LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

Liberty's summary of the Investigatory Powers Bill for Second Reading in the House of Lords

June 2016

About Liberty

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

Liberty Policy

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

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

Contact

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

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

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

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

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

Background

1. The Investigatory Powers Bill will have its Second Reading in the House of Lords on Monday 27 June 2016.

2. Liberty has been calling for a new investigatory powers framework for over a decade. In a world where the threat of terror and other serious crime is never far, surveillance powers play an important part in helping the agencies of the state to protect our human rights. Liberty absolutely supports the provision of targeted, proportionate and necessary investigatory powers which are exercised subject to robust safeguards. We also agree that in a changing world, our law enforcement and intelligence agencies must have powers that recognise and reflect the modern nature of our communications.

3. Evidence increasingly shows that in order to keep us safe, these investigatory powers must be targeted. Intelligence whistle-blowers have warned that the agencies are drowning in data and in a recent document from 2010 uncovered in the Snowden leaks the UK Government admitted that the extent of mass surveillance undertaken by their agencies posed a risk to human life, stating: *"This creates a real risk of 'intelligence failure' i.e. from the Service being unable to access potentially life-saving intelligence from data that it has already collected."*[1] In the US, a Government commissioned review into their domestic bulk phone records programme found it did not contribute to a single counter-terrorism investigation in any way that targeted methods could not have done – so Congress shut it down.

4. The fact that all major terrorist attacks in recent years have involved individuals believed to be known to the state agencies supports this view. Following the tragic death of Fusilier Lee Rigby in 2013, the Intelligence and Security Committee uncovered a catalogue of missed opportunities by the intelligence agencies. The report explains that prior to events of May 2013 both Michael Adebolajo and Michael Adebowale – subsequently convicted of the murder – were known to the security services, but they weren't treated as priority suspects. The warning signs were there, but over the course of several years - and seven Agency operations - landline telephone records went unchecked, links with other suspected terrorists weren't followed up, and warrants for targeted, intrusive surveillance were not requested in

[1] https://theintercept.com/2016/06/07/mi5-gchq-digint-surveillance-data-deluge/

circumstances which the Committee describes as 'surprising'. When it was finally decided to place Adebowale under surveillance, there was a huge delay in granting authorisation for this request. The report reveals that, had this request been dealt with in a timely manner, at least one of the men would have been under surveillance in the days leading up to the murder. Those involved in the atrocities in Brussels earlier in 2016 were known to be linked to those who had previously committed murder in the streets of Paris.

5. Human Rights law provides guidance as to the shape that a human rights compliant surveillance framework must take. Recent Strasbourg judgments, handed down since the publication of the IP Bill, make clear that "*a measure of secret surveillance can be found as being in compliance with the Convention only if it is strictly necessary, as a general consideration for the safeguarding the democratic institutions and moreover if it is strictly necessary as a particular consideration, for the obtaining of vital intelligence in an individual operation."*[2] In circumstances where a measure is strictly necessary *"in view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse."*[3] The minimum safeguards laid down by Strasbourg include (i) the nature of offences which may give rise to a surveillance order and the definition of the categories of people liable to have their communications surveilled[4] (ii) verifiable reasonable suspicion thresholds for the authorisation of investigatory powers[5] (iii) the independent and substantive judicial authorisation of warrants (and a rejection of political authorisation)[6] and a presumption in favour of post-notification to those subjected to such powers.[7]

6. It is clear that the requirements of our security and our privacy both demand targeted surveillance, where strictly necessary, subject to clear checks and balances. Keeping us safe and keeping us free are not opposing and incompatible positions, but in fact require the same approach. But instead of heeding the lessons from past horrors and taking guidance from the Court of Human Rights, the Government has brought forth

[2] Szabo and Vissy v Hungary, 12 January 2016, para 73.
[3] Szabo and Vissy v Hungary, 12 January 2016, para 57.
[4] Szabo and Vissy v Hungary, 12 January 2016, para 56.
[5] Zakharov v Russia, 4 December 2015, ECHR, para 260.
[6] Szabo and Vissy v Hungary, 12 January 2016, para 75.
[7] Szabo and Vissy v Hungary, para 86.

legislation that enshrines mass rather than targeted surveillance and is devoid of substantive safeguards to protect against mistakes and abuse.

7. It has been argued that this Bill simply puts on a clear statutory basis powers that already existed and were exercised by the security and intelligence agencies in secret. In fact, the use of mass surveillance powers was not authorised by the previous legislation and constituted powers that were taken, not granted. It is a complete inversion of democratic process to say that since those powers have been taken and used unlawfully, the only thing that can now be done is to enshrine them in legislation. The Home Secretary also argues that the Bill provides for "world leading oversight". Again, this claim bears no scrutiny. The Bill's safeguards are half-hearted, inadequate, and do not come close to implementing the requirements of recent case law.

8. There is no doubt that new legislation is needed, but the fact that it is needed must not be used by the Government to pressure parliamentarians into waving it through without challenge or improvement. This is a once in a generation opportunity to provide a framework that will keep us safe and free. It should not be used simply to nod through unlawful practices.

9. During the course of the scrutiny of the Bill in the House of Lords, we urge parliamentarians to:

    - Reject bulk and thematic surveillance in favour of surveillance of a clearly defined target
    - Require a threshold for the use of surveillance powers, set at reasonable suspicion of involvement in a serious crime
    - Insert a definition of national security
    - Provide for a single-stage judicial authorisation process
    - Provide for institutionally separate authorisation and oversight bodies
    - Require post-notification where it will not damage the public interest
    - Insert protections for confidential and privileged correspondence
    - Protect encryption
    - Require audit trails for the use of hacking powers
    - Reform the Investigatory Powers Tribunal