warrant system subject to any form of oversight at all is to test whether individuals ought to be subject to surveillance. It is no minor modification to subject an individual or set of premises to interception powers – it is the entire purpose of the system. Allowing the state to add an intercept subject to a warrant without prior judicial authorisation undermines the entire legislative scheme and circumvents the most basic safeguard provided by Part 1. For the Bill to have any credibility at all, this provision must be removed.

If the Bill provided for one-stage judicial authorisation of warrants, on properly defined grounds, as per the amendments suggested above, only then would modifications be appropriate as they would be subject to a proper legal test.

## **Urgent Warrants**

### **Amendment**

Clause 22, page 17, line 29, insert new clause 22(1)(A): “A warrant under this section can only be issued in an emergency situation posing immediate danger of death or serious physical injury.”

### **Effect**

This amendment specifies that urgent warrants can only be issued where it is necessary in an emergency situation posing immediate danger of death or serious physical injury.

### **Amendment**

Page 17, line 30, after “must” insert “immediately”

### **Effect**

This amendment requires that a Judicial Commissioner be informed that an urgent has been issued immediately. The current provision makes no stipulation as to timeframe for informing a judicial commissioner.

### **Amendment**

Clause 22, page 17, line 35, delete “the third working day after the day on which” and replace with “48 hours after”

### **Effect**

This amendment reduces the period within which a judicial commissioner must decide whether to authorise a warrant to 48 hours after it was issued.

### **Amendment**

Clause 23, page 18, line 7, delete “may” and replace with “must”

Clause 23, page 18, line 9, leave out subclauses (b) and (c) and insert (3A) –

3A If the Judicial Commissioner determines that there are exceptional circumstances, the Judicial Commissioner must instead impose conditions as to the use or retention of any of that material.

### **Effect**

These amendments require a Judicial Commissioner to order that material collected under an emergency warrant which he does not authorise be destroyed, except in exceptional circumstances.

### **Briefing**

In urgent cases warrants can be issued without the authorisation of a Judicial Commissioner, but the Judicial Commissioner must give ex post facto authorisation within 3 working days.<sup>26</sup> However, a 48-hour timeframe for authorisation would be the maximum to harmonise the process with recent case law from Strasbourg, as *Zakharov* included a complaint that urgent

---

<sup>26</sup> Clause 22(3)

interception could occur without judicial authorisation for up to 48 hours<sup>27</sup>. There is no reason that we should allow a longer period for unapproved surveillance than Russia. Following scrutiny of the Draft Bill, the Joint Committee recommended that urgent warrants should be reviewed by a Judicial Commissioner within 24 hours (Recommendation 36), whilst the Intelligence and Security Committee recommended review within 48 hours (Recommendation v). These amendments implement this recommendation.

Should material be obtained under an urgent warrant later unapproved by a JC, a JC may, but is not required to, order the destruction of the material obtained. Once again, this provision creates a significant loophole that can be used to bypass the legal protections which purport to be provided the judicial review mechanism provided by the Bill. An urgent warrant allows the relevant agency to access material which it may not be authorised to do so in law, and permitting the retention of this material in anything other than exceptional circumstances creates a clear incentive to use the urgent process in inappropriate cases. In order to ensure that the applying agencies only use the urgent process where it is strictly necessary, the Bill must ensure that there are no advantages that can be gained from doing so. Where a JC does not authorise the issue of a warrant retrospectively, the position must be that the material collected is destroyed except in exceptional circumstances.

