LIBERTY

PROTECTING CIVIL LIBERTIES
PROMOTING HUMAN RIGHTS

# Liberty's briefing on Part 5 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

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

**Introduction**

Liberty welcomes the opportunity to brief on Part 5 of the Investigatory Powers Bill for Committee Stage in the House of Commons.

In this briefing we propose amendments to:

- Ensure that an examination warrant is required to look at *all* data gathered under bulk equipment interference warrants
- Tighten the subject matter for warrants to ensure that individuals, organisations, and locations are all specified rather than loosely described/alluded to
- Give power to issue warrants to judicial commissioner rather than Secretary of State and law enforcement chiefs
- Require a threshold of reasonable suspicion of a criminal offence in order for warrant to be granted
- Remove economic wellbeing of UK as separate purpose for grant of a warrant
- Strengthen proportionality protections, including requiring that the Judicial Commissioner conducts a technical review of implications of each hack for collateral intrusion and threat to integrity of communications systems and computer networks
- Require that urgent warrants are only granted in an emergency situation for the protection of life or prevention of injury or where the physical integrity of the UK is threatened
- Limit duration of warrants to one month
- Replicate current legislative protections for confidential and privileged communications
- Remove duty of telecommunications operators to assist with hacks
- Require that material gained through hacking is only shared with overseas partners in accordance with a treaty
- Delete provisions to serve warrants extraterritorially
- Provide for whistle-blower protection
- Require that warrants only authorise conduct that relates to the offence which initially provided the purpose for the hack (replicating PACE provisions for search)
- Provide for a proper audit trail, particularly to protect the integrity of evidence for use in trials
- Create presumption of after the fact notification by JC

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

**Background**

Part 5 of the Bill makes provision for targeted hacking, euphemistically termed "*equipment interference*". There are two types of warrant: "targeted equipment interference warrants" and "targeted examination warrants", the latter of which can be issued in relation to material obtained via the bulk hacking powers in Part 6. Secretaries of State (and in certain circumstances Scottish Ministers[1]) can issue both types of warrants to the intelligence agencies and the Chief of Defence Intelligence where he or she considers it necessary and proportionate on the three main grounds. In contrast to the scheme for interception, the power to issue hacking warrants is also extended to chief constables, deputy chief constables, assistant chief constables and senior HMRC officers on application from junior HMRC and police officers 'for the purpose of preventing and detecting serious crime".[2]

A hacking warrant authorises a person to interfere with any equipment for the purpose of obtaining "communications", "equipment data", or "any other information".[3] There are no limits as to what information could be obtained. Information can be obtained by *"monitoring, observing or listening to a person's communications or other activities and recording anything that is monitored, observed or listened to*".[4]

Warrants last for six months and can be renewed potentially indefinitely. Warrant applications will be subject to the weak system of judicial review. Warrants can be modified by ministers without the approval of a JC and modification can include changing the name,

[1] Clause 92.
[2] The majority of police forces can only hack devices and networks with a "British Isles connection" (although NCA has global powers) and this requirement is made out if any of the conduct, equipment interfered with or private info sought is in the British Islands.

[3]Equipment data is defined at clause 89.

[4] Clause 88(4).

descriptions and scope of the warrant.[5] Chief constables are required to have their decisions to modify warrants reviewed by a JC, unless they consider the modification to be urgent.[6]

*New power*

Hacking is prima facie unlawful as a matter of domestic criminal law and before 2015, hacking was not avowed as an intelligence agency or law enforcement capability. This only changed in February 2015 when the Home Office published a consultation on a Draft Code of Practice for Equipment Interference in response to Privacy International and others' claim in the IPT concerning the hacking disclosures within the Snowden documents. This Code referred only to the intelligence agencies and did not make reference to police hacking powers, which were not officially acknowledged until the publication of the draft Bill.

There is currently no clear or accessible legal framework governing the hacking of electronic devices and networks making current use of the practice likely unlawful on grounds that it is not in accordance with law to comply with the requirements of the HRA. Government claims the Agencies' hacking powers derive from broad and vague enabling powers contained in sections 5 and 7 of the Intelligence Services Act 1994. Yet the enabling power bears no resemblance to the power now contained in the Bill and the legislation pre-dates the powerful electronic hacking capabilities now utilised.

Police apparently derive hacking powers from section 93 of the Police Act 1997 - yet when the head of the Metropolitan Police's Technical Unit, Paul Hudson, gave oral evidence to the Draft Bill Committee, he seemed unsure as to legal basis for the Met's powers. Section 93 similarly bears no resemblance to the powers now contained in the Bill and even as recently as 2010, the related Code of Practice on "Covert Surveillance and Property Interference" referred only to physical property interference and not to electronic hacking. Despite this, in a potentially explosive admission before the Draft Bill Committee, Hudson disclosed that the Met uses equipment interference in a "majority" of serious crime cases. Over the past few years, various media outlets have sought to investigate hacking by the police. The Times and Sky News have reported that the Met has purchased and begun using "IMSI catchers" and when Hacking Team (a private company offering hacking services to Governments worldwide) was recently itself hacked, it was revealed that the Met, NCA and Staffordshire police had shown interest in their products before apparently getting cold feet. Until the publication of the draft Bill the Met had adopted a NCND approach to hacking.

