HOUSE OF COMMONS LIBRARY

BRIEFING PAPER

Number 7518, 11 March 2016

Investigatory Powers Bill

By Joanna Dawson

Inside:

1. Background
2. Part 1: General Privacy Protections
3. Part 2: Lawful interception of communications
4. Part 3: Authorisations for obtaining communications data
5. Part 4: Retention of communications data
6. Part 5: Equipment Interference
7. Part 6: Bulk warrants
8. Part 7: Bulk personal datasets
9. Part 8: Oversight arrangements
10. Part 9: Miscellaneous and general provisions

Contents

Summary **4**

1. Background **5**
Legislative framework 5
Reports on Investigatory Powers 7
The Draft Bill 10
Initial reaction 11

2. Part 1: General Privacy Protections **14**
2.1 What does the Bill do? 14
2.2 Changes following pre-legislative scrutiny 15
2.3 What did the reports on investigatory powers say? 15
2.4 Debate and comment 16

3. Part 2: Lawful interception of communications **17**
3.1 What does the Bill do? 17
3.2 Changes following pre-legislative scrutiny 20
3.3 What did the reports on investigatory power say? 23
3.4 Debate and comment 24

4. Part 3: Authorisations for obtaining communications data **28**
4.1 What does the Bill do? 28
4.2 Changes following pre-legislative scrutiny 31
4.3 What did the reports on investigatory powers say? 34
4.4 Debate and comment 35

5. Part 4: Retention of communications data **38**
5.1 What does the Bill do? 38
5.2 Changes following pre-legislative scrutiny 39
5.3 What did the reports on investigatory powers say? 41

6. Part 5: Equipment Interference **42**
6.1 What does the Bill do? 42
6.2 Changes following pre-legislative scrutiny 44
6.3 What did the reports on investigatory powers say? 47
6.4 Debate and comment 47

7. Part 6: Bulk warrants **50**
7.1 What does the Bill do? 50
Chapter 1: Bulk interception warrants 50
Chapter 2: Bulk acquisition warrants 51
Chapter 3: Bulk equipment interference warrants 51
7.2 Changes following pre-legislative scrutiny 52
7.3 What did the reports on investigatory powers say? 54
7.4 Debate and comment 54

8. Part 7: Bulk personal datasets **58**
8.1 What does the Bill do? 58
8.2 Changes following pre-legislative scrutiny 59

8.3 What did the reports on investigatory powers say? 61
8.4 Debate and comment 61

9. Part 8: Oversight arrangements 62
9.1 What does the Bill do? 62
Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners 62
Chapter 2: Other arrangements 62
9.2 What has changed following pre-legislative scrutiny? 63
9.3 What did the reports on investigatory powers say? 68

10. Part 9: Miscellaneous and general provisions 69
10.1 What does the Bill do? 69
Chapter 1: Miscellaneous 69
Chapter 2: General 70
10.2 Changes following pre-legislative scrutiny 70
10.3 Debate and comment 73

Summary

The Investigatory Powers Bill would overhaul the framework governing the use of surveillance by the intelligence and security agencies and law enforcement to obtain the content of communications and communications data. It follows three important reports published in 2015, all of which concluded that the law in this area is unfit for purpose and in need of reform, and a draft Bill that has been subjected to pre-legislative scrutiny by three parliamentary committees.

Many of the capabilities for which the Bill provides have been in use for a number of years. Some are openly provided for in the *Regulation of Investigatory Powers Act 2000*, whereas others have been only recently avowed, having operated on the basis of vaguely drawn provisions in legislation governing the general powers of the security, intelligence and law enforcement agencies.

The capabilities for which the Bill provides are the interception of communications, the retention and acquisition of communications data, equipment interference, and the retention and examination of bulk personal datasets. Interception, acquisition of communications data, and equipment interference powers are provided for both on a targeted basis and in bulk.

The Government have said that the only new capability provided for by the Bill is the ability to require retention of Internet Connection Records, a kind of communications data that reveals the websites an individual has visited.

The Bill would also reform the oversight regime for the use of these powers, replacing the three existing Commissioners with a single body of Judicial Commissioners led by the Investigatory Powers Commissioner. For the first time, these Commissioners would bring an element of judicial oversight to the process of issuing warrants to the intelligence services.

The Bill, and the powers for which it would provide, raise questions of profound importance. These include the balance to be struck between privacy and security; the extent to which Parliament, and the public, should be aware of conduct exercised on their behalf; and the trust that should be placed in the agencies and Government not to abuse powers that have the potential to be deeply intrusive.

Debate around these issues has been heated. Some believe that intrusive capabilities should only ever be exercised on the basis of reasoned suspicion, arguing that this reflects long standing British legal convention. Others take the view that an unprecedented terrorist threat, coupled with a constantly evolving technological landscape, mean that the agencies tasked with protecting the public should be endowed with whatever capabilities they believe necessary in order to fulfil that role.

The Bill also has important implications for the technology industry, on whose cooperation and expertise the exercise of investigatory powers at times depends. Industry has raised concerns about the feasibility and cost impact of the proposed measures, and the competitiveness of the UK's technology sector.

Whatever the practices of the past (and present), it is clear that this Bill provides Parliament with an unprecedented opportunity to consider these questions in full view of the public. Nonetheless, the complexity of the technological issues and the necessarily secretive nature of the subject matter, mean that the Bill seeks approval of a framework governing conduct which at times remains opaque.

1. Background

Legislative framework

The Regulation of Investigatory Powers Act 2000

The *Regulation of Investigatory Powers Act 2000* (RIPA) contains much of the existing legal framework governing the powers of the security and intelligence agencies and law enforcement agencies to intercept communications in order to access their content, and to acquire communications data. The Act provides for a scheme of warrants and oversight which was intended to be comprehensive and compliant with the European Convention on Human Rights (ECHR).

When RIPA was introduced the then Home Secretary Jack Straw described it as an "important bill, and … a significant step forward for the protection of human rights in this country".[1] However, the Act has been the subject of persistent criticism, focusing on the arcane and inaccessible style in which it was drafted. Furthermore, since RIPA came into force, methods of communicating, and the volume of communications data potentially available, have increased significantly. There now exists a broad consensus that the legislative framework is in need of modernisation and clarification.

In addition to RIPA, the *Wireless Telegraphy Act 2006* allows for the interception of communications and a number of other statutes also provide for the acquisition of communications data. These include, the *Telecommunications Act 1984*, the *Police and Criminal Evidence Act 1984* and the *Terrorism Act 2000.* The *Intelligence Services Act 1994* gives the Secretary of State the power to issue warrants authorising MI5, MI6 and GCHQ to interfere with property, and the *Police Act 1997* provides a similar power in relation to law enforcement. The Government has recently acknowledged that this power is used to authorise computer network exploitation (CNE), also known as hacking.

Interception
Interception is defined as making available the content of a communication – such as a telephone call, email or social media message – in the course of its transmission or while stored on a telecommunications system

Communications data
Communications data is described as information about communications, the 'who', 'where', 'when', 'how', and 'with whom' but not what was written or said

Data retention

RIPA does not regulate what data must be retained, dealing only with acquisition and disclosure. Therefore when RIPA was introduced, the only data available to be accessed was the data retained by the Communications Service Providers (CSPs) for their own purposes. In 2005 the EU adopted the Data Retention Directive, requiring the mandatory retention of data on communication networks. The UK transposed the directive into national law via the Data Retention Regulations.[2]

In 2009 the Labour Government consulted on a plan to legislate to compel CSPs based in the UK to collect and keep all data public authorities might need, including third party data crossing their networks, and to make all this data accessible on a case-by-case basis to

[1] HC Deb 6 March 2000, c 767
[2] Data Retention (EC Directive) Regulations 2009/859 (now repealed)

public authorities.[3] No legislation was put forward before the 2010 general election.

In June 2012 the coalition Government published the *Draft Communications Data Bill.* The Bill, which was dubbed the "Snoopers' Charter" by critics due to the breadth of the powers sought, would have replaced those parts of RIPA that deal with the acquisition of communications data. It proposed significantly extending the range of data CSPs would have to store. It would have included for the first time records of each user's internet browsing activity (websites visited but not pages within websites), details of messages sent on social media, webmail, voice calls over the internet, and gaming, in addition to emails and phone calls.

The Government believed that the Bill was necessary in order for the police and intelligence and security agencies to operate effectively in a fast-changing environment of communications technology, in which far more communications take place over the internet.

A Joint Committee set up to scrutinise the Bill reported in December 2012. The Committee concluded that the powers to order the retention of data contained in the Bill should be significantly narrowed, and safeguards against abuse introduced, before it could be workable. It also recommended that there should be much better consultation with industry, technical experts, civil liberties groups, public authorities and law enforcement bodies before a new Bill was introduced.[4]

The Intelligence and Security Committee published a report raising similar concerns, including that there had been insufficient consultation with industry.[5]

Following publication of these reports the draft Bill did not progress.

Data Retention and Investigatory Powers Act 2014

In 2014 the issue was reignited when the Court of Justice of the European Union (CJEU) declared the Data Retention Directive invalid, on the basis that it infringed privacy and data protection rights guaranteed by the European Union Charter of Fundamental Rights ('the Charter').[6] In the absence of a framework requiring the retention of communications data by service providers, the ability of law enforcement agencies to access that data would be impeded. Therefore, the Government fast-tracked the *Data Retention and Investigatory Powers Act 2014* (DRIPA) in order to recreate a regime that would ensure that data was retained.

A subsequent judicial review of DRIPA, brought by MPs David Davis and Tom Watson, found that section 1 was incompatible with EU law, as

---

[3] Protecting the Public in a Changing Communications Environment, Home Office, April 2009

[4] Joint Committee on the Draft Communications Data Bill, *Draft Communications Data Bill*, 11 December 2012, HL Paper 79, HC 479

[5] Intelligence and Security Committee, Access to communications data by the intelligence and security Agencies, Cm 8514, 5 February 2013

[6] Digital Rights Ireland C-293/12

interpreted by the CJEU.[7] Section 1 allows the Home Secretary to issue a retention notice to a service provider requiring them to retain communications data where the requirement is necessary and proportionate for a purpose falling under RIPA. The Government are in the process of appealing the decision, but regardless of the outcome of that appeal, alternative measures would be required by the end of 2016 due to a sunset clause in DRIPA.

Part 3 of the *Counter-Terrorism and Security Act 2015* amended DRIPA to enable the Secretary of State to require internet service providers to retain data allowing the authorities to identify the person or device using a particular internet protocol (IP) address at any given time.

Box 1: IP address resolution

An Internet Protocol (IP) address is a numerical label that acts much like any address for a computer on the Internet, allowing data to be delivered to that computer. Every device requires an IP address to be able to request and receive content from websites. These IP addresses can be recorded by website operators.

Communications Service Providers (CSPs) providing connections assign IP addresses to computers as and when they connect to the internet. The public IP address you are allocated by your CSP may be permanent (static) or temporary (dynamic). Businesses tend to have static addresses, whilst individuals tend to be assigned a dynamic address. This means an individual's IP address can change frequently.

CSPs have a limited number of IP addresses available that it can assign at any one time—there may be 20,000 IP addresses and 40,000 customers. Since not everyone is connected at the same time, the CSP assigns a different IP address to each computer that connects, and reassigns it when they disconnect. Because of this, the IP address assigned to your computer one day may get assigned to several other computers (and different users) before a week has passed. Furthermore, if you share your computer or even just your connection to your ISP, then multiple people are sharing one IP address.

IP resolution is the ability to identify who was using an IP address. Identifying individuals using nothing more than their IP address has become a key part of anti-piracy and criminal investigations.