---

<sup>27</sup> Roman Zakharov v. Russia, 4<sup>th</sup> December 2015, (Application no. [47143/06](http://hudoc.echr.coe.int/eng?i=001-159324)) available at - <http://hudoc.echr.coe.int/eng?i=001-159324>

## **Confidential and privileged communications**

### **Amendment**

Clause 24, page 18, line 37, after 'Members of Parliament' insert – ' and Journalists etc'

Clause 24, page 19, line 7, delete subsection (2)

Clause 24, page 19, line 14, insert new clause 24 A -

- (1) Where a warrant is likely to cover special procedure material, the procedure set out at section 3 below must be followed
- (2) Where a warrant is likely to cover excluded procedure material, the procedure set out at section 4 below must be followed
- (3) 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:
    - a. the democratic importance of freedom of expression under article 10 ECHR to grant the warrant; or
    - b. the democratic interest in the confidentiality of correspondence with members of a relevant legislature
- (4) Further to the requirements set out elsewhere in this part, the Judicial Commissioner may only issue a warrant in accordance with provisions made in Schedule 1 of the Police and Criminal Evidence Act and Schedule 5 of the Terrorism Act
- (5) An application for a warrant under this Part must not be granted where the information could be sought using a warrant under schedule 1 PACE, unless seeking this information under PACE doing so would defeat the purpose of the investigation.
- (6) Special procedure material means:
  - a. Special material as defined in section 14 of the Police and Criminal Evidence Act 1984
  - b. Correspondence sent by or intended for a member of the relevant legislature
- (7) Excluded material procedure has the same meaning as section 11 of the Police and Criminal Evidence Act 1984

### **Effect**

This amendment would ensure that when a warrant is requested to intercept confidential material that is of a confidential nature, including journalistic material and material relating to a journalist's sources, additional protections are applied. The protection would also cover

correspondence sent by or intended for a Member of Parliament or other legislatures. The tests to be applied prior to granting a warrant broadly replicate those already provided for in the Police and Criminal Evidence Act 1984. The amendment provides for two procedures: special material procedure and excluded (source) material, which is subject to a stricter test in accordance with current legislation.

The special material procedure applies, broadly speaking, where there is non-excluded journalistic material and or where material has been acquired in the course of a profession or trade and that material is held subject to an express or implied undertaking to hold that material in confidence. (clause 14 PACE)

Where material to be accessed is under this procedure, 4 conditions must be met: There are reasonable grounds for believing that an indictable offence has been committed; 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); 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; and It is in the public interest.

Excluded material procedure applies, broadly speaking, where there is journalistic material which a person holds in confidence and consists of documents or records. It also covers other personal records which a person has acquired in the course of a profession or trade and holds in confidence. (clause 11 PACE).

Under this procedure, PACE only permits access where a search warrant power prior to PACE would have granted access, or separately schedule 5 of the Terrorism Act 2000 permits access in excluded cases where: the order is sought for the purposes of a terrorist investigation, and there are reasonable grounds for believing that the material is likely to be of substantial value, whether by itself or together with other material, to a terrorist investigation; and there are reasonable grounds for believing that it is in the public interest that the material should be produced.

Journalistic material means material acquired for the purposes of journalism. (clause 13 PACE)

## **Briefing**

### ***Journalists***

Journalists generally have no protection in the Bill, and have no protection at all from interception, hacking, or any bulk powers. The one supposed safeguard is in clause 68,

which would require a public authority to apply to a Judicial Commissioner to confirm an authorisation to obtain communications data if the stated purpose of access is to identify or confirm a journalistic source. However, this is a significant reduction of the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE). The Bill fails to define a journalist, and offers a questionable definition of journalistic sources (cl. 68(7)) that is unlikely to meet the standard set by recent case law from ECtHR<sup>28</sup>.