[5] Investigatory Powers Bill 2016, clause 104
[6] Investigatory Powers Bill 2016, clause 106 subsection (3)(b)

*Intrusiveness of hacking*

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

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

*Security concerns*

When malware is deployed, there is often a risk of contagion, both overseas and at home. This was dramatically demonstrated by the Stuxnet virus, believed to be an American-Israeli cyberweapon, which intended to hack a single Iranian uranium enrichment facility but infected energy giant Chevron among many other companies as well as Microsoft PCs around the world. The risks of hacks spreading 'in the wild' cannot be overstated: Professor of Security Engineering at Cambridge University, Ross Anderson wrote to the Science and Technology Select Committee, *"it is only a matter of time before interference with a safety-critical system kills someone".* There is also the risk that hacks can malfunction, with severe consequences for critical infrastructures and even international relations. For example, Snowden revealed that NSA hacking malfunctions were responsible for the outage of Syria's internet in 2012, which may have caused simultaneous flight-tracking issues, and led government and opposition forces to erroneously blame each other for the incident.

Given the potential damage to computer security and corresponding vulnerability to criminal elements that results from hacking, the use of this technology poses clear risks both to those it is used against and the wider population, in a way that engages more rights than traditional forms of communications surveillance. Parliamentarians should consider the cost of widespread hacking by the authorities. Hacks create and maintain permanent vulnerabilities that can be further exploited by criminal elements, raising the potential for hacking to be counterproductive in the fight against serious crime. Cybercrime already costs the UK £34bn per year, and these proposed powers seem certain to ensure that this cost rises.

*Repercussions for fair trials*

As hacking by its nature requires the alteration of content on a target device or network, it also raises new questions concerning the potential for electronic surveillance to undermine the integrity of a device or material located on a device that may later be sought to be used in evidence in criminal and civil trials. There is presently no specific regulation of the use of hacking product in criminal trials, and none presented in either the Bill or the Code of Practice.

The present position at common law is that the prosecution are under a duty to disclose all material in their possession or that they have inspected which may reasonably be considered capable of undermining the case against the defendant. Following the scandal concerning the non-disclosure of the identity of undercover police officers during the trial of Ratcliffe-on-Soar protesters, that principle now extends to material relating to the manner in which evidence is obtained where such material might support an argument that its acquisition has resulted in unfairness or abuse. The Rose Report into the Ratcliffe-on-Soar Power Station Protest found that the CPS and the police had together failed to discharge the prosecution's disclosure duties.

In recognition of the unique potential of hacking capabilities and to avoid future miscarriages of justice and collapsed trials, the Bill should contain specific proposals to ensure audit trails and police disclosure where prosecutions result from investigations that utilise hacking capabilities.

**Warrants under this part: definitions of data**

Amendment

Clause 88, page 66, line 38, delete ‘other information’ and insert ‘other specified data’

Effect

This amendment seeks to more clearly outline what material may be obtained by hacking.

Briefing

The Bill grants extremely broad powers to obtain “any information” through hacking. Yet in order for the warrant issuing body to conduct a thorough analysis of necessity and proportionality and reduce collateral intrusion, it is imperative that warrants specify which information is permitted to be obtained.

Amendment

Clause 88, page 67, line 40, delete ‘other than material which is – ‘and delete subclauses (a) and (b).

Effect

This amendment requires that an examination warrant is required for the examination of all data, removing the exception of equipment data and the broad category of ‘not private information’ which is collected under bulk warrants.

Amendment

Clause 89, page 68, line 13, delete ‘disregarding any meaning arising from the fact of the communication or the existence of the item of information or from any data relating to that fact’.

Effect

This amendment removes provision that seeks to insert a legal assertion that the fact of a communication and other data have no meaning.

Briefing

Historically communications data was considered much less revealing than the content of the communication and consequently the protections offered to communications data under RIPA are even weaker than those existing in the interception regime. However as communications have become increasingly digital, the data generated is much more revealing and copious than before, allowing the state to put together a complete and rich

picture of what a person does, thinks, with whom, when and where. Often, communications data can be of more use than content: it is vast, easy to handle, analyse and filter; and, it tends to be collected in a consistent manner.

As the Bill currently stands, clause 88 (9) would allow for the examination of potentially vast amounts of data on people in Britain that has been obtained under a bulk equipment interference warrant, as vague categories of data (88 (9)(a) and (b)) are asserted to have no meaning. ‘Data’ relating to the fact of a communication or the existence of information does indeed have meaning, and must not be exempt from privacy protections afforded to other categories of data.

**Subject matter of warrants**

Amendment

Clause 90, page 68, line 24, delete subclause (b)

Clause 90, page 68, line 33, delete subclause (f)

Clause 90, page 68, line 35, delete subclause (g)

Clause 90, page 68, line 38, delete subclause (h)

Clause 101, page 78, line 21, delete lines 21-27

Clause 101, page 79, line 3, delete lines 3-7

Clause 101, page 79, line 8, delete lines 8-12

Clause 101, page 79, line 13, delete lines 13-18

Effect

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

Amendment

Clause 90, page 68, line 41, insert new clause 1A:

1A: A targeted equipment interference warrant may only be issued in relation to any of the matters that fall under subsection (1) if the persons, organisations or location to which the warrant relates are named or otherwise identified.