Reports on Investigatory Powers

A Question of Trust

Section 7 of DRIPA required the Government's independent reviewer of terrorism legislation, David Anderson QC, to conduct a review of the operation and regulation of investigatory powers, with specific reference to the interception of communications and communications data. The outcome of this review, A Question of Trust ("the Anderson Report"), was published on 11 June 2015.[8] It made extensive and detailed recommendations for a new legislative framework to replace RIPA and DRIPA. Key recommendations included:

- RIPA and related legislation should be replaced with a new law that would be both "comprehensive" and "comprehensible".
- Security and intelligence agencies should have powers to carry out "bulk collection" of intercepted material but there must be "strict additional safeguards".

[7] *Davis et al v SSHD* [2015] EWHC 2092
[8] David Anderson QC, *A Question of Trust*, June 2015

- Judges should authorise requests to intercept communications, limiting the Home Secretary's current role in deciding which suspects are monitored.
- The definition of communications data should be reviewed, clarified and brought up to date.
- Oversight should be provided by an Independent Surveillance and Intelligence Commissioner, replacing the three existing Commissioners' offices.
- The controversial proposals contained in the draft Communications Data Bill to provide for the compulsory retention of web logs (user interaction with the internet) and third party data (the entire content of third party communications that passed over the network of a UK Communications Service Provider) should not be pursued before a compelling operational case has been made out.[9]

Intelligence and Security Committee

The Intelligence and Security Committee of Parliament (ISC) announced on 17 October 2013 that it would be broadening its inquiry into the laws governing the intelligence agencies' ability to intercept private communications.[10] It held public evidence sessions in October 2014 as part of its Privacy and Security Inquiry. These sessions explored a number of themes, including:

- expectations of privacy, and the extent to which it may be appropriate to intrude into an individual's privacy in order to protect the rights and safety of others;
- whether it is acceptable to use intrusive capabilities in a targeted way against known threats, and whether it is ever acceptable to use such capabilities to gather information in larger quantities;
- whether the current statutory framework governing and regulating the Agencies' intrusive activities delivers those principles; and,
- whether there is scope for greater transparency in this area.[11]

The Committee published its report on 12 March 2015. Although the Committee were satisfied that the UK's intelligence and security agencies do not seek to circumvent the law when carrying out surveillance, the ISC had misgivings about the existing laws. The legal framework had developed "piecemeal" and was "unnecessarily complicated", the Committee felt, resulting in a lack of transparency that was not in the public interest:

---

[9] David Anderson QC, *A question of trust: report of the Investigatory Powers Review,* June 2015, see Executive summary paras 10-34
[10] Intelligence and Security Committee press release, 17 October 2013
[11] Intelligence and Security Committee press release, 9 October 2014

> Our key recommendation therefore is that the current legal framework be replaced by a new Act of Parliament governing the intelligence and security Agencies. This must clearly set out the intrusive powers available to the Agencies, the purposes for which they may use them, and the authorisation required before they may do so.[12]
>
> The report also contains substantial recommendations about each of the agencies' intrusive capabilities, which the Committee considered essential to improve transparency, strengthen privacy protections, and increase oversight. Given the recent controversy surrounding GCHQ's bulk interception capability, the Committee scrutinised this aspect in particular detail.[13]

Independent Surveillance Review

On 4 March 2014, the then Deputy Prime Minister, Nick Clegg, announced an Independent Surveillance Review (ISR), to be carried out by the Royal United Services Institute (RUSI). This review into surveillance technologies and the problems of control and oversight would examine surveillance practices in the UK in the context of new communications technologies. It would make recommendations for legislative and policy reform and would deliver a report after the General Election to be considered by the Government alongside the ISC review and the Anderson review.[14]

The report was published on 14 July 2015.[15] The accompanying press release summarised its recommendations:

> The Review Panel makes the case for a radical reshaping of the way that intrusive investigative techniques using the Internet and digital data are authorised that is fully compliant with the human rights framework.
>
> It recommends that requests for interception for the prevention and detection of serious crime in future be authorised by a senior judge, and that the warrants that are signed by Secretaries of State for purposes relating to national security (including counter-terrorism) should in future all be subject to judicial scrutiny, according to arrangements set out in the report.
>
> …
>
> Like other recent reviews, the ISR highlights inadequacies in law and oversight and calls for urgent new legislation in this session of Parliament to provide a new democratic mandate for digital intelligence. The present arrangements are too complex to be understood by the citizen and have contributed to a public credibility gap that must be addressed. The Review therefore sets out ten tests that any new legislation must pass before it can be regarded as giving the police and the intelligence agencies a democratic licence to operate.[16]

---

12 Intelligence and Security Committee, *Privacy and security: a modern and transparent legal framework*, HC 1075 2014/15, 12 March 2015, p2
13 Intelligence and Security Committee, press release, 12 March 2015
14 RUSI News, *RUSI to convene independent review on the use of internet data for surveillance purposes*, 4 March 2014. This press notice includes the review's terms of reference.
15 RUSI, *A democratic licence to operate: report of the Independent Surveillance Review*, July 2015
16 RUSI News, *Independent Surveillance Review publishes report: 'A Democratic Licence to Operate'*, 14 July 2015

The Draft Bill

In November 2015 the Government published the *Draft Investigatory Powers Bill*. A Joint Committee was formed to provide pre-legislative scrutiny. The Committee reported on 11 February 2016.[17] The Intelligence and Security Committee[18] and the Commons Science and Technology Committee[19] also published more limited reports on the draft Bill in February 2016. The Government has published a Command Paper setting out its response to pre-legislative scrutiny.[20]

The Joint Committee's report made 86 recommendations as to how the Bill, and the wider process, might be improved. The Committee did not raise principled objections in relation to the majority of the capabilities provided for. However, it did conclude that, due to a lack of access to classified materials, in relation to certain issues it was not in a position to reach an informed view. The Report highlighted the importance of the Intelligence and Security Committee's role in this respect.

The Report recommended that the Government should ensure that Codes of Practice and further justification as to the need for the capabilities sought should be published alongside the Bill in order to inform Parliamentary scrutiny. It also recommended that the Government should improve technical definitions and address witnesses' concerns about costs and feasibility.

In relation to the authorisation of warrants the Committee accepted that there should be ministerial authorisation, with approval by a Judicial Commissioner on the basis of judicial review principles.

In relation to the oversight regime generally, the Committee questioned why the Government had decided to create a group of Judicial Commissioners, rather than an Independent Surveillance and Intelligence Commission, as recommended by the Anderson report. It also recommended that Judicial Commissioners should be appointed by the Lord Chief Justice, rather than the Prime Minister as proposed in the Bill, in order to ensure public confidence.

Another area in which the Committee recommended a number of substantive amendments to the Bill was in relation to the treatment of confidential and privileged material, deeming the limited safeguards contained in the draft Bill to be insufficient.

The Science and Technology Committee's overall conclusion was that the UK's tech businesses need certainty over the obligations the draft Bill would impose, and reassurance that these obligations would be reasonably practicable and that the costs would be met fully, in order to avoid being put at a commercial disadvantage with overseas competitors.

---

[17] Draft Investigatory Powers Bill Report, HL Paper 93, HC 651, 11 February 2016
[18] Report on the Draft investigatory Powers Bill, HC795, 9 February 2016
[19] Investigatory Powers Bill: technology issues, Third report of Session 2015-2016, HC 573, 1 February 2016
[20] Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny, Cm 9219, March 2016

The Committee expressed concern that the provisions on internet connection records (ICRs) lack clarity. Given the volume of data involved in the retention of ICRs, and the security and cost implications associated with their collection and retention, industry were concerned about what they would mean for business plans and competitiveness. The Committee recommended that the Government should review the draft Bill to ensure that the obligations it created are both clear and proportionate.

The Committee also suggested that the Government should work with industry to improve estimates of the costs of complying with the measures in the Bill, and that the Bill should include an explicit commitment to meeting the full costs.

The Intelligence and Security Committee were able to take evidence on classified matters, unlike the other Committees, and so sought to provide scrutiny on aspects of the Bill relating to the agencies' use of investigatory powers.

The tone of the ISC's report was considerably more negative than the Joint Committee. It expressed disappointment that the draft Bill did not cover all of the agencies' intrusive capabilities, meaning that various powers remain scattered throughout different pieces of legislation.

The Report listed a number of issues that gave cause for concern. In particular the ISC concluded that privacy protections were inconsistent and in need of strengthening. It recommended that a new part be added to the Bill to provide universal privacy protections which apply across the full range of investigatory powers. The ISC also felt that the agencies had not made the case for the need to engage in bulk equipment interference,[21] and recommended that these provisions be removed from the Bill.

Initial reaction

Writing in the Telegraph, David Anderson QC suggested that, although some issues still remain to be resolved, the Bill

> Charts a bold route forward – and gets the most important things right. By avowing every one of the remarkable powers that police and intelligence agencies exercise or aspire to, it restores the rule of law and sets an international benchmark for candour.[22]

The Telegraph's editorial was broadly supportive, but with the significant caveat that the powers of the intelligence agencies should be separated from those of the police and other public bodies:

> Those who object to the speed of the process are in truth questioning whether the Government and its agencies need to exercise these powers of bulk data surveillance at all. But given the level of the terrorist threat and the increased use of the internet by the enemies of the state it is hard to make that

[21] During the Second Reading debate, the Chair of the ISC indicated that since publication of the Report, the Government had provided the Committee with further information, and it was now convinced that there is a valid case for the powers to remain in the Bill: HC Deb 15 Mar 2015, col 838

[22] David Anderson QC, The Investigatory Powers Bill is still a work in progress, *The Telegraph*, 2 March 2016

> argument credibly. It is doubtful that a large majority of the country would agree, either.
>
> …
>
> However, critics are right to say that the powers of the police and other state bodies to carry out surveillance should be separated from the national security requirements of the intelligence agencies. People believe surveillance powers should be directed at terrorists and it is their general and arbitrary use that most damages public trust.[23]

The Times was supportive of the Bill insofar as it relates to national security, suggesting that in the face of terrorist aggression, there are strong arguments for its prioritisation over privacy concerns. However the Times also had reservations about the coupling of police powers with those of the security and intelligence agencies, suggesting that police powers had been expanded in the revised Bill as a result of police lobbying:

> Quite unlike the security services, there is a long and regrettable history of British police exploiting for other purposes powers that were designed to combat serious crime. The existing Regulation of Investigatory Powers Act (Ripa) has been used frequently to expose the sources of journalists reporting on the police themselves, most notoriously in the Metropolitan police's investigation into *The Sun* newspaper's reporting of the "Pleb-gate" scandal involving the MP Andrew Mitchell.
>
> Britain's security services are known to use their powers discerningly. The same cannot be said about Britain's police. The House of Commons should be wary of gifting them new powers requiring little oversight from anybody other than senior police officers. The home secretary, meanwhile, should not have jeopardised the vital preservation of national security by packaging it alongside new domestic powers that are almost certain to be abused.

The Guardian expressed concern about the extension of existing powers, and the reach of surveillance in the digital age. It also suggested that concessions following pre-legislative scrutiny had been minimal, and noted that some powers had been expanded:

> But at the same time, and without any advertisement, some tentacles of surveillance are being licensed to creep further than before.
>
> Communication providers, who were already set to be tasked with keeping exhaustive data on phone calls, social messages and unlawful sites, will now be expected to keep automatically a year of internet connection records – which could include a deeply private browse of, say, the Marie Stopes or Gamblers Anonymous site. Alert citizens may have grown uneasily used to the idea that GCHQ can get its hands on such information, and the police will have the facility too. Knowledge is power, and the number of fallible human beings who possess it – and perhaps misuse or mislay it – could soar. Measures initially advanced to deal with serious criminals will be turned on migrants, with new powers for officials pursuing immigration and nationality offences, and immigrant detention facilities subject to domestic interception.