In September 2014, it was revealed that the Metropolitan Police had used the RIPA internal authorisation route to access communications data of a journalist from The Sun newspaper as part of their “plebgate” inquiry, circumventing the well-established judicial process set out in the Police and Criminal Evidence Act 1984 (PACE). In response to public outcry, the Government updated the Acquisition and Disclosure of Communications Data Code of Practice, advising law enforcement that where an application to access the communications data of a journalist in order to determine the source of journalistic information is made, it must be via the PACE route. It is therefore extremely unclear why rather than replicated these protections in the Bill, the Government has seemingly sought to leave journalistic material subject to essentially no additional protection,

The procedure to be followed in PACE requires a hearing on notice in front of a judge - with both parties permitted to make legal representations. This is in recognition of the vital democratic importance in the confidentiality of journalistic material and in particular their source material, as protected by the right to freedom of expression in article 10 of the European Convention on Human Rights. Where possible, it is clearly in the interests of democracy that where journalistic material is sought by the state, the journalist has the opportunity to make their case to a judge. It is imperative that this vital safeguard is not circumvented by state agencies choosing to request interception (or hacking) warrants where an *inter partes* hearing will not apply rather than access information by more proportionate and restricted route that requires a full hearing. For this reason the amendment would require that where the information sought can be achieved via PACE without undermining the purpose of the investigation then the warrant must not be granted.

In addition to concerns about the democratic and human rights importance of protecting journalistic material and sources, the accessing of this information can also raise human rights concerns about the right to life. Suzanne Breen, the editor of Northern Ireland’s Sunday Tribune conducted interviews with members of the Real IRA, following which police sought to force her to give up her interview notes and other information, facing up to five

---

<sup>28</sup> *Guseva v Bulgaria* application no. 6987/07, 17 Feb 2015, para 38 and the cases cited.

years' imprisonment for failing to do so. However, she used Article 2 of the HRA – the right to life – to win her case, relying on clear evidence that, were she to hand over the material, she and her family would face attack by dissident Republican groups.

## **MPs**

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.”<sup>29</sup>*

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

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 held that the doctrine had been unilaterally rescinded by the Executive.<sup>31</sup> Liberty disputes this

---

<sup>29</sup> HC Deb 17 November 1966 Vol 736, columns 634-641.

<sup>30</sup> HC Deb 4 December 1997 Vol 302, Col 321.

<sup>31</sup> 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 warranting will apply with “particularly careful consideration” given

finding. The unequivocal statement made by Prime Minister Wilson back in 1966 was a constitutional convention protecting vital discourse between the people and their ultimate representatives, creating a legitimate expectation on the part of parliamentarians and their constituents that their correspondence was protected. However, there is currently no right of appeal against decisions of the IPT.

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 if the express purpose is the interception of constituency communications. Instead of securing an independent authorisation process, involving two politicians rather than one would make the process more political rather than less. It is difficult to see why Members of Parliament and other elected representatives should have confidence that “consultation” with the Prime Minister can act as a bulwark against unjustified surveillance of constituency communications. Liberty does not suggest that parliamentarians should be above the law, but in recognition of their unique constitutional role we advocate a strong legislative presumption against surveillance of elected representatives, that can only be rebutted in in clear and specific circumstances overseen by judicial commissioners.

## **Legally privileged material**

### **Amendment**

#### **Clause 25**

#### **Page 19, line 15 leave out Clause 25 and insert -**

- (-) A warrant under this Chapter, or under Chapter 1 of Part 6, may not authorise conduct undertaken for the purpose of doing anything in relation to—
- (a) a communication, insofar as the communication consists of matters subject to legal privilege;
  - (b) related communications data, insofar as the data relate to the communication of matters subject to legal privilege.

---

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.

(-) For the purposes of subsection (1), legal privilege means –

- (a) Communications between a professional legal adviser and his client or any person representing his client made in connection with the giving of legal advice to the client;
- (b) Communications between a professional legal adviser and his client or any person representing his client and any other person with or in contemplation of legal proceedings or for the purposes of such proceedings;
- (c) Items enclosed with or referred to in such communications and made:
  - i. In connection with the giving of legal advice or
  - ii. In connection with the contemplation of legal proceedings or for the purposes of such proceedings.
- (d) Communications made with the intention of furthering a criminal purpose are not subject to legal privilege.

(-) An application which contains a statement that the purpose of a warrant is to access communications made for the purpose of furthering a criminal purpose, but which would otherwise attract legal privilege must be considered by a Judicial Commissioner.