Effect

This amendment would ensure that all targets of hacking are properly named or otherwise identified.

Amendment

Clause 90, page 68, line 44, delete subclause (b)

Clause 90, page 69, line 1, delete subclause (d)

Clause 90, page 69, line 3, delete subclause (e)

Clause 101, page 79, line 31, delete lines 31-36

Clause 101, page 80, line 3, delete lines 3-6

Clause 101, page 80, line 8, delete lines 8-12

Effect

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

Amendment

Clause 90, page 69, line 4, insert new clause (2A) –

2A A targeted examination warrant may only be issued in relation to any of the matters that fall under subsection (2) if the persons, organisations or location to which the warrant relates are named or otherwise identified.

Effect

This amendment would ensure that all targets of hacking are properly named or otherwise identified.

Briefing

Clause 90 provides for thematic hacking warrants which amount to general warrants to hack groups or types of individuals in the UK. Hacking is not restricted to equipment belonging to, used by or in possession of particular persons. Instead the subject matter of warrants can target equipment "*belonging to, used by or in the possession of a particular person or organisation*" or "*a group of persons who share a common purpose or who carry on, or may carry on, a particular activity*" or more than one person or organisation "*where the interference is for the purpose of a single investigation or operation."* A hacking warrant can further authorise hacking "*equipment in a particular location*" or "*equipment in more than one location, where the interference is for the purpose of the same investigation or operation*" or "*equipment that is being, or may be used, for the purposes of a particular activity or activities of a particular description*" as well as testing, developing or maintaining capabilities. The ISC

reported that, "*the Director of GCHQ suggested that, hypothetically, a Targeted EI warrant could cover a target as broad as an entire hostile foreign intelligence service".* The breadth of targeted hacking warrants was "*a concern recognised by the Director of GCHQ who noted that* 'the dividing line between a large-scale targeted EI and bulk is not an exact one'".[7]

In addition, the Draft Equipment Interference Code of Practice permits the targeting of people who are "not of intelligence interest".[8] It is difficult to foresee a more enabling and open-ended framework of the scope of domestic hacking capabilities. Hacking is by its nature much more prone to collateral intrusion than traditional forms of surveillance. IMSI catchers can for example pick up stored content of all mobile phones in a particular area. If use of the capability is to stand a chance of meeting the UK's human rights obligations, it is even more imperative that the legal framework for hacking requires specificity of targets.

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

**Judicial authorisation**

Amendment

Clause 91, page 69, line 6, after ‘Power’ insert ‘of Judicial Commissioners’; delete ‘: the Secretary of State’

Clause 91, page 69, line 7, delete ‘The Secretary of State’ and insert ‘Judicial Commissioners’ (and repeat on lines 9, 11, 14).

Clause 91, page 69, line 17, delete subclause (d).

Clause 91, page 69, line 20, delete ‘the Secretary of State’ and insert ‘Judicial Commissioners’ (and repeat on lines 22).

Clause 91, page 69, line 31, delete ‘The Secretary of State’ and insert ‘Judicial Commissioners’ (and repeat on lines 33, 35, 38).

Clause 91, page 69, line 43, delete subclause (d).

Clause 91, page 70, line 2, delete ‘Secretary of State‘ and insert ‘Judicial Commissioner’ (and repeat on line 24).

Clause 93, page 71, line 21, ‘Secretary of State‘ and insert ‘Judicial Commissioner’ (and repeat on lines 23, 25, 28).

Clause 93, page 71, line 31, delete subclause (d).

Page 72, line 18, delete clause 95.

Page 74, line 36, delete clause 97.

Effect

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

Amendment

Clause 91, page 69, line 25, delete subclause (b).

Clause 91, page 69, line 29, delete ‘For the power of Scottish Ministers to issue a targeted equipment interference warrant, see section 92’.

Clause 91, page 69, line 46, delete subsection (4).

Clause 91, page 70, line 23, delete subsection (9).

Page 70, line 26, delete clause 92.

Effect

These amendments would remove the responsibility of Scottish ministers to issue warrants for targeted equipment interference and targeted examination within Scotland, replacing the dual political authorisation processes with a single judicial authorisation process for all targeted equipment interference warrants and targeted examination warrants within the UK.

Amendment

Page 72, line 35, delete clause 96

Clause 91, page 69, line 6, after 'intelligence services' insert 'and law enforcement chiefs'

Clause 101, page 78, line 2, after 'intelligence service' insert 'or to a law enforcement chief'

Clause 101, page 78, line 6, delete subsection (c)

Effect

These amendments would remove the power of law enforcement chiefs to issue warrants within their own respective law enforcement bodies. This amendment would complement the amendment to give warrantry powers to Judicial Commissioners.

Briefing

The Bill's authorisation process for hacking warrants grants the Secretary of State the power to issue warrants to the intelligence services 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', in particular given the exceptionally intrusive and potentially destructive nature of hacking. 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.