---

[23] Powers to tackle terrorism are vital, *The Telegraph*, 2 March 2016

> …
>
> For as cars, watches and even white goods acquire connectivity, it will become possible to build up exhaustive logbooks on the lives of others. Bluntly described powers to switch on cameras and microphones on people's own phones starkly reveal how the tide of technology is washing away all need for the old art of installing bugs, as well as the old practical and procedural limits on their use. In purely technical terms, the depth of the monitoring that the smartphone can enable goes way beyond anything afforded by the electronic tag.[24]

This paper

This paper provides an overview of the Bill's main provisions, together with some analysis of the changes that have been made following pre-legislative scrutiny, and the extent to which the Committees' recommendations have been met. Further detail on the Government's reasons for accepting or rejecting recommendations is provided in the Government's response to pre-legislative scrutiny.

The paper does not cover every clause in the Bill. The Bill and the Explanatory Notes should be referred to for a detailed description of each clause.

Other relevant materials on the Bill , available on Gov.uk, include:

Overarching documents

Codes of Practice

Factsheets

At the time of publication, detailed reaction to the Bill has been limited. This paper therefore largely reflects comment and debate around key issues raised during pre-legislative scrutiny.

Territorial extent

The Bill applies to the whole of the United Kingdom. Annex A of the Explanatory Notes includes a summary of the position regarding territorial extent and application in the UK.

The Speaker has yet to issues certificates for the new English Votes for English Laws procedures. When he does so, these will be available from the All Bill Documents page for this Bill on the Parliamentary Website.

[24] The Guardian view on surveillance: keep a vigilant eye on the snoopers, *The Guardian*, 1 march 2016

2. Part 1: General Privacy Protections

2.1 What does the Bill do?

Part 1 of the Bill sets out certain key principles and offences.

RIPA 2000 currently defines lawful and unlawful interception

Clauses 2-6 define interception and "lawful authority"; would create an offence of unlawful interception; and provide for the imposition of fines in situations in which unlawful interception has taken place unintentionally.[25]

Clause 7 provides that an appropriate warrant must be in place before a request may be made to the authorities of another country to carry out interception of a person believed to be in the British Isles.

Clause 8 provides that an appropriate warrant must be place before a request for interception can be made to the authorities of another country under a mutual assistance agreement.

Clause 9 would create a new offence of unlawfully obtaining communications.

Clause 10 and Schedule 2 would abolish or restrict existing powers to acquire communications data under various pieces of legislation. This is intended to ensure that communications data may only be acquired, for the purposes set out in the Bill, subject to the safeguards provided.[26]

Equipment interference (also known as computer network exploitation (CNE) or cyber espionage) is the practice of gaining access to people's devices and computers in order to monitor data, such as geolocation, texts and emails, in real time.

Clauses 11 and 12 relate to equipment interference, setting out the conditions in which a warrant must be sought. A warrant must be sought under the Bill for equipment interference for the purposes of obtaining communications or private information, if the conduct involved would otherwise constitute an offence under the *Computer Misuse Act 1990* and there is a connection to the British Islands. The explanatory notes state that this provision would not remove or limit the ability to authorise equipment interference under the *Police Act 1997* for other purposes, but not for obtaining communications or private information.

[25] Monetary penalty notices are notices served by the Investigatory Powers Commissioner in these circumstances requiring payment of a penalty not exceeding £50,000. Schedule 1 sets out further detail.

[26] It will also mean that other legislation cannot be used to acquire communications data without the consent of the operator.

2.2 Changes following pre-legislative scrutiny

Key changes to the Bill and relevant recommendations

Change	JC	ISC
The word 'Privacy' has been inserted into the title of **Part 1**		**Recommendation A**: the new legislation should include a single additional Part that addresses privacy safeguards and clearly sets out universal privacy protections which apply across a full range of investigatory powers.
Clause 7 has been amended to ensure that an overseas agency cannot be asked to undertake interception on behalf of a UK authority, in respect of an individual in the UK, without a targeted interception or examination warrant being in place.	**Recommendation 44**: The Committee also recommends that the Bill should make it illegal for UK bodies to ask overseas agencies to undertake intrusion which they have not been authorised to undertake themselves.	
Clause 9 – which would create a new offence of unlawfully obtaining communications data - has been amended with the addition of a new defence in subsection (3) where the person acted in the reasonable belief that they had lawful authority.		

2.3 What did the reports on investigatory powers say?

Anderson	ISC	ISR
The Anderson Report recommended that existing legislation should be replaced by a comprehensive new law, drafted from scratch, which affirms the privacy of communications and prohibits interference with them by public authorities, save on specific terms. The new law should replace both RIPA and existing powers under other pieces of legislation in this area.[27]	The purposes, functions, capabilities and obligations of the Agencies should be clearly set out in a new single Act of Parliament. This should be distinct from legislation covering law enforcement and other bodies currently covered by RIPA … .[28] The new legislation should clearly list each intrusive capability available to the Agencies, and set out the purposes for which it can be used, the relevant human rights obligations, authorisation procedures and safeguards. The law should be amended to make abuse of intrusive capabilities (such as interception) a criminal offence.[29]	Current surveillance powers are needed but they require a new legislative framework and oversight regime. Specifically, RIPA Part I, DRIPA and Part 3 of CTSA 2015 should be replaced by a comprehensive new law. [30]

[27] Recommendations 1, 6 and 7.
[28] Annex A, paras XX & YY
[29] Annex A, para T
[30] Recommendation 1

2.4 Debate and comment

A number of commentators have picked up on the apparent response to the ISC's recommendation that there should be a new part aimed at addressing privacy concerns.

Writing in the Guardian, Carly Nyst[31] said:

> With deeply regrettable flippancy, the Home Office has responded to the ISC's recommendation that the draft legislation contain "an entirely new part dedicated to overarching privacy protections [to ensure that] privacy is an integral part of the legislation rather than an add-on" by adding one word to the bill – the word "privacy" to the title of part one, previously "general protections".[32]

Open rights group said:

> **Privacy**: The ISC said: "privacy protections should form the backbone of the draft legislation, around which the exceptional powers are then built" and said that "one might have expected an overarching statement at the forefront of the legislation". The Home Office response seems to have been to add the word "Privacy' to a heading in Part One of the Bill.

David Allen Green said:

> So "privacy" is mentioned more often in the headers to pages than in the Bill itself, and it is only once used anywhere in the Bill when it is not in a title.
>
> …
>
> Of course, this is not a complete way of assessing how privacy is addressed in the Bill – privacy points can be covered without necessarily using the word, and a search for "privacy" in the (non-binding) explanatory notes is an instructive exercise. [33]

Mike Harris in the *Independent* said:

> Parliament's Intelligence and Security Committee - the only security-checked committee with access to the most sensitive workings of our intelligence agencies -told May to place privacy at the heart of the Bill. Her Home Office officials simply added the word "privacy" to a chapter heading. To treat Parliament with such contempt is beneath one of the great offices of state.[34]

---

[31] Human rights consultant, previously Legal Director of Privacy International

[32] The snooper's charter shows the government's total contempt for privacy, The Guardian, 1 March 2016

[33] "Privacy is Surveillance" – Part 1 of the Investigatory Powers Bill, 2 March 2016, jackofkent.com [accessed 10 March 2016]. David Allen Green is editor of the Jack of Kent blog and legal commentator for *FT.com*

[34] Only China and Russia violate their citizens privacy as much as the Snoopers' Charter allows, *The Independent*, 2 March 2016

3. Part 2: Lawful interception of communications

3.1 What does the Bill do?

Chapter 1: interception and examination with a warrant

Clause 13 sets out the various types of interception warrant that may be sought under the Bill. The three types of warrant are as follows:

- A targeted interception warrant authorises the interception of communications and acquisition of associated communications data. It may relate to a particular person, organisation or premises, or groups of connected subjects.
- A targeted examination warrant authorises the examination of intercepted material obtained under a bulk interception warrant.
- A mutual assistance warrant authorises requests for, and the provision of, assistance with overseas interception.

Clause 14 sets out further detail as to what would constitute 'secondary data' in different contexts. Secondary data is data that may be obtained under a targeted interception warrant, other than the content of the communication itself.[35]

Clause 15 would govern the subject matter of warrants. It states that warrants may relate to a particular person, organisation or set of premises. Targeted warrants may also relate to a group who share a common purpose or carry on a particular activity. They may also apply to multiple persons, organisations or premises, provided they are all part of a single investigation.

Clauses 16-23 would provide for the authorisation of warrants. The "intercepting authorities" are those persons able to apply for a warrant under Chapter 1. These are the heads of the intelligence services, the National Crime Agency, the Metropolitan Police, the Police Services of Scotland and Northern Ireland, HM Revenue and Customs, the Chief of Defence Intelligence, and a competent authority from another jurisdiction.

The Secretary of State[36] would be able to issue a warrant if he or she believes that it is necessary on certain grounds and proportionate to what is sought. The grounds are national security; preventing or detecting serious crime; safeguarding the economic wellbeing of the UK, insofar as that is relevant to national security; or giving effect to an international mutual assistance agreement.

The decision would then be subject to approval by a Judicial Commissioner.[37] The Judicial Commissioner would be required to look

[35] Secondary data was referred to as "related communications data" under the draft Bill, a term which is taken from RIPA.

[36] Or Scottish Minister in a relevant Scottish application, relating to a person or premises believed to in Scotland, and sought for the purposes of preventing or detecting serious crime in Scotland. .

[37] See Part 10 on oversight arrangements for further information

at the necessity and proportionality test applied by the Secretary of State or Scottish Minister on the same grounds as would be applied by a court in an application for judicial review. If the Judicial Commissioner refused to approve a warrant they must set out written reasons for the refusal. The requesting agency may then seek to address any concerns and resubmit the request.

The Secretary of State may ask the Investigatory Powers Commissioner[38] to reconsider an application that has been refused but if the Investigatory Powers Commissioner also refuses it there is no further appeal process.

In urgent cases a warrant may be issued without the approval of a Judicial Commissioner, but the Judicial Commissioner must still be notified and must decide whether to approve the warrant within three working days. If the Judicial Commissioner refuses to approve the warrant then it ceases to have effect. The Judicial Commissioner may then direct what can happen to any material or intelligence gathered.

Clause 24 would provide that the Secretary of State must consult the Prime Minister before deciding to issue a warrant relating to the communications of a Member of either House of Parliament, the Scottish Parliament, the National Assembly for Wales, the Northern Ireland Assembly, or a UK MEP.

The convention that MPs' communications should not be intercepted by police or security services is known as the 'Wilson Doctrine'. It is named after the former Prime Minister Harold Wilson who announced the policy in 1966 in response questions from MPs who were concerned that their phones were being tapped. Recent case law established that the doctrine does not have any legal effect, and the Prime Minister confirmed that in practice the Secretary of State would consult the Prime Minister before authorising a warrant to intercept an MP's communications.

Clause 25 sets out safeguards that would apply when one of the purposes of a warrant is to obtain or look at items which are subject to legal privilege, or where it is likely that such material will be obtained or examined. In these circumstances the person applying for the warrant must make this clear. The person authorising it must be satisfied that specific handling arrangements are in place, and where obtaining privileged items is a purpose of the warrant, that there are exceptional and compelling circumstances to justify it.

Legal professional privilege is the right of a client to have private communication with a lawyer and to obtain legal advice and assistance in the course of litigation

Clauses 26-33 would make further provision in relation to warrants, including the information that must be contained in a warrant, the normal duration of warrants, and the process for the renewal, modification and cancellation of warrants.