(-) A Judicial Commissioner may issue a warrant sought under subsection (3), if satisfied that:

- (a) There are reasonable grounds to believe that the communications are made with the intent of furthering a criminal purpose;
- (b) That the material is likely to be of substantial value to the investigation in connection with which the application is made; and
- (c) That the material concerned is likely to be relevant evidence;
- (d) Other proportionate methods of obtaining the information have been tried without success or were not tried because they were bound to fail
- (e) It is in the public interest that the warrant is granted, having regard to the
  - i. The benefit likely to accrue to the investigation and prosecution if the information is accessed
  - ii. The importance of the prosecution
  - iii. The importance of maintaining public confidence in the confidentiality of material subject to legal professional privilege,

(-) A code of practice issued under Schedule 6 must contain provision about—

- (a) the steps to be taken to minimise the risk of conduct undertaken pursuant to a warrant to which this section applies resulting in accidental acquisition of a communication, or communications data, falling within subsection (1);
- (b) the steps to be taken if it appears that such conduct has accidentally resulted in acquisition of such a communication or data.’

### **Effect**

This amendment provides interception warrants may not be authorised to intercept communications subject to legally privileged material, and sets out a special procedure to be followed by the Judicial Commissioner where it is believed that a communication between and lawyer and client may have been made to further a criminal purpose.

### **Briefing**

Legal privilege is an essential protection in a free society governed by the Rule of Law. The doctrine is intended to ensure fair trial integrity and ensure both defendants and civil claimants can communicate with their lawyers without inhibition. Legally privileged communications are those between a client and their lawyer which come into existence for the dominant purpose of being used for legal advice, or in connection with actual or pending litigation. The Bar Council reminded the Joint Committee scrutinising the Bill that, “*The privilege is that of the client, and failure to protect that right against the state amounts to a significant inroad into a long-standing principle, which has formed an important foundation of our rule of law*”.<sup>32</sup> Without assured confidentiality, clients feel unable to speak openly with their lawyers and may not know about the proper defences available to them, thus obstructing a fair trial. Breaching privilege can also obstruct justice by jeopardising the integrity of criminal trials, or giving the state an unfair advantage.<sup>33</sup> Legal privilege does not apply where client-lawyer communications are made in furtherance of a criminal activity.

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

---

<sup>32</sup> *Written Evidence on Investigatory Powers Bill* – Bar Council, 21 Dec 2015

<sup>33</sup> *Ibid.*

Abdel Hakim Belhaj alleges he is a victim of CIA-SIS rendition and torture and is attempting to hold the UK Government to account for this. During the course of legal proceedings and in the wake of the Snowden revelations, his lawyers came to fear that they were under surveillance. In the course of proceedings before the Investigatory Powers Tribunal the Government conceded that **“since January 2010 the policies and procedures for the interception/obtaining, analysis, use, disclosure and destruction of legally privileged material have not been in accordance with human rights legislation specifically Article 8(2) of the ECHR.”**<sup>34</sup> Instead, they allowed for legally privileged communications of between a victim of SIS-CIA rendition and torture and his lawyer to be targeted for surveillance. It is unacceptable that the Government could have used its surveillance powers to undermine attempts to hold it to account for its complicity in torture, but that is what existing legislation has permitted and this would remain permitted under the terms of the Bill.

The Bill therefore represents an important and timely opportunity to ensure statutory protection for LPP. However, the only ‘safeguard’ for protecting lawyers from targeted interception or hacking, or targeted examination following bulk interception or hacking – if the stated purpose is to intercept or examine material subject to legal privilege (not if the purpose is more generally investigative) – is that there are deemed to be “*exceptional and compelling*” circumstances.<sup>35</sup> This ‘safeguard’ is not accompanied by any objective threshold or definition in the Bill, and therefore is a subjective value judgement that provides no real protection or reassurance.

---

<sup>34</sup> “Government concedes policies on lawyer-client snooping were unlawful”, Reprive, 15 February 2015, available at - <http://www.reprive.org.uk/press/government-concedes-policeson-lawyer-client-snooping-were-unlawful/>

<sup>35</sup> See clauses 25, 100, 135 and 171

## **Interception taking place in certain institutions**

### **Amendment**

Clause 42, page 33, line 9, delete clause 42

Clause 43, page 33, line 31, delete clause 43

Clause 44, page 34, line 21, delete clause 44

### **Effect**

These amendments would delete clauses which permit the creation of additional interception powers in prisons (clause 42), psychiatric institutions (clause 43), and immigration detention facilities (clause 44).

### **Briefing**

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 these clauses permit for these additional regimes 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.

While we note that proposals in clause 42 relating to prisons and clause 43 relating to psychiatric institutions appear to broadly replicate provisions currently contained in RIPA, 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.

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 include individuals with significant mental health difficulties and asylum seekers fleeing persecution by their own state.

## **Service of warrants outside the UK**

### **Amendments**

Clause 35, Page 29, line 3, delete clause 35

Clause 36, page 29, line, 31, delete clause 36

### **Effect**

These amendments would delete provisions which purport to give interception warrants extraterritorial effect.

### **Briefing**

Clauses 35 and 36 replicate provisions created by the Data Retention and Investigatory Powers Act 2014. At the time DRIPA was passed, the Government sought to claim that RIPA had always had extraterritorial effect and these provisions were simply intended as clarification. This claim was both misleading and absurd. In general terms, legislation passed by the UK does not have direct effect in other jurisdictions, just as we would not expect the law of, say, France to apply automatically in the UK. For the Government to claim that RIPA had extraterritorial effect without it even stating so in the legislation made no sense. In A Question of Trust, this was confirmed:

*“Overseas service providers are generally unhappy with the assertion of extraterritoriality in DRIPA 2014, which they did not necessarily accept (despite the view of the UK Government) to have been implicit in the previous law and had not encountered in the laws of other countries. While legal compulsion was in principle preferable to voluntary compliance, it was thought that the unilateral assertion of extraterritorial effect would be met by blocking statutes, was not “scalable to a global approach” and was viewed as “a disturbing precedent” for other, more authoritarian countries.”<sup>36</sup>*

The Reviewer’s report notes that when countries seek to enforce legislation extraterritorially these powers may come into conflict with legal requirements in the country in which companies being asked to comply with a legal request is based or stores information. Companies explained to the reviewer that they did not consider it was their role to arbitrate between conflicting legal systems. Liberty completely agrees: the protection of vital human

---

<sup>36</sup> Paragraph 11.17.

rights should not be left to the goodwill and judgement of a company. The report also notes principled concerns from companies:

*“They expressed concerns that unqualified cooperation with the British government would lead to expectations of similar cooperation with authoritarian governments, which would not be in their customers’, their own corporate or democratic governments’ interests.”<sup>37</sup>*

The alternative, most appropriate – and probably most successful way – for Government to seek to access information held overseas or by companies based overseas is to extend and improve the use of Mutual Legal Assistance Agreements (MLATs) with other States. A Question of Trust concluded that the Government should *“seek the improvement and abbreviation of MLAT procedures, in particular with the US Department of Justice and the Irish authorities”* and *“take a lead in developing and negotiating a new international framework for data-sharing among like-minded democratic nations.”<sup>38</sup>* The report also refers to the work of Sir Nigel Sheinwald as Special Envoy to the Prime Minister on law-enforcement and intelligence data sharing and suggests that Sir Nigel’s will be *“the decisive voice”* on this matter. On 11 June 2015, the Prime Minister’s written statement responding to the Anderson review noted: *“the Government will be taking forward Sir Nigel’s advice, including pursuing a strengthened UK-US Mutual Legal Assistance Treaty process and a new international framework. As David Anderson recognises in his report, updated powers, and robust oversight, will need to form the legal basis of any new international arrangements.”<sup>39</sup>*

However the Bill is completely silent on this promised new framework and instead returns to the lazy and dangerous assertion of extraterritorial effect. It is baffling and concerning that a piece of legislation which purports to be comprehensive in this area is silent on the significant issue of how surveillance operates in the global communications environment, despite the fact that the need for reform in this area has been acknowledged by the Prime Minister.

---

<sup>37</sup> Paragraph 11.24.

<sup>38</sup> Recommendation 24.

<sup>39</sup> House of Commons: Written Statement (HCWS27)

## **Intercept as evidence**

### **Amendment**

Page 37, line 31, delete clause 48

### **Effect**

This amendment would provide for the use of intercept as evidence in criminal trials.

### **Briefing**

Clause 48 maintains the section 19 RIPA bar on admissibility of interception material in criminal trials and Inquiries Act 2005 proceedings. There is not justifiable reason for maintaining the bar on intercept admissibility. The first consequence of lifting the ban would be an increase in successful prosecutions for serious offences. The latest Privy Council review into the issue, which reported in December 2014, concluded that a properly funded use of intercept material as evidence may result in a “*significant increase in the number of successful prosecutions.*”<sup>40</sup>

Removal of the ban would also ensure that criminal defendants’ rights are not breached in cases where interception has formed part of the investigation. The ECtHR has ruled that failure to disclose intercept evidence in certain circumstances will breach Article 6 ECHR.<sup>41</sup> Furthermore, the current ban has fuelled a corruption of domestic fair trial standards and abusive counter-terrorism laws, from control orders to TPIMs, to the corrosive growth of Closed Material Procedures across our justice system.

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

Successive Government-initiated reviews over the past two decades have concluded that intercept should be made admissible. A remaining objection from the Agencies seems to be

---

<sup>40</sup> See *Intercept as Evidence*, December 2014, Page 23.

<sup>41</sup> *Natunen v Finland* (Application no. 21022/04).

on cost grounds. No doubt the requirement to transcribe and disclose intercept evidence would impose an additional burden on the authorities – as do all requirements to ensure that the criminal process is effective, efficient and just. But it would only be material that fulfills the test for disclosure at trial that would need to be presented.<sup>42</sup> Given the current volumes of interception it would likely be only an infinitesimal fraction, and could have the salutary effect of focusing the authorities' minds on the primacy that should be given to criminal investigations, prosecutions and trials over speculative, intelligence gathering fishing expeditions.

---

<sup>42</sup> Section 3 of the Criminal Procedure and Investigations Act 1996.

## **Whistle blower protection**

### **Amendment**

Clause 51, page 41, line 19, insert new subsection (4) –

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

### **Effect**

This amendment would provide a defence to the criminal offence of disclosure in relation to a warrant issued under this Part. 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.

### **Briefing**

By their very nature, surveillance powers are used in secret, with the vast majority of those subject to their use never realising that surveillance has taken place. This means that it is vital that there are in place sufficient checks, balances and safeguards to ensure that these powers are used appropriately. As part of this, it is essential to ensure that those who in one way or another witness or have knowledge that abuse or mistakes are taking place are able to bring those to the attention of individuals capable of addressing them. This may include bringing information to public attention.

Provisions in Clause 51 which criminalise disclosure of information relating to the use of interception powers risk shutting down a vital route to ensuring accountability for the use of surveillance powers. They help to enshrine an unnecessarily secretive culture which punishes those who seek to reveal wrongdoing rather than encourage a robustly honest working environment. Individuals who wish to make reports – even internally – of unlawful or otherwise inappropriate behaviour will know that taking steps to do the right thing could expose them to significant criminal sanction. In a Bill that seeks to bring new levels of transparency to the UK's surveillance regime, this is clearly both undemocratic and unacceptable.

**Sara Ogilvie**