Recently, the ECtHR ruled in *Roman Zakharov v Russia* that the Russian regime for interception violated Article 8. The Court highlighted that while Russian law requires prior judicial authorisation for interception measures, Russian judges in practice only apply purely

formal criteria in deciding whether to grant an authorisation, rather than verifying the necessity and proportionality of imposing such measures.[9] Strasbourg case law is clear on the need for a fully independent body, with sufficient expertise and agency to engage in a review of the evidence put forward to justify a surveillance warrant.

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

**Purposes for which warrant granted**

Amendment

Clause 91, page 69, line 17, delete subclause (d) and insert new subclause (d) –

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

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

Clause 93, page 71, line 31, delete subclause (d) and insert new subclause (d) –

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

Effect

These amendments would introduce a requirement that warrants are only granted where there are reasonable grounds for believing material to be obtained will be of substantial value to the investigation or operation, and requires a threshold of reasonable suspicion that a serious criminal offence has been committed in order for a warrant to be granted.

Amendment

Clause 91, page 70, line 26, add new subclause (10) –

> (10) A warrant may only authorise targeted equipment interference or targeted examination as far as the conduct authorised relates –
>
> (a) to the offence as specified under (5)(b), or
>
> (b) to some other indictable offence which is connected with or similar to the offence as specified under (5)(b)

Effect

This amendment would require that a warrant only authorises conduct in relation to the offence for which the warrant was sought, or other similar offences.

Briefing

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

Amendment

Clause 91, page 70, line 9, delete subclause (5)(c) and 91 (6).

Effect

This amendment would refine the purposes for which a targeted examination warrant can be issued to reflect the ISC's policy recommendation that 'economic wellbeing' is subsumed within a formal definition of national security on the face of the Bill.

Briefing

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[10] and economic well-being[11]; the ISC further recommended that economic well-being should be subsumed within a national

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

security definition, finding it "*unnecessarily confusing and complicated"*.[12] The ISC queried both the Agencies and the Home Office on this point but reported that '*neither have provided any sensible explanation'*.[13] 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.

[12] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J (i)
[13] Ibid.

**Confidential and privileged material**

Amendment

Page 71, line 40, delete clause 94 and insert new clause 94 –

94: Confidential and privileged material.

(1) Where any conduct under this Part will cover or is likely to cover special procedure material, or relates to individuals handling special procedure material, the application must contain –

a. A statement that the conduct will cover or is likely to cover special procedure material, or relates to individuals handling special procedure material, and

b. An assessment of how likely it is that the material is likely to cover special procedure material.

(2) Where any conduct under this Part is likely to cover excluded procedure material, or relates to individuals handling excluded procedure material, the application must contain –

a. A statement that the conduct will cover or is likely to cover excluded procedure material, or relates to individuals handling excluded procedure material, and

b. An assessment of how likely it is that the material is likely to cover excluded procedure material.

(3) Where a warrant issued under this Part will cover or is likely to cover special procedure material, or relates to individuals handling special procedure material, the procedure set out at section 5 below must be followed

(4) Where a warrant issued under this Part will cover or is likely to cover excluded procedure material, or relates to individuals handling excluded procedure material, the procedure set out at section 6 below must be followed

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

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

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

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

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

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

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

c. the democratic importance of freedom of expression under article 10 ECHR to grant the warrant; or

d. the democratic interest in the confidentiality of correspondence with members of a relevant legislature; or

e. the importance of maintaining public confidence in the confidentiality of material subject to legal professional privilege.

(6) 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

(7) 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.

(8) 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

(9) Excluded material procedure has the same meaning as section 11 of the Police and Criminal Evidence Act 1984

(10) A warrant under this Part may not authorise any conduct undertaken for the purpose of accessing any material relating to matters subject to legal privilege

(11) For the purposes of subsection (10), legal privilege means –

(a) Communications between a professional legal adviser and their client or any person representing their client made in connection with the giving of legal advice to the client;

(b) Communications between a professional legal adviser and their client or any person representing their 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.

(12) Where the purpose of the warrant is to conduct interference to obtain material that would normally be subject to legal privilege but that falls within subsection (11)(d), the interference and examination conduct authorised must relate –

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

(5) to some other indictable offence which is connected with or similar to the offence as specified under (5)(a)

Page 76, line 39, delete clause 100.

Effect

These amendments would maintain the PACE protections for special procedures and excluded material that are currently observed in law.

Briefing

The concept of members of the legislature, lawyers, or journalists having their devices hacked is alarming, making potentially vast amounts of highly confidential and privileged information available to the state.

In keeping with the inconsistent and weak protections, journalists receive no protection from hacking in the Bill.

At present the clause 94 'safeguard' for MPs regarding targeted hacking applies only if the express purpose of the intrusion is to obtain of communications relating to constituency matters – not national matters or private/other matters. The 'safeguard' requires that the Secretary of State 'consults' the Prime Minister before authorising activity. Given recent revelations of police spying on MPs[14], and the Prime Minister's frequent assertions that the Leader of the Opposition is a national security threat, it is important to have robust independent safeguards, such as those under PACE, implemented by a Judicial Commissioner.

Similarly, the only 'safeguard' for protecting lawyers from targeted hacking, or targeted examination following bulk interception or hacking, applies if the stated purpose is to intercept or examine material subject to legal privilege (not if the purpose is more generally investigative). The 'safeguard' is that there must be deemed to be "*exceptional and compelling"* circumstances. 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.