Clauses 34-36 deal with the implementation and service of warrants, and impose a duty on operators to assist with implementation. The operator would be required to take all reasonably practicable steps to give effect to the warrant, whether or not they are located in the UK.

[38] See Part 10 on oversight arrangements for further detail

Any requirements or restrictions under the laws of the country in which the operator is based would be relevant to determining what is reasonable. Clause 36 would create an offence of knowingly failing to comply with an interception warrant.

Chapter 2: Other forms of lawful interception

Clauses 37-44 set out other limited forms of lawful interception. These include interception with consent; interception in prisons and psychiatric hospitals; interception for certain regulatory and enforcement purposes; interception in immigration detention facilities, and; interception for certain business purposes.

Clause 45 sets out the conditions for complying with overseas interception requests.

Chapter 3: Other provisions about interception

Clauses 46 and 47 set out safeguards for the storage and disclosure of material obtained under a warrant, including safeguards for the disclosure of material which is shared with overseas agencies. Where an item subject the legal privilege is retained, the Investigatory Powers Commissioner must be informed as soon as is reasonably practicable.

Clause 48 provides that material obtained under a warrant may not be used in legal proceedings. **Schedule 3** sets out a number of exceptions to this principle, for example, that intercept material may be used in proceedings before the Investigatory Powers Tribunal.

Clause 49 would impose a duty not to disclose the existence or details of a warrant or any intercepted material. **Clause 50** would provide for an exception to this duty in certain circumstances, namely, a where disclosure is authorised by the warrant; where it is made to, or authorised by, a Judicial Commissioner; where it is made by a legal adviser to a client (or vice versa); or where it is a disclosure by an operator of a general nature and does not relate to a specific warrant. **Clause 51** would create an offence of unauthorised disclosure.

3.2 Changes following pre-legislative scrutiny

Key changes to the Bill and relevant recommendations

Change	JC	ISC
Clause 22 of the Bill (previously 20) provides that urgent warrants would have to be approved within three (rather than five) working days of authorisation by a Secretary of State[39]	**Recommendation 36:** The Committee therefore recommends that the period in which urgent warrants must be reviewed by a Judicial Commissioner should be shortened significantly. We suggest that they must be reviewed within 24 hours of their signature by the Secretary of State.	**Recommendation J(v):** We have similar concerns regarding the timeframes in respect of 'urgent' warrants. The draft Bill allows for a five working day 'grace period' in circumstances where the Agencies consider that a warrant is required urgently: in these circumstances, the Secretary of State may issue the warrant before the Judicial Commissioner has approved it. While we recognise the need for a procedure to handle urgent cases, five working days is unnecessarily long. The Committee recommends that the maximum period for which a warrant may be operational without judicial authorisation is two working days.
Clause 25 of the Bill contains additional safeguards for items subject to legal privilege that have been acquired by targeted interception[40]	**Recommendation 46**: The Committee recommends that provision for the protection of Legal Professional Privilege (LPP) in relation to all categories of acquisition and interference addressed in the Bill should be included on the face of the Bill and not solely in a code of practice. The Government should consult with the Law Societies and others as regards how best this can be achieved.	**Recommendation B:** Where additional protection is provided for sensitive professions, these safeguards must be applied consistently, no matter which investigatory power is used to obtain the information. The new legislation should be amended to rectify this inconsistency.

Other relevant recommendations and responses

JC Recommendation 32: The Committee recommends that major modifications for targeted interception warrants, as defined in the draft Bill, should also be authorised by a Judicial Commissioner.	**The Government has not accepted this recommendation**. The response to pre-legislative scrutiny states: "To require authorisation by a Judicial Commissioner for each such modification would drastically reduce the operational agility of the agencies."
JC Recommendation 37: The Committee recommends the inclusion of a definition of the word 'urgent' for the purposes of authorising urgent warrants.[41]	**The Government accepted this recommendation** but has included a definition of 'urgent' in the draft Codes of Practice published alongside the Bill. Urgent warrant would need to fall into one of three categories: imminent threat to life; a significant intelligence gathering opportunity; or a significant investigative opportunity.

[39] An equivalent change has been made with respect to Equipment Interference warrants.

[40] Clause 100 contains equivalent provision in relation to equipment interference, and clauses 135 and 171 set out safeguards that apply before content that contains legally privileged material can be selected for examination following acquisition under a bulk warrant

[41] This change relates to all urgent warrants.

JC Recommendation 38: The Committee recommends that the language of the Bill be amended so that targeted interception and targeted equipment interference warrants cannot be used as a way to issue thematic warrants concerning a very large number of people.	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny pointed to the finding of the Investigatory Powers Tribunal[42] and the 2014 Annual Report of the Interception of Communications Commissioner,[43] both of which concluded that thematic warrants may be lawful provided that identification of the subject matter is sufficiently specific. The draft Codes of Practice for Interception and Equipment Interference seek to reflect these requirements.
JC recommendation 43: The Committee would like to see more safeguards for the sharing of intelligence with overseas agencies on the face of the Bill. These should address concerns about potential human rights violations in other countries that information can be shared with.[44]	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny points to the requirements set out in clause 47 (and clause 113 in the context of EI warrants), that the Secretary of State must be satisfied that satisfactory and equivalent handling arrangements are in place before sharing UK intercept material with an overseas authority. These have not changed substantively from the draft Bill.
JC Recommendation 47: The Home Office should review its proposals in relation to LPP to ensure that they meet the requirements of Article 8 and relevant case law	The ECHR Memorandum that accompanies the Bill points to the safeguards in relation to LPP in support of the conclusion that the measures in the Bill constitute a proportionate means of achieving a legitimate aim, as compliance with Article 8 would require. Particular emphasis is placed on the requirement for there to be exceptional and compelling circumstances in order to issue a warrant authorising the interception of such material.
JC Recommendation 48: The Committee recommends that the Home Office reconsiders the level of protection which the Bill affords to journalistic material and sources. This should be at least equivalent to the protection presently applicable under PACE and the Terrorism Act 2000.[45]	The Government's response to pre-legislative scrutiny states: "The Government is satisfied that the additional protections set out in the new draft Codes of Practice … are appropriate in relation to journalistic material. This reflects the fact that it is much harder to define in law what constitutes a journalist"
ISC Recommendation J(i): A Secretary of State may issue a Targeted Interception warrant if it is necessary for (a) national security; (b) preventing or detecting serious organised crime; or (c) economic well-being so far as is relevant to national security and relates to people outside the British Islands. This is unnecessarily confusing and complicated: if 'national security' is sufficient in itself, then *"economic wellbeing… so far as [is] relevant to the interests of national security"* is redundant, since it is a subset of the former. We have questioned both the Agencies and the Home Office on this matter and neither have provided any sensible explanation. In our opinion, this area is already sufficiently complex so drafters should seek to minimise confusion wherever possible. We therefore recommend that 'economic well-being' is removed as a separate category.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states: "The 'economic well-being' purpose for which warrants may be sought is not precisely identical to the 'national security' purpose. Consequently, removing 'economic well-being' from the Bill could have the effect of preventing the agencies from undertaking operations in future that they would be able to undertake today." This does not directly address the ISC's point that 'economic well-being' is expressed in the Bill as a subset of 'national security'.
ISC Recommendation J(vii): In the Committee's Report on *Privacy and Security*, we recommended that 'thematic' Targeted Interception warrants be used sparingly and subject to greater safeguards; unfortunately this has not been reflected in the draft Bill.	**The Government did not accept this recommendation.**

[42] IPT 14/85/CH *Privacy International and Greennet & Others v FCO & GCHQ*
[43] IOCCO Annual Report 2014
[44] This recommendation also related to Equipment Interference warrants
[45] This is a general recommendation that applies to all of the capabilities contained in the Bill

The Committee reiterates its earlier recommendation: as a minimum, 'thematic' warrants should be authorised for a shorter time period (one month, as opposed to the usual six) to ensure that they receive the greater scrutiny required	
ISC Recommendation J(xii): The statutory basis for the Agencies' exchange of material with international partners will continue to sit under general authorisations in the Security Service Act 1989 and the Intelligence Services Act 1994. The draft 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. The Committee recommends that the new legislation is amended to reflect this recommendation: the proportion of intercept material obtained from international partners is such that it is not appropriate to exclude it from legislation which purports to cover interception.	**The Government did not accept this recommendation.**
ISC Recommendation J(xiii): The Mutual Assistance warrant regime in the draft Bill seeks to replicate the infrequently used provisions in the Regulation of Investigatory Powers Act 2000 (RIPA) governing interception undertaken under Mutual Legal Assistance Treaties. The Committee considers that these warrants have been given greater prominence in the draft Bill than they deserve which may give a misleading impression as to their nature. We recommend this should be clarified. Clause 39 of the draft Bill seeks to replicate existing provisions in RIPA which give effect to the EU's Convention on Mutual Assistance in Criminal Matters, allowing interception in the UK to be conducted on behalf of a foreign partner. However, it omits the restriction in RIPA that the person being intercepted must be outside the UK. This therefore would allow for UK residents to be intercepted in the UK without a warrant being in place. Given that the Committee has not been given a reason for this omission, we presume this is a drafting error: in our view it is essential that the original RIPA safeguard is reinstated, and the communications of those in the UK properly protected.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that further conditions concerning interception in the UK conducted on behalf of a foreign partner will be specified in secondary legislation, including the stipulation that the subject must be outside the UK, where appropriate.

3.3 What did the reports on investigatory power say?

Anderson	ISC	ISR
Warrants should only be granted for the purposes of: Preventing or detecting serious crime (including giving effect to a mutual legal assistance agreement); or In the interests of national security (including safeguarding the economic well-being of the UK in a respect directly linked to the interests of national security).[46]	The targeted interception of communications is an essential investigative capability.[47]	
Specific interception warrants should be issued and renewed only on the authority of a Judicial Commissioner.[48] Where a warrant is sought for the purpose of protecting national security, and the purpose relates to the defence of the UK or the Government's foreign policy, the Secretary of State should have the power to certify that the warrant is required in respect of those interests.[49]	Ministers should continue to be responsible for issuing warrants, because they are able to take account of the wider context of warrants and are democratically accountable.[50]	Where a warrant is sought for a purpose relating to the detection or prevention of serious crime, it should be authorised by a judicial commissioner, and a copy provided to the Home Secretary. Where a warrant is sought for purposes relating to national security, the warrant should be authorised by the Secretary of State, subject to judicial review by a judicial commissioner. The review should take place before implementation of the warrant, except in urgent cases.
	Disclosure of the existence of a warrant should be permissible where the Secretary of State considers that this could be done without damage to national security.[51]	
Arrangements should be put in place for the consideration of urgent applications.[52]		
Specific interception warrants should be limited to a single person, premises or operation. Where a warrant relates to an operation, each person or premises to which the warrant is to apply should be individually specified in a schedule to the warrant.	Thematic warrants should be used sparingly and authorised for a shorter timescale than a targeted warrant.[53]	

[46] Recommendation 28
[47] Annex A, para A
[48] Recommendations 20 and 22
[49] Recommendation 30
[50] Ibid, paras FF & GG
[51] Ibid, para C
[52] Recommendation 31
[53] Ibid, para D

3.4 Debate and comment

Judicial authorisation

The question of the "double lock" of approval of warrants by Judicial Commissioners has been particularly contentious during the pre-legislative scrutiny process. Warrants under Parts 2, 5, 6 and 7 of the Bill are issued by the relevant Secretary of State, who must believe that the warrant is necessary on certain specified grounds,[54] and that the conduct authorised by the warrant is proportionate to what is sought to be achieved. The warrant must subsequently be approved by a Judicial Commissioner (save in urgent cases, where it may be approved, or refused subsequently). Clause 21, dealing with interception warrants, would provide that the Judicial Commissioner must review the Secretary of State's conclusions as to whether the warrant is necessary and proportionate, applying the same principles as would be applied by a court on an application for judicial review. Equivalent provisions exist for the other warrantry processes.