An authorisation to hack a device creates a clear risk that the content of a lawyer's entire email inbox will be taken or, even worse, that the way to access this information will be to take the contents of the server of a whole law firm. It is inevitable that legally privileged communications will be collateral damage and risks the right to a fair trial of a significant number of individuals. It is essential that the highest safeguards are afforded to hacks involving lawyers.

As a minimum, it is essential that PACE protections are maintained, as per these amendments, to ensure that intrusion is strictly limited to circumstances where serious crime

[14] *Police face questions over covert monitoring of Jeremy Corbyn and other MPs* – Rob Evans, The Guardian, 2 October 2015. http://www.theguardian.com/uk-news/undercover-with-paul-lewis-and-rob-evans/2015/oct/02/police-facing-hard-questions-over-covert-monitoring-of-jeremy-corbyn-and-other-mps

is suspected. It is also important that protections are equivalent to those currently in PACE in order to ensure that law enforcement agencies do not seek to circumvent the well-established PACE procedures. Hacking authorisations will enable law enforcement to access information that may previously have only been accessible via a search warrant which requires independent judicial authorisation given on notice and with representations. It is not difficult to imagine which route will be taken. In the recent Plebgate scandal, it was revealed that police had in fact chosen to use RIPA rather than PACE powers to access information about journalistic sources. Creating this legal loophole will undermine over thirty years of statutory protections for police searches.

**Targeted Equipment Interference may only be authorised under this Part.**

Amendment

Clause 91, page 70, line 26, insert new subclause (10) –

(10) Targeted equipment interference is only lawful if authorised under this Act.

Effect

This amendment would require that targeted equipment interference ceases to be conducted under the Intelligence Services Act 1994, the Police Act 1997, or any other prior legislation. This would ensure that equipment interference always benefits from the safeguards and oversight that may be provided for in this Bill. It would also improve public accountability and clarity of the state's powers.

Briefing

The ISC's report on the draft Bill expressed concern that "*the Agencies also conduct several forms of EI that are not provided for under the draft Bill"* meaning that "*certain IT operations will require a different standard of authorisation (without Judicial Commissioner approval) than Computer Network Exploitation and that similar activities undertaken by the Agencies will be authorised under different pieces of legislation".* The ISC concluded that the Bill therefore "*fails to achieve transparency in this area and effectively means that such operations remain 'secret' and thus not subject to clear safeguards*". Furthermore, the ISC "*recommends that all IT operations are brought under the provisions of the new legislation (…) with the same authorisation process and the same safeguards*". Given the failure of the Home Office to bring all EI powers under this legislation, this amendment reflects the recommendation of the ISC that all types of EI should be governed under one clear piece of legislation.

**Proportionality and technical assessment**

Amendment

Clause 91, page 70, line 18, delete ‘whether what is sought to be achieved by the warrant could reasonably be achieved by other means’ and insert new subclause –

(a) the requirement that other proportionate methods of obtaining the material have been tried without success or have not been tried because they were assessed to be bound to fail, and
(b) the requirement that a risk assessment has been conducted by the Investigatory Powers Commissioner’s technical advisors with regard to the specific equipment interference proposed, accounting for –
    i. the risk of collateral interference and intrusion, and
    ii. the risk to the integrity of communications systems and computer networks, and
    iii. the risk to public cybersecurity.

Clause 93, page 71, line 35, delete ‘whether what is sought to be achieved by the warrant could reasonably be achieved by other means’ and insert new subclause –

(a) the requirement that other proportionate methods of obtaining the material have been tried without success or have not been tried because they were assessed to be bound to fail, and
(b) the requirement that a risk assessment has been conducted by the Investigatory Powers Commissioner’s technical advisors with regard to the specific equipment interference proposed, accounting for –
    a. the risk of collateral interference and intrusion, and
    b. the risk to the integrity of communications systems and computer networks, and
    c. the risk to public cybersecurity.

Clause 96, page 74, line 13, delete ‘whether what is sought to be achieved by the warrant could reasonably be achieved by other means’ and insert new subclause –

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

(b) the requirement that a risk assessment has been conducted by the Investigatory Powers Commissioner's technical advisors with regard to the specific equipment interference proposed, accounting for –

i. the risk of collateral interference and intrusion, and

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

iii. the risk to public cybersecurity.

Effect

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

Briefing

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

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

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

**Power to issue hacking warrants to law enforcement**

Amendment

Clause 96, page 72, line 35, delete ‘officers’ and insert ‘chiefs’.

Clause 96, page 72, line 36, delete ‘law enforcement chief described in Part 1 or 2 of the table in Schedule 6’ and insert ‘Judicial Commissioner’.

Clause 96, page 72, line 37, delete ‘person who is an appropriate law enforcement officer in relation to the chief’ and insert ‘law enforcement chief described in Part 1 of the table in Schedule 6’.

Clause 96, page 72, line 40, delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’.

Clause 96, page 72, line 42, delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’.

Clause 96, page 73, line 1, delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’.

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

Clause 96, page 73, line 7, delete ‘law enforcement chief described in Part 1 of the table in Schedule 6’ and insert ‘Judicial Commissioner’

Clause 96, page 73, line 8 delete ‘person who is an appropriate law enforcement officer in relation to the chief’ and insert ‘law enforcement chief described in Part 1 of the table in Schedule 6’

Clause 96, page 73, line 10 delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’

Clause 96, page 73, line 14, delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’

Clause 96, page 73, line 17, delete ‘law enforcement chief’ and insert ‘Judicial Commissioner’

Clause 96, page 73, line 20, leave out (d)

Clause 96, page 73, line 23, leave out (3)

Clause 96, page 73, line 29, leave out (b) and (c)

Clause 96, page 73, line 35, after ‘Where’ insert ‘an application for an equipment interference warrant is made by a law enforcement chief and’

Clause 96, page 73, line 39, leave out (6) – (10)

Clause 96, page 74, line 16, leave out (12) – (13)

Consequential amendment

Schedule 6, page 213, line 15, leave out Part 2

Effect

These set of amendments would remove the power to issue equipment interference warrants from law enforcement chiefs, immigration officers, officers of Revenue and Customs, Customs officials the Chair of the Competition and Markets Authority and the Police Investigations & Review Commissioner. Instead Judicial Commissioners would be responsible for issuing warrants on application from law enforcement chiefs.

Briefing

It is a disturbing anomaly that this Bill proposes that authorisation for the most intrusive form of surveillance should be self-issued by a range of public bodies. This process would put a range of actors from chief constables to immigration officers in charge of issuing hacking warrants. This proposal would give these individuals greater powers of intrusion than the security services who are at least required to seek authorisation from the Secretary of State for their hacking activities. For countless obvious reasons it is important that this process is transferred to Judicial Commissioners.

**Urgent warrants**

Amendment

Clause 98, page 75, line 26, sub-clause (b), delete ‘considered’ and insert ‘had reasonable grounds for believing that it was necessary’

Clause 98, page 75, line 25, delete ‘that there was an urgent need to issue it’ and insert ‘there was an emergency situation posing immediate danger of death or serious physical injury or that the physical security or integrity of the nation was endangered’

Effect

This amendment requires that an urgent warrant can only be issued where there is a reasonable belief that doing so was necessary for the purpose of protecting life or preventing serious injury.

Amendment

Clause 98, page 75, line 28, after ‘issued’ insert ‘immediately’

Effect

This requires that the judicial commissioner is informed immediately that an urgent warrant has been issued.

Amendment

Clause 99, page 76, delete line 10 and sub-clause 4 and insert (4A)

4A Where the judicial commissioner refuses to approve an urgent warrant, they must direct that all of the material obtained under the warrant is destroyed, unless there are exceptional circumstances.

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.

Amendment

Clause 102, page 80, line 21, delete ‘fifth working day’ and insert ‘twenty four hours’

Effect

This specifies that urgent warrants can only last for 24 hours.

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. For interception, 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 interception could occur without judicial authorisation for up to 48 hours[15]. Given the potentially more significant nature of hacking, it seems likely that a more restricted timeframe would be required. 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. 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.

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

**Further provision about warrants: improving quality of details to be included**

Amendment

Clause 101, page 78, line 18, delete ‘or a description of the person or organisation’ and insert ‘or another identifier of the person or organisation’.

Clause 101, page 78, line 27, before ‘A description’ insert ‘The name and’

Clause 101, page 78, line 27, delete ‘or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe’ and insert ‘or another identifier of, each person or organisation’

Clause 101, page 78, line 36, delete ‘description’ and insert ‘specification’

Clause 101, page 78, line 37, before ‘A description’ insert ‘The name and’

Clause 101, page 78, line 40, delete ‘a description of as many of the locations as it is reasonably practicable to describe’ and insert ‘specification of each location’

Clause 101, page 79, line 19, delete ‘describe’ and insert ‘specify’

Clause 101, page 79, line 29, delete ‘or a description of the person or organisation’ and insert ‘or another identifier of the person or organisation’.

Clause 101, page 79, line 37, delete ‘or a description of, as many of the persons or organisations as it is reasonably practicable to name or describe’ and insert ‘or another identifier of, each person or organisation’

Effect

Further to amendments under the heading “subject matter”, these amendments require that warrants are targeted.

Briefing

See pages 11-12 of this briefing.

**Duration of warrants**

Amendment

Clause 102, page 80, line 24, replace ‘6’ with ‘1’

Effect

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

Briefing

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

**Additional Safeguards: audit trail and post-notification**

Amendment

Page 76, line 39, under 'Additional safeguards' insert new clause 100A –

(100) Audit trail of equipment interference

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

Effect

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

Briefing

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

Amendment

Page 76, line 39, under 'Additional safeguards' insert new clause 100B –

(100) Notification

(1) Upon completion of conduct authorised by a warrant under this Part, or the cancellation of a warrant issued under this Part, a Judicial Commissioner must notify the affected party, in writing, of –

(a) the conduct that has taken place, and

(b) the provisions under which the conduct has taken place.

(2) The notification under subsection (1) must be sent within thirty days of the completion of the conduct or cancellation of the warrant.

(3) A Judicial Commissioner may postpone the notification under subsection (1) beyond the time limit under subsection (2) if the Judicial Commissioner assesses that notification may defeat the purposes of an on-going serious crime or national security investigation relating to the affected party.

(4) A Judicial Commissioner must consult with the person to whom the warrant is addressed in order to fulfil an assessment under subsection (3).

Effect

This amendment would require that targets of hacking are notified after the fact, as long as it does not compromise any ongoing investigation.

Briefing

Liberty believes that JCs should be under a mandatory statutory duty to notify those subjected to surveillance once a particular operation or investigation has ended. At present, unlawful surveillance only comes to light as a result of a chance leak, whistleblowing or public interest litigation brought by Liberty and other NGOs and concerned citizens. This is deeply unsatisfactory.

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

> *"The Court reiterates that the question of subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and hence to the existence of effective safeguards against the abuse of monitoring powers, since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively"* (see Klass and Others, cited above, pp. 26-27, § 57).[16]

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

In *Zakharov v Russia* the ECtHR found that that judicial remedies for those subjected to interception in Russia were generally ineffective, particularly in light of the total absence of any notification requirement with regard to the interception subject, without any meaningful ability of retrospective challenges to surveillance measures.

The Bill provides a new power for the Investigatory Powers Commissioner to inform someone subjected to a surveillance error by a public authority (but not a CSP) if the IPC is made is aware of it; considers it sufficiently serious; and that it is in the public interest; and that it does not prejudice national security, the prevention or detection of crime, the economic well-being of the UK, or the continued discharge of the functions of any intelligence service.[17] For it to be serious it must have caused '*significant prejudice or harm to the person concerned'*. The Bill states that a breach of the HRA is not sufficient for an error to be considered a serious error.[18] Before making its decision the IPC must ask the public authority responsible for the error to make submissions to the IPC about the matter concerned. This is a narrow, arbitrary and highly discretionary power that will relate only to the most serious errors that the JCs discover during their very limited audit of the use of surveillance powers. It highlights the conflicted position that JCs may find themselves in and it does not discharge the Government's human rights obligations to provide post-notification by default unless it can justify continued secrecy.

The security repercussions of hacking into a device or network creates an even greater imperative for post-notification. The hack may have compromised the security of the device, leaving it open to further exploitation by criminals or even other Governments. It is the equivalent of the state breaking into a house, conducting a search, then leaving but without locking the doors and without the individual concerned realising this. It is one thing for the state to hack into a device where it is strictly necessary and proportionate; it is quite another for them to leave individuals vulnerable to criminal attacks with no way of protecting themselves. If the Government wishes its security and law enforcement agencies to have this significant power, it must accept the concomitant responsibility.

[17] The definition of an error includes failure to comply with requirements under this Act and in Code of Practice under Schedule 6.
[18] Investigatory Powers Bill 2016, clause 198, subsection (3)

**Renewal of warrants**

Amendment

Clause 103, page 80, line 36, delete ‘an instrument issued by the appropriate person (see subsection 3))’ and insert ‘by a Judicial Commissioner’

Clause 103, page 80, line 38, delete ‘appropriate person’ and insert ‘Judicial Commissioner’ (and repeat on lines 40, 43)

Clause 103, page 81, line 3, delete subsection (d) and insert new subsection (d) –

(d) that the Judicial Commissioner is satisfied that the applicant has explained -

(i) to what extent the previous warrant achieved the stated purpose, and

(ii) why the previous warrant failed to fully achieve the stated purpose, and

(ii) why the conduct proposed is likely to support the achievement of the stated purpose.

Clause 103, page 81, line 5, delete subsection (3)

Clause 103, page 81, line 27, delete subsection (5)

Clause 103, page 81, line 30, delete subsection (6)

Clause 103, page 81, line 33, delete subsection (7)

Clause 103, page 81, line 36, delete ‘Secretary of State’ and insert ‘Judicial Commissioner’

Effect

These amendments would provide for Judicial Commissioners to renew warrants rather than the Secretary of State. They also provide for a test for renewal to prevent indefinite, unjustified renewals of warrants that are unsuccessful in their goals.

Briefing

Under clause 103, a warrant may be renewed by the person who initially issued it - Secretary of State, Scottish Ministers or Law Enforcement Chiefs – with no requirement for judicial authorisation.

While Liberty has concerns that the process of judicial authorisation provided by the Bill is inadequate and does not meet human rights standards, permitting the renewal of hacking warrants without even the pretence of this purported safeguard is deeply problematic. While the issuing authority's initial assessment of necessity and proportionality will have been reviewed by a judge, this assessment would have taken place six months previously. There can be no basis for assuming that the circumstances remain the same or that these conditions will necessarily be met. Given the fast-paced changes that take place to modern technology, the assessment of technical proportionality and any threat it poses to cyber-security will also be out of date. If hacking has taken place during the initial six month period and has not yielded the required results, it seems essential that the requesting agency be required to justify the continued use of this intrusive technique. Hacking is an extremely invasive technique, and its use over a prolonged period of time raises significant questions concerning human rights and cyber protection and should be subject to strict safeguards, of which judicial authorisation is the most basic.

**Implementation and service of warrants outside the United Kingdom**

Amendment

Clause 109, page 87, line 39, delete sub-clause 3

Effect

This amendment deletes provision which allows a targeted equipment interference warrant to be served on a person outside the UK for the purpose of requiring that person to take action outside the UK.

Amendment

Clause 110, page 88, line 7, delete clause 110

Effect

This will delete provision setting out how warrants may be served outside the UK.

Briefing

Liberty has grave concerns that permitting the UK Government to serve hacking warrants on those outside the UK will set a worrying precedent for other countries to do the same. The Government Reviewer's report notes that when countries seek to extend their 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. 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 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."*[19]

[19] Paragraph 11.24.

**Duty of telecommunications operators to assist with implementation**

Amendments

Clause 111, page 88, line 35, delete clause 111

Effect

This amendment removes the duty on telecommunications operators to assist with implementation of warrants.

Briefing

The Bill would oblige any "*telecommunications operator"* to conduct hacking*,* which is defined as *"a person who offers or provides a telecommunications service to persons in the United Kingdom, or controls or provides a telecommunications system which is (wholly or partly) in the United Kingdom or controlled from the United Kingdom."* This expansive definition would include not only public services such as Gmail, Facebook, Twitter and Dropbox, but also private offices, businesses, law firms, government department networks (such as the NHS), and institutional networks such as universities. This was confirmed by the Home Secretary in her oral evidence to the Joint Committee. There is no requirement for judicial authorisation in order to compel a telecommunications operator to hack. This extraordinarily expansive power could force companies to engage in highly controversial work on behalf of the government, which is likely to be counter to the interests of cybersecurity and product security that companies strive to innovate, protect and extend. Furthermore, the non-disclosure provisions (clause 114) would prevent operators from revealing the existence of a warrant. Thus, were the *Apple v FBI* case to occur in the UK, the public would be entirely unaware of it.

Companies have consistently expressed deep concerns about this and similar provisions during pre-legislative scrutiny of the draft Bill, as being forced to compromise the security of their products of their customer's products is counter to companies' business interests and may undermine years of technical innovation.

Whilst the intelligence agencies may seek to develop equipment interference capabilities, it is entirely disproportionate to oblige the unwilling complicity of an open-ended number of 'telecommunications operators'.

**Safeguards relating to disclosure of material or data overseas**

Amendment

Clause 113, page 91, line 23, insert new sub-clause (1A) –

(1A) Material obtained via a warrant under this Part may only be shared with overseas authorities in accordance with the terms of an international information sharing treaty.

Effect

This amendment would require that information obtained via an equipment interference warrant is only shared with overseas authorities where a mutual legal assistance treaty has been put in place for the purpose of doing so.

Briefing

Liberty is disappointed that the Bill is silent on the intelligence sharing relationship between the Agencies and foreign intelligence agencies, in particular the Five Eyes. The ISC noted that the Bill "*does not, therefore, meet the recommendations made in the Committee's* Privacy and Security *Report that future legislation must set out these arrangements more explicitly, defining the powers and constraints governing such exchanges".*[20] However, international raw intelligence sharing remains absent from the revised Bill.

The Reviewer's report "A Question of Trust" described an "international trade in intelligence" between the Five Eyes partners – the UK, USA, Canada, Australia and New Zealand. Insofar as material gathered by the British services is shared with other countries, the report explained that the security services take the view that under their founding statutes, information can be shared if it is *"necessary for the purpose of the proper discharge of the security and intelligence agencies' functions"* and that when it is considered that this test is met certain RIPA safeguards apply. However, the report concluded that *"in practical terms, the safeguards applying to the use of such data are entirely subject to the discretion of the Secretary of State*."[21]

RIPA and the Codes of Practices are silent on British services receiving or accessing information from foreign services, with the security services only limited by the "general constraints" on their actions in various statutes.[22] It was only during the course of Liberty's

[20] *Report of the draft Investigatory Powers Bill* – The Intelligence and Security Committee, 9 February 2016; Recommendation J (xii)
[21] Paragraph 6.87.
[22] Paragraph 6.89.

legal action against the security services in the IPT that limitation information about the way in which the security services approach such situations was revealed. In its first finding against the Agencies, the IPT held that prior to these disclosures, the framework for information sharing was not sufficiently foreseeable and was not therefore "in accordance with law". The Tribunal held that as a result of the fact that the litigation had resulted in disclosures of information, the security services were no longer acting unlawfully when accessing information from the U.S.

David Anderson's report recommended that information sharing with foreign countries be subject to strict, clearly defined and published safeguards.[23] The report added that the *"the new law should make it clear that neither receipt nor transfer as referred to in recommendations 76-77 above should ever be permitted or practised for the purpose of circumventing safeguards on the use of such material in the UK".*[24] Such safeguards and guarantees are notably absent from the Bill.

[23] Recommendations 76 and 77.
[24] Recommendation 78.

**Offence of making unauthorised disclosure**

Amendment

Clause 116, page 93, line 42, insert new sub-clause (3) –

(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 unauthorised 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 116 which criminalise disclosure of information relating to the use of hacking 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 of unlawful or otherwise inappropriate behaviour will know that taking steps to do the right thing could expose them to significant criminal sanction. While the Bill provides that certain disclosures will be authorised, such as those to a Judicial Commissioner[25], prescribing this as the only route for whistle-blowers to take is unwise, unfair, and risks wrongdoing going unreported and unchallenged. 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, Silkie Carlo, Bella Sankey**

[25] Clause 115