The Judicial Review test

Aside from the question of whether warrants should be authorised by Ministers or judges, much of the debate focused on the degree of scrutiny a Minister's decision would be subjected to under the judicial review test.

Judicial review is a type of court proceeding in which a judge reviews the lawfulness of a decision or action by a public authority, looking at the way in which a decision has been made, rather than the rights and wrongs of the conclusion reached. In this context the court is exercising a supervisory, rather than appellate jurisdiction. There are a number of grounds on which a court can determine whether or not a decision has been reached lawfully, including irrationality and proportionality. The courts can overturn a decision if it is so demonstrably unreasonable as to be irrational. The legal test is whether the decision is so unreasonable that no reasonable authority could have come to it. Where human rights or EU law are concerned, the test is one of proportionality, that is, whether the means employed to achieve the aim correspond to the importance of the aim, and whether they are necessary to achieve the aim.

What this means is that in judicial review proceedings, the court would not approach the situation as though it was responsible for making the decision in the first instance. Instead it would consider whether the decision-maker had gone about making the decision in the right way. Insofar as the decision-maker has a degree of discretion in arriving at a decision, the court cannot override the exercise of that discretion, even if it disagrees with the decision.

Because of this there have been suggestions that the Judicial Commissioner will merely be looking at the decision-making process,

[54] Including in the interests of national security or the detection or prevention of serious crime.

rather than the "merits" of the decision, and therefore that the significance of the judicial authorisation procedure has been overstated.

Lord Pannick QC, writing in the Times, suggested that criticisms of the judicial oversight scheme are unjustified, and that it adopts "the right balance in this difficult area":

> [I]t is well established that judicial review is a flexible concept, the rigour of which depends on the context. The Court of Appeal so stated in 2008 in the T-Mobile case.
>
> The closest analogy to the provisions in the draft bill is judicial review of control orders and Tpims (terrorist prevention and investigation measures). The Court of Appeal stated in the MB case in 2006 that judges applying a judicial review test must themselves consider the merits and decide whether the measure is indeed necessary and proportionate. It is true that the context there involves restrictions that vitally affect liberty — in the sense of freedom of movement. But I would expect the courts to apply a very similar approach in the present context, concerned as it is with the important issue of privacy. So those who are concerned that a judicial review test does not give judges sufficient control should be reassured.
>
> However, in a national security context, the judiciary adopts a self-denying ordinance, applying the principle stated by Lord Neuberger (president of the Supreme Court) and Lord Dyson (master of the rolls) in a Supreme Court judgment in July in the Beghal case. In a terrorism context, judges have a function that involves a "tension" between "vigilance" to ensure that the powers are exercised only where necessary and proportionate, and "circumspection", because of the superior knowledge and experience of the executive in assessing risks to national security. Judges also recognise the institutional responsibility of the home secretary who is answerable to parliament. Judges therefore accord the executive a margin of discretion.
>
> That tension, and margin of discretion, is inherent in judicial control of the exercise of powers relating to national security. It would apply even if the legislation were to adopt criteria other than those applied on a judicial review application. The margin of discretion does not alter the power and duty of the judges to scrutinise decisions intensely and to impose restraints where appropriate, depending, of course, on the circumstances of the individual case.[55]

The article draws an analogy with the role of the courts in the (now repealed) control order regime. Under the *Prevention of Terrorism Act 2005*, the Secretary of State had the power to impose control orders on individuals (restricting their movements, associations, access to communications) where they were suspected of involvement in terrorism but could not be prosecuted. Where a control order subject applied for the order to be revoked, there was a right of appeal against the Secretary of State's decision, in which the court was required to apply the "principles applicable on an application for judicial review".[56] In the case of MB, the Court of Appeal concluded that this should

[55] David Pannick, Safeguards provide a fair balance on surveillance powers, The Times, 12 November 2015

[56] Section 10(6)

encompass consideration of the merits of the decision, as Lord Pannick notes.[57]

The *Terrorism Prevention and Investigation Measures Act 2011* (TPIMs Act) provides for a system whereby the initial decision of the Home Secretary to impose a TPIM is subject to court approval. According to section 6, the court must decide whether the Home Secretary's decision is obviously flawed, applying the principles applicable on an application for judicial review.

Lord Pannick's analysis has been endorsed by the existing Interception of Communications Commissioner and the Intelligence Services Commissioner,[58] both of whom previously held high judicial office, and by David Anderson QC. Mr Anderson did however caveat his agreement with a reservation about the role of ministers in authorising law enforcement warrants:

> I would make one point in respect of which I think the double lock, in a sense, is unduly cumbersome. There may have been an echo of that from a previous witness. It is in relation to police warrants, which, in nearly all countries I know about, are perfectly straightforward: the police go to a judge and the judge gives them the warrant. It is not seen as an area where the intervention of a government Minister is necessary. I can see that, in national security matters, different criteria apply. Indeed, I recommended a double lock myself in relation to foreign policy and defence warrants. But in relation to police warrants, which are 70% of the whole and therefore represent 70% of those 2,300 warrants that the Home Secretary authorises every year, it seems to me that one could do without the politician or the Minister and go straight to the judicial commissioner. [59]

The issue - that the standard of review applied in judicial review proceedings varies depending on the context - was considered recently by the Supreme Court. Lord Mance stated:

> [B]oth reasonableness review and proportionality involve considerations of weight and balance, with the intensity of the scrutiny and the weight to be given to any primary decision maker's view depending on the context. The advantage of the terminology of proportionality is that it introduces an element of structure into the exercise, by directing attention to factors such as suitability or appropriateness, necessity and the balance or imbalance of benefits and disadvantages. There seems no reason why such factors should not be relevant in judicial review even outside the scope of Convention and EU law. Whatever the context, the court deploying them must be aware that they overlap potentially and that the intensity with which they are applied is heavily dependent on the context. In the context of fundamental rights, it is a truism that the scrutiny is likely to be more intense than where other interests are involved. But that proportionality itself is not always equated with intense scrutiny was clearly identified by Lord Bingham of Cornhill CJ in *R v Secretary of State for Health, Ex p Eastside Cheese Co [1999] 3 CMLR 123* , paras 41-49, … . As Lord Bingham explained, at para

---

[57] [2006] EWCA Civ 1140

[58] Joint Committee on the Draft Investigatory Powers Bill, Volume of Oral Evidence, 11 February 2016

[59] Joint Committee on the Draft Investigatory Powers Bill, Oral evidence, Q 68

> 47, proportionality review may itself be limited in context to examining whether the exercise of a power involved some manifest error or a clear excess of the bounds of discretion … .
>
> … But the right approach is now surely to recognise, as *de Smith's Judicial Review* , 7th ed (2013), para 11-028 suggests, that it is inappropriate to treat all cases of judicial review together under a general but vague principle of reasonableness, and preferable to look for the underlying tenet or principle which indicates the basis on which the court should approach any administrative law challenge in a particular situation. Among the categories of situation identified in *de Smith* are those where a common law right or constitutional principle is in issue.[60]

The Bill and explanatory notes do not provide any additional guidance regarding the standard of review to be applied in this context. Therefore, there is disagreement as to the approach that will be taken by the Judicial Commissioners in practice.

Witnesses from Liberty, Open Rights Group, Privacy International, and Big Brother Watch gave evidence to the Joint Committee on the Draft Bill on 9 December.[61] In response to questions on the subject of judicial authorisation, they submitted that there is nothing in the Bill to suggest that the standard of review will go beyond the traditional approach in judicial review proceedings of looking at the process that has been followed in reaching the decision. Shami Chakrabarti, Director of Liberty, questioned the view that judicial review on proportionality grounds, as would be required under the Bill, would allow for a full review of the evidence on which the decision has been made. She pointed out that, if the intention is to provide for a full merits review of the Secretary of State's decision, there are more straightforward ways of achieving this, one of which would be simply to remove the reference to judicial review.[62]

---

[60] Kennedy v Charity Commission [2014] UKSC 20, paras 54-55
[61] Joint Committee on the Draft Investigatory Powers Bill, Volume of Oral Evidence, 11 February 2016
[62] Q129

4. Part 3: Authorisations for obtaining communications data

4.1 What does the Bill do?

Clauses 53-54 would provide for the power to grant authorisations for obtaining communications data.

Chapter 2, Part 1 of RIPA currently governs authorisations for obtaining communications data

The public bodies listed in Schedule 4 ("relevant public authorities") would have the power to obtain communications data. These include law enforcement agencies (LEA), security and intelligence agencies (SIA), government departments, regulatory bodies and the NHS. Under Part 3 an authorisation may be granted where a designated person ("designated senior officer") at the public authority in question (also listed in Schedule 4) is content that a request is necessary and proportionate for one of 10 purposes:

- In the interests of national security;
- In the interests of preventing or detecting crime or preventing disorder;
- 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;
- In the interests of public safety;
- For the purposes of protecting public health;
- For the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- For the purpose of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any such injury or damage;
- To assist investigations into miscarriages of justice;
- To assist in identifying a person who has died or is unable to identify themselves because of a physical or mental condition; or
- For the purpose of exercising functions relating to the regulation of financial services and markets, or financial stability.

Public authorities can only obtain communications data for these purposes, and only certain authorities can use certain purposes (as listed in Schedule 4).

Authorisations must be given by a designated person who is independent of the operation or investigation in question, save in exceptional circumstances such as when there is an imminent threat to life. The authorisation may permit conduct for the purposes of obtaining data, including:

- Serving a notice on a telecommunications service provider that requires them to disclose the relevant data;
- Serving a notice on a telecommunications service provider that requests that they obtain and then disclose the relevant data;
- Acquiring the data directly from a communications service provider through a secure auditable system.

Clause 54 defines Internet Connection Records (ICRs) and places additional restrictions on the grant of authorisations. ICRs may only be obtained for the following purposes:

- To identify the sender of an online communication;
- To identify which communication services a person has been using, for example determining whether they are communicating through apps on their phone;
- Identifying where a person has accessed illegal content, for example an internet service hosting child abuse imagery.
- To identify which internet service is being used and when and how it is being used.

Local authorities would be prohibited from acquiring internet connection records for any purpose.

An **internet connection record** is a record of the internet services a specific device has connected to, such as a website or instant messaging application. It does not reveal every webpage that a person has visited, or what they did on a particular webpage

Clause 55 sets out the information that would need to be contained in an authorisation or authorisation notice, including the purpose for which it is granted and the conduct that is authorised.

Clause 56 would set a limit of one month on the duration of authorisation, and provides for renewal and cancellation.

Clause 57 would place a duty on CSPs to comply with requests for communications data in so far as is reasonably practicable.

Clauses 58-60 relate to the filtering of communications data. They would provide a power for the Secretary of State to establish a "Request Filter" system, whereby when a complex request for communications data is made by a public authority, any material that is not directly relevant to the investigation or operation would be filtered out before the data is supplied. Data that is not relevant would be deleted. Oversight of the Request Filter would be provided by the Investigatory Powers Commissioner, to whom would be submitted an annual report on the operation of the system, and an immediate report of any significant processing errors. **Clause 74** provides that the Secretary of State's powers in these provisions may be transferred to a public authority; **Schedule 5** contains further safeguards with respect to such arrangements.

Clauses 61-63 provide for the definition of "relevant public authority" and "designated senior officer" for the purposes of Part 3, as listed in Schedule 4. **Schedule 4** includes a table which lists the public authorities permitted to obtain communications data; the minimum office or rank of the designated senior officer; the types of communications data that may be obtained; and the purposes for which they may be obtained. The Secretary of State may modify these provisions through regulations.

Clauses 64-66 provide that local authorities are relevant public authorities for the purposes of Part 3, but they may only obtain communications data through a shared single point of contact service (see below), and with the approval of a relevant judicial authority. In England and Wales this would be a justice of the peace, in Northern Ireland a district judge, and in Scotland a sheriff.

Clause 67 provides that, before granting an authorisation, the designated senior officer would have to consult a single point of contact (SPoC), unless there are exceptional circumstances, such as a threat to life. A SPoC is an officer in a relevant public authority trained to facilitate lawful acquisition of communications data and effective cooperation between public authorities and CSPs. SPoCs would have a responsibility to advise those applying for the acquisition of communications data and designated persons that authorise the applications.

Clause 68 provides that a public authority would have to obtain the approval of a Judicial Commissioner before obtaining communications data for the purpose of identifying a journalist's source, unless there is an imminent threat to life. There is no requirement to notify the journalist or their legal representative of the application.

Clauses 69-71 provide for agreements to allow designated senior officers and SPoCs to be shared between public authorities.

Clause 72 provides that any conduct carried out in accordance with an authorisation or notice would be lawful.

Clause 73 creates an offence of unlawful disclosure of the existence of an authorisation. This is intended to prevent the 'tipping-off' of suspects or subjects of interest that their data has been sought, thus informing them that they are under suspicion.

Clause 76 provides for the extra-territorial application of Part 3. The Bill asserts that overseas CSPs that handle communications data of UK citizens would be covered by these provisions.

4.2 Changes following pre-legislative scrutiny

Key changes to the Bill and relevant recommendations

Change	JC	ISC
Clause 53 (7)(g) (previously 46(7)(g)) has been amended to remove the words 'in an emergency'. Previously, LEAs would only have been able to obtain communications data for the purpose of preventing death or injury in an emergency situation. This limitation has been removed.	**Recommendation 4** - We believe that law enforcement should be able to apply for all types of communications data for the purposes of 'saving life'	
The definition of ICR in **Clause 54(6)** (previously 47(6)) has been revised in an effort to make it clearer. Chapters 2 and 7 of the draft Code of Practice on Communications Data provide further information, guidance and examples	**Recommendation 7** – We recommend that the definition of Internet Connection Record should be made consistent throughout the Bill and that the Government should give consideration to defining terms such as 'internet service' and 'internet communications service'	
Clause 54 (previously 47) has been amended to add a fourth purpose for which ICRs can be sought: to determine which internet service is being used, and when and how it is being used	**Recommendation 9** – We recommend that the purposes for which law enforcement may seek to access ICRs should be expanded to include information about websites that have been accessed that are not related to communications services nor contain illegal material, provided that it is necessary and proportionate for a specific investigation	
Clause 63 (previously 56) has been amended so that the enhanced affirmative procedure is required for any change to the list of ranks and offices which would have the effect of reducing the rank of the person authorising the application. Clause 64 has been amended so that the enhanced affirmative procedure is required for any amendments to the rank held by a designated senior officer in a local authority.	**Recommendation 41**: The Committee agrees with the recommendation of the Delegated Powers and Regulatory Reform Committee (DPRRC) on modifications to the list of ranks and offices which must be held by a designated senior officer. We recommend that Clause 56(1) and Clause 57(4) should be amended accordingly.	
Clause 68 (previously 61) has been amended so as to remove the exemption for SIA from obtaining approval from a Judicial Commissioner prior to acquiring communications data for the purposes of identifying a journalistic source.		**Recommendation B:** Where additional protection is provided for sensitive professions, these safeguards must be applied consistently, no matter which investigatory power is used to obtain the information. The new legislation should be amended to rectify this inconsistency.

Other relevant recommendations

Recommendation	Response
JC Recommendation 3: We recommend that Parliament should give further consideration to defining the purposes for which local authorities should may be allowed to apply for communications data when the Bill is introduced	This recommendation was aimed at Parliament
JC Recommendation 5: We recommend that that the Government should publish in a Code of Practice alongside the Bill advice on how data controllers should seek to minimise the privacy risks of subject access requests for ICRs under the Data Protection Act 1998.	**The Government accepted this recommendation.** The draft Code of Practice on Communications Data includes suggestions for how subject access requests might be treated (11.13-11.21)
JC Recommendation 6: While we recognise that ICRs could prove a desirable tool for law enforcement agencies, the Government must address the significant concerns outlined by our witnesses if their inclusion within the Bill is to command the necessary support.	The documents supporting the revised Bill provide further detail and seek to address the points on the technical feasibility of ICRs raised by witnesses.[63]
JC Recommendation 8: We recommend that the Government should publish a full assessment of the differences between the ICR proposal and the Danish system alongside the Bill.	**The Government accepted this recommendation.** The Government has published an assessment of differences alongside the Bill.
JC Recommendation 39: The Committee is satisfied that the proposed authorisation process for targeted communications data is appropriate but recommends that extra protections for privileged and confidential communications should be applied in the same way as is proposed for journalists in Clause 61 (now clause 68).	**The Government did not accept this recommendation**. The Bill does not apply the same protections for privileged and confidential communications as it does for journalists in relation to communications data. However, the draft Code of Practice requires applicants to flag cases in which an application is made for access to data from people in privileged professions to the IPC.
JC Recommendation 40: The Committee recommends the removal of emergency procedures for communications data so that the Single Point of Contact (SPOC) process can never be bypassed.	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny stated that: "In very limited circumstances it is important that an emergency process is available … ."
JC Recommendation 49: The Committee recommends that if Clause 61 (now 68) remains in its present form the Bill should make it clear that RIPA and Clause 61 do not act so as to enable the investigatory authorities to avoid the application of PACE or the Terrorism Act and the ability they afford to media to know about an application for communications data and make representations as to the proposed acquisition.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny distinguishes the purpose of the Bill in obtaining communications data from CSPs, from that of PACE and the Terrorism Act 2000 in obtaining journalistic materials from journalists themselves.
JC Recommendation 50: The Home Office should review Clause 61 (now 68) to ensure that it meets the requirements of Article 10 ECHR.	**The government accepted this recommendation** by amending clause 68 to remove the exemption for SIA. The response to pre-legislative scrutiny states that clause 68 is Article 10 compliant, and points to the judgment of the IPT in News Group Newspapers v The Commissioner of the Metropolitan Police[64] as authority for the conclusion that the process for independent authorisation under the Bill is sufficient in this regard.

63

64 [2016] UKIPTrib 14_176-H

ISC Recommendation H: The approach towards the examination of Communications Data in the draft Bill is inconsistent and largely incomprehensible. The Committee recommends that the same process for authorising the examination of any Communications Data (including Related Communications Data) is applied, irrespective of how the Agencies have acquired the data in the first instance. This must be clearly set out on the face of the Bill: it is not sufficient to rely on internal policies or Codes of Practice.	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny explains the safeguards in place for the different methods for acquiring communications data and states that any "further authorisation processes for examination of all bulk CD would threaten to undermine the operational agility of the agencies without providing any further material protection for privacy."
ISC Recommendation I: The draft Bill provides for access to Internet Connection Records through a specific request to a Communications Service Provider under Part 3. This could be interpreted as being the only way in which Internet Connection Records may be obtained. However, this is misleading: the Agencies have told the Committee that they have a range of other capabilities which enable them to obtain equivalent data. In the interests of transparency, the draft Bill should be amended to make this clearer.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that Chapter 7 of the draft Code of Practice provides further information and clarity on how and for what purposes public authorities may obtain ICRs.
ISC Recommendation J(viii): The Committee recommended previously that there should always be a clear line of separation between investigative teams who request approval for a particular activity and those within the Agency who authorise it. The draft Bill requires this division when obtaining Communications Data but the Agencies are exempt from this requirement. Whilst we have been told that this would create an unnecessary burden and time delay, given how regularly the Agencies use Communications Data, we nevertheless consider separation an important matter of principle and recommend that this is reconsidered before legislation is brought forward.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that the exemption from the requirement for the designated senior officer to be independent from the investigation is not a blanket exemption and applies only in exceptional or particular cases.

4.3 What did the reports on investigatory powers say?

Anderson	ISC	ISR
Public authorities with relevant criminal enforcement powers should in principle be able to acquire communications data. There should be a mechanism for removing public authorities which no longer need the powers and for adding those which need them.[65]	Communications data do not require the same degree of protection as the full content of a communication. However, some categories of communications data have the potential to reveal details about a person's private life that are more intrusive than the basic 'who, when and where' of a communication, and therefore require greater safeguards.[66]	There should be a periodic review of which public bodies have the authorisation to use intrusive powers and all relevant applications from authorised public bodies to obtain communications data should be made via the National Anti-Fraud Network.[67]
Authorisations for the acquisition of communications data should be issued on the authority of a designated person authorised to do so by an authorising body.[68] Authorisations should only be given if the designated person is satisfied that it is necessary and proportionate to do so.[69]	There should always be a clear line of separation within the Agencies between investigative teams who request approval for a particular activity, and those within the Agency who authorise it.[70]	
When data is sought which relates to a person known to be a member of a professions that handles privileged or confidential information (such as doctors, lawyers, journalists, MPs or ministers of religion), the designated person should be required to ensure that special consideration is given to the possible consequences and the application is flagged to the new oversight body.[71]		
Where data is sought for the purpose of determining matters that are confidential or privileged, judicial authorisation should be sought.[72]		
Judicial authorisations should also be sought for novel or contentious requests.[73]		

[65] Recommendation 50
[66] Annex A, paras V & W
[67] Recommendation 4
[68] Recommendations 20 and 23
[69] Recommendation 55
[70] Ibid, para HH
[71] Recommendation 67
[72] Recommendation 68
[73] Recommendation 70.

4.4 Debate and comment

Internet connection records

Box 2: Retention of Internet connection records

What is an internet connection record (ICR)?

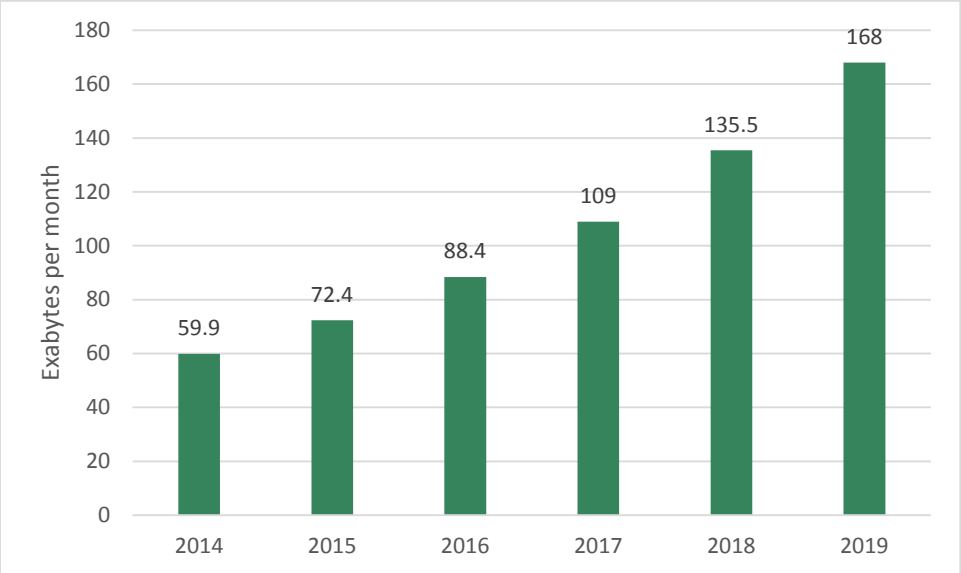
The Bill would create provisions for UK CSPs to retain internet connection records (communications data). The Home Office define communications data as the 'who', 'when', 'where' and 'how' of a communication. This is sometimes referred to as the 'metadata'. But it does not include the content of a communication—every web page that a person has visited or any action carried out on that web page.

Distinguishing between content and metadata is not necessarily straightforward because the web is not a single application. For a typical internet user, a number of different services are being used at any one time all of which blur the lines between content and metadata. At present, in order to understand what someone is doing online, CSPs effectively need to track all of the data all the time.

How much data will CSPs have to store?

A conservative estimate is that a tenth of all internet traffic could be considered as metadata. Cisco have forecast global internet traffic to nearly triple by 2019, up from nearly 60 exabytes per month in 2014.[74] One Exabyte is equal to 1 billion gigabytes. There are technical difficulties and concerns over the costs and of the feasibility of storing this much data both now and in the future. However, the Home Office point out that notices will only be served where necessary and proportionate and would not necessarily include all internet traffic which meets the communications data definition.

Forecast Global Monthly Internet Protocol (IP) Traffic, 2014-2019



Source: Cisco VNI Global IP Traffic Forecast, 2014–2015

The Joint Committee on the Draft Bill received a substantial quantity of evidence on ICRs.[75] Many witnesses suggested that the definition in the draft Bill was vague, both in terms of what information would be collected and who would collect it. A number of witnesses from the technology sector noted that ICRs did not currently exist, were not a recognised term in the industry and did not refer to datatypes

[74] Cisco, *Cisco VNI Global IP Traffic Forecast, 2014–2019*, May 2015

[75] Joint Committee on the Draft Investigatory Powers Bill Report, 11 February 2016, HL Paper 93, HC 651, paras 109 - 126

recognised by internet engineers. The Internet Service Providers Association suggested that the lack of clarity made it difficult to assess the impact on business and consumers. The Centre for Democracy & Technology told the Committee that:

> Definitions should be drafted to map unambiguously onto current features of Internet architecture and protocols so that communications service providers (CSPs) can understand what they will need to collect, retain and be prepared to produce with the proper legal authorisation.

CSPs who gave evidence indicated that they were in discussions with the Home Office regarding the definition of ICRs but were not yet clear exactly what they would comprise.

The Home Office subsequently submitted further written evidence to the Committee on the definition of ICRs.[76] This provided a diagram of the components of an ICR, and explained that

> Internet Connection Records is a record of the internet services a specific device is connected to, such as a website or instant messaging application. It is captured by the company providing access to the internet.
>
> Each ICR is a record of a single Internet Protocol event that occurs during the communication process and is made up of a number of components of communications data.

The Joint Committee acknowledged that it is difficult to provide definitions broad enough to capture the variety of ways in which communications are conducted on the internet, and may be conducted in the future, while still providing sufficient clarity, technical detail and precision, and recommended that the definition should be made consistent throughout the Bill. [77]

The Committee also concluded that it "did not believe that ICRs are the equivalent of an itemised telephone bill. However well-intentioned, this comparison is not a helpful one".[78]

The Science and Technology Committee also took evidence on ICRs.[79] Several witnesses questioned the Home Secretary's analogy with an itemised phone bill, noting that ICRs have the potential to be considerably more intrusive.[80]

Graham Smith[81] pointed out that the definition of ICR in clause 47 (now 56) of the Bill differed from the way in which relevant communications data are defined in clause 71 (now 78). He suggested that it would be helpful if the Home Office provided full, detailed and clear technical information about what data-types it believes would fall within these definitions.

---

[76] Written evidence from the Home Office (IPB0146), Volume of Written Evidence, p 522
[77] Para 122
[78] Para 126
[79] Investigatory Powers Bill: technology issues, Science and Technology Committee, HC 573, February 2016
[80] Paras 20-21
[81] Partner at Bird & Bird and editor of the Cyberleagle blog

Open Rights Group considered that the definition used in the (original) Operational Case for the Retention of Internet Connection Records was narrower than that contained in the Bill, which could be used for a much broader range of purposes than those stated in the guidance.

The Committee concluded that definitions in the Bill needed to be revised to ensure consistency and clarity.

Responding to the revised Bill, techUK has praised the fact that the Government has responded to this criticism, and that there is a single definition of ICRs that remains consistent throughout the course of the Bill, with references to ICRs appearing in both the authorisation and retention sections of the Bill. However, techUK also noted that

> Tellingly, the Codes of Practice admit that there will be no single set of data that constitutes an internet connection record and that in practice "it will depend on the service and service provider concerned". This acknowledgement highlights the difficulties that industry will face if required to generate and retains ICRs.[82]

In relation to costs, techUK noted that, although the Bill does not go as far as the Science and Technology Committee would have liked by putting 100% cost recovery on the face of the Bill, the supporting documents do reaffirm the Government's longstanding position of reimbursing 100% of costs.

[82] techUK Briefing and Response to New investigatory Powers Bill, 2 March 2016, techUK.org

5. Part 4: Retention of communications data

5.1 What does the Bill do?

This part would replace the existing data retention powers in DRIPA

Clauses 78 and 79 would provide a power for the Secretary of State to require the retention of communications data for up to 12 months and set out the matters that the Secretary of State should consider before giving a retention notice to a CSP.

Relevant communications data is defined as that which may be used to identify:

a. The sender or recipient of a communication (whether or not a person),

b. The time or duration of a communication,

c. The type, method or pattern, or fact, of communication,

d. The telecommunications system (or any part of it) from, to or through which, or by means of which, a communication is or may be transmitted, or

e. The location of any such system,

The Bill states explicitly that this includes internet connection records.[83]

Clause 80 would permit the recipient of a notice to refer it back to the Secretary of State for review, for example if they consider an obligation unreasonable. The Secretary of State must review the notice in consultation with the Technical Advisory Board and the Investigatory Powers Commissioner, and may then vary, revoke or confirm the notice.

Clauses 81 and 82 would require CSPs to take steps to ensure that retained data is stored securely, protected against unlawful disclosure, and destroyed when retention ceases to be authorised.

Clauses 83 and 84 deal with the variation, revocation and enforcement of notices. **Clause 84** also states that CSPs and the Information Commissioner may not disclose the existence or contents of a notice without the permission of the Secretary of State.

Clause 85 would provide for the application of Part 4 to postal operators and services in the same way as for telecommunications services and operators.

Clause 86 provides that CSPs based overseas may comply with a retention notice but they cannot be compelled to do so.

[83] For further information, see the Government's Operational case for the retention of Internet Connection Records, Gov.uk

5.2 Changes following pre-legislative scrutiny

Key changes to the Bill and relevant recommendations

Change	JC	S&T
Clause 78 (formerly 71) has been amended to include a specific reference to ICRs	**Recommendation 7** – We recommend that the definition of Internet Connection Record should be made consistent throughout the Bill and that the Government should give consideration to defining terms such as 'internet service' and 'internet communications service'	**S&T Recommendation 1:** While we are encouraged to learn of the Government's ongoing engagement with the internet industry, there seems still to be confusion about the extent to which 'internet connection records' will have to be collected. … Given the volume of data involved in the retention of ICRs and the security and cost implications associated with their collection and retention for the CSPs on whom ICR obligations might be placed, it is essential that the Government is more explicit about the obligations it will and will not be placing on industry as a result of this legislation.
Clause 84(4) has been added to the Bill which, together with paragraph 18.5 of the draft Code of Practice, would enable CSPs to disclose the existence and contents of a notice to the relevant oversight bodies and other CSPs, with permission of the Secretary of State.	**Recommendation 15:** "We understand the Government's position for not allowing the fact that a data retention notice has been served to be referred to in public. We suggest that some forum or mechanism … is made available so that CSPs subject to such notices can share views on how best to comply with them.	

Other relevant recommendations

Recommendation	Response
JC Recommendation 10: we urge the Government to consider the suggestion to work with the Information Commissioner's Office, the National Technical Assistance Centre and the Communications-Electronics Security Group at GCHQ … to draw up a set of standards for CSPs [in the area of data retention security].	Chapter 16 of the draft Code of Practice on Communications Data covers the security, integrity and destruction of retained data
JC Recommendation 11: While we do not agree that 100% cost recovery should be on the face of the Bill, we do recommend that CSPs should be able to appeal to the Technical Advisory Board on the issue of reasonable costs	The Government has not included a direct appeal for CSPs to the Technical Advisory Board on the issue of costs, however clause 80 provides for a route of appeal to the Secretary of State, who would be required to consult the TAB and the IPC before reaching a decision
JC Recommendation 12: Our view is that the Government should provide statutory guidance on the cost recovery models, and that particular consideration should be given to how the Government will support smaller providers served with data retention notices.	The Government has not included detailed models for cost recovery. However, the section in the draft Code of Practice for Communications Data has been significantly expanded, and makes specific reference to the fact that smaller CSPs may require additional resources in order to comply with notices.

JC Recommendation 13: The Bill should be amended to make [the fact that CSPs will not be required to retain third party data] clear, either by defining or removing the term 'relevant communications data'	The Bill has not been amended to reflect this recommendation; the definition of 'relevant communications data' in clause 78 (previously 71) is largely unchanged. However, the draft Code of Practice includes a section on third party data, which includes a statement that "A retention notice cannot require a CSP to retain third party data" (2.71)
JC Recommendation 14: We recommend that the Government should clarify the types of data it expects CSPs to generate and in what quantities so that this information can be considered when the Bill is introduced.	The draft Code of Practice includes a section on the generation and processing of data (14.28-14.29)
S&T Recommendation 1: While we are encouraged to learn of the Government's ongoing engagement with the internet industry, there seems still to be confusion about the extent to which 'internet connection records' will have to be collected. This in turn is causing concerns about what the new measures will mean for business plans, costs and competitiveness. Although the Government maintains that ICR notices will be served on particular Communications Service Providers (CSPs) on a case by case basis in a way which takes account of the circumstances of the particular communications provider, based on the text of the draft Bill some envisage a situation where ICRs could be required from all CSPs. Given the volume of data involved in the retention of ICRs and the security and cost implications associated with their collection and retention for the CSPs on whom ICR obligations might be placed, it is essential that the Government is more explicit about the obligations it will and will not be placing on industry as a result of this legislation. (Paragraph 30)	The response to pre-legislative scrutiny states that Part 4 of the Bill sets out the factors that must be taken into account when deciding whether it is necessary and proportionate to serve a data retention notice. The draft Code of Practice provides information about what ICRs are and the practical steps the Government will take to consult CSPs before issuing notices.
S&T Recommendation 7: Given the speed with which this legislation must be in force, the Government must work with industry to improve estimates of all of the compliance costs associated with the measures in the draft Bill, for meeting ICR-related and other obligations, as a matter of urgency. Should the measures in the draft Bill come into force, it will be important for Parliament to have access to information on actual costs incurred in order to assess the proportionality and economic impact of the investigatory powers regime and its effectiveness. (Paragraph 65)	The response to pre-legislative scrutiny states that the Government will continue to work with industry to improve cost estimates, but that it is unlikely that final costs will be published during the passage of the Bill.
S&T Recommendation 8: Larger CSPs may be able to take some assurance from the Government's commitment to meet their "reasonable" costs and avoid putting any affected businesses "at commercial disadvantage". However, smaller CSPs may not be certain that they will be served with a notice to collect ICRs and, if they do have to, whether their costs will in fact meet the Government's 'reasonable costs' criteria for reimbursement. The Government should reconsider its reluctance for including in the Bill an explicit commitment that Government will pay the full costs incurred by compliance. (Paragraph 66)	**The Government did not accept the recommendation** that 100% cost recovery should be on the face of the Bill.

S&T Recommendation 9: The Government intends to publish draft Codes of Practice when it introduces the Bill itself, later this year. It is essential that this timetable does not slip and that the Codes of Practice are indeed published alongside the Bill so they can be fully scrutinised and debated. The Government should reduce uncertainty about compliance burdens for businesses, proportionality and about cost recovery, by explicitly addressing such issues in the Codes of Practice. These Codes of Practice should clearly address the requirements for protecting ICR data that will have to be retained and managed by CSPs, along with the security standards that will have to be applied to keep them safe. Businesses based in the UK and those serving UK customers should not be placed at a commercial disadvantage compared with their overseas competitors. (Paragraph 71)	**The Government accepted this recommendation**. The response to pre-legislative scrutiny states that the six draft Codes of Practice published alongside the Bill contain information on all the issues which the Committee has suggested.

5.3 What did the reports on investigatory powers say?

Anderson	**ISC**
The Home Secretary should be able by Notice to require service providers to retain relevant communications data for periods of up to one year.[84]	It is essential that the agencies maintain the ability to access communications data.[85]
Government should formulate an operational case for adding web logs (internet connection records) to the data categories that CSPs may be required to retain. Full consideration should be given to alternative means of achieving those purposes. If a sufficiently compelling operational case has been made out, a rigorous assessment should then be conducted of the lawfulness, likely effectiveness, intrusiveness and cost of requiring such data to be retained. [86]	
The rules regarding retention of data should be compliant with EU law (as set out in the Digital Rights Ireland case) and the European Convention on Human Rights.[87]	

[84] Recommendation 14
[85] Annex A, para U
[86] Recommendation 15
[87] Recommendation 16

6. Part 5: Equipment Interference

Box 3: Equipment interference

Equipment interference (also known as Computer Network Exploitation (CNE)) is the practice of gaining access to people's devices and computers in order to obtain data, such as geolocation, texts and emails.

Equipment interference is not passive. It is more likely to involve actively breaking into an adversary's computer network in order to monitor, disrupt, deny or degrade their communications. This could be as straightforward as using someone's login credentials to gain access to data held on a computer. But there are also more sophisticated means of gaining access to people's devices and computers, such as through infecting them with malware.

Equipment interference is one way in which law enforcement agencies can get access to otherwise encrypted communications.

6.1 What does the Bill do?

Clauses 88-90 would provide for warrants for equipment interference. There would be two types of warrant:

- Targeted equipment interference warrant – would authorise the interference with equipment for the purpose of obtaining communications, private information or equipment data.[88] It may authorise the recipient to obtain, disclose, monitor and examine any such material. Any conduct necessary can be carried out in order to give effect to an equipment interference warrant, except activities which should be carried out under an interception warrant.
- Targeted examination warrant – would authorise the person to whom it is addressed to carry out the examination of material obtained under a bulk equipment interference warrant.

Warrants may cover a particular person or persons; organisation or organisations; or a particular location or locations where the relevant equipment is located.

A targeted warrant may also relate to equipment where there is a common link between multiple people, locations or organisations where the interference is for the purpose of the same investigation or operation or equipment that is being used for a particular activity. These warrants are sometimes referred to as 'thematic'.

Clauses 91-96 deal with the authorisation of equipment interference warrants. Warrants may be issued by the Secretary of State following an application by or on behalf of the heads of the intelligence services, namely GCHQ, the Security Service (MI5) and the Secret Intelligence Service. They must be necessary on the grounds of national security, preventing or detecting serious crime, or in the interests of the economic well-being of the UK, and proportionate. In the case of serious crime in Scotland, warrants must be authorised by Scottish Ministers. Warrants may also be issued to the Chief of Defence Intelligence, but only for national security purposes. Decisions to sign

Equipment interference is currently carried out using powers in the Intelligence Act 1994 and the Police Act 1997, covering SIA and LEA respectively. These provisions would not be repealed by the Bill. This is because the Bill only deals with the use of EI for the purposes of obtaining communications, equipment data and other information, whereas the existing powers are used for additional purposes

[88] Equipment data is defined by clause 89.

warrants must be taken personally by the Secretary of State or Scottish Minister, and where the purpose of the application is to obtain the communications of a parliamentarian, the Prime Minister must be consulted.

Clause 96 would provide that warrants may be applied for law enforcement officers and issued by a law enforcement chief, for the purpose of preventing and detecting serious crime, subject to the same test of necessity and proportionality. Warrants may in some circumstances be issued for purposes other than serious crime, where necessary to prevent death, injury or damage to a person's physical or mental health, or mitigate injury or damage to physical or mental health. This power is limited to certain agencies [see Schedule 6].

Clauses 97-99 provide that, as with interception warrants, equipment interference warrants must be approved by a Judicial Commissioner, applying the same principles as in an application for judicial review. In urgent cases, approval must be sought after the warrant has been issued. Where a Judicial Commission decides to refuse an urgent warrant, he or she may also direct that the material obtained be destroyed, or impose conditions as to its use or retention.

Clause 100 sets out additional safeguards which would apply when the purpose of a targeted equipment interference or examination warrants is to obtain items which are subject to legal privilege. In such cases the warrant would need to make clear that this was the intention. The person issuing the warrant would need to be satisfied that there were exceptional and compelling circumstances which would justify acquisition, and that there were adequate handling arrangements in place.

Clause 101 sets out the information that would need to be included in a warrant application, such as the intended activities and reasons why the warrant is needed.

Clauses 102-108 provide for the duration, renewal, modification and cancellation of warrants. Modifications, such as additions to the types of equipment covered by the warrant, may be made by the Secretary of State or Scottish Minister (or their delegates). In urgent cases it would be possible for modifications to be made without such approval by the person to whom the warrant was addressed. However this would be subject to subsequent approval, either by a Judicial Commissioner in the case of LEA warrants, or by an official designated by the Secretary of State or Scottish Minister in the case of SIA warrants.

Clauses 109 and 110 provide that the recipient of a warrant may serve a copy of it on anyone they think may be able to assist, including a person outside the UK.

Clause 111 places a duty on telecommunications providers to assist with the implementation of equipment interference warrants.

Clauses 112 and 113 would require that safeguards be put in place to protect any data acquired and that equivalent safeguards should be in place before material is shared with an overseas agency.

Clause 114 would create a duty not to make unauthorised disclosures in relation to the existence or details of a warrant or material obtain thereunder. Any disclosure would be classed an unauthorised apart from "excepted" disclosures provided for by **clause 115**. As with interception warrants, these exceptions are for disclosures authorised by the warrant; disclosures made to or authorised by a Judicial Commissioner or to an oversight body; disclosures in relation to legal proceedings; and general disclosures that do not relate to any particular warrant.

Clause 116 would provide for an offence of unauthorised disclosure of the existence or details of such a warrant.

Clause 117 would provide that certain LEAs may only apply for warrants where there is a connection to the British Islands.

6.2 Changes following pre-legislative scrutiny

Key changes in the Bill and relevant recommendations

Change	Recommendation
Clause 96 (previously 89) has been amended with the addition of a new subsection (2). Subsection 2 would enable a law enforcement chief (listed in Part 1 of Schedule 6) to issue an EI warrant for the purpose of preventing death or injury or damage to a person's physical or mental health, or mitigating any such damage.	See below at 6.4 for discussion of this change
Clause 98 (previously 91) has been amended to allow for the urgent approval of examination warrants, in additional to targeted EI warrants.	

Other relevant recommendations and responses

Recommendation	Response
JC Recommendation 18: We recommend that the Government should produce a Code of Practice on [EI] to cover the activities both of the security and intelligence agencies and of law enforcement.	**The Government accepted this recommendation.** The Equipment Interference draft Code of Practice published alongside the Bill covers the security and intelligence agencies and law enforcement.
JC Recommendation 19: We recommend that the Government should produce more specific definitions of key terms in relation to EI to ensure greater confidence in the proportionality of such activities and that a revised Code of Practice is available alongside the Bill.	Chapter 2 of the draft Code of Practice provides further information on key terms.

JC Recommendation 20: We acknowledge the importance of data protection in relation to EI activities. We recommend that the assessments undertaken by Judicial Commissioners when authorising warrants should give consideration to data protection issues.	**The Government did not accept this recommendation.** Clause 112 (previously 103) has not been amended substantially in relation to data protection issues. It requires the issuing authority to ensure that arrangements are in place for securing information obtained under EI warrants. There is no specific requirement for Judicial Commissioners to consider data protection issues when issuing warrants. Chapter 6 of the draft Code of Practice refers to data protection only to note that the authorised activities would otherwise constitute an offence under data protection legislation.
JC Recommendation 21: We further recommend that the Home Office should make clear in the explanatory notes to the Bill or in a Code of Practice how EI activities can be conducted within the constraints of data protection legislation.	**The Government accepted this recommendation.** Chapter 6 of the draft Code of Practice states that clause 88(5)(b) makes lawful any conduct taken in pursuance of a warrant that would otherwise be an offence under Data Protection legislation.
JC Recommendation 22: We urge the Government to consider how it will reconcile the understandable desire of law enforcement and the security and intelligence services to keep their techniques secret with the need for evidential use and disclosure regimes [with respect to material acquired through EI] in legal proceedings.	**The Government accepted this recommendation.** Chapter 8 of the draft Code of Practice has a section on the use of material as evidence (8.4-8.7)
JC Recommendation 26: We recommend that applications for targeted and bulk EI warrants should include a detailed risk analysis of the possibilities of system damage and collateral intrusion and how such risks will be minimised. We also recommend that such warrants should detail how any damaged equipment will be returned to its previous state at the point that the authorisation or operational need ceases.	The draft Code of Practice includes guidance on proportionality and how collateral intrusion should be considered in any decision to issue a warrant, and on the considerations that should be made in regards to the security of networks and systems.
JC Recommendation 27: We recommend that the Code of Practice on equipment interference should set out how individuals and companies should be engaged with when conducting authorised EI activities to make the process more transparent and foreseeable.	**The Government accepted this recommendation.** Chapter 6 of the draft Equipment Interference Code of Practice considers the "Provision of reasonable assistance to give effect to a warrant" (6.5-6.14) and contributions towards costs (6.15-6.21)
JC Recommendation 35: We recommend that the approach to targeted equipment interference warrants should be standardised and that all modifications should be subject to judicial authorisation.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states: "The Government considers that it is necessary to maintain different authorisation processes for modifications to equipment interference warrants in order to maintain an element of independent oversight of modifications. The distinction reflects the different authorisation regimes for the issue of EI warrants for law enforcement and the security and intelligence agencies."
ISC Recommendation C: The Committee recommends that all IT operations are brought under the provisions of the new legislation. This will ensure that all types of Equipment Interference are governed under the same legislation, with the same authorisation process and same safeguards.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny explains that the Bill would bring together existing powers to obtain communications and communications data, reflecting the recommendations of the three reports. It does not seek to legislate for all the powers available to SIA.

ISC Recommendation D: The Committee acknowledges that the Agencies need the capability to undertake Equipment Interference as necessary. However, the Committee has not been provided with sufficiently compelling evidence as to why the Agencies require Bulk Equipment Interference warrants, given how broadly Targeted Equipment Interference warrants can be drawn. The Committee therefore recommends that Bulk Equipment Interference warrants are removed from the new legislation.	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny states that: "Further evidence on the operational requirements for bulk equipment interference warrants has been provided to the [ISC] in advance of publication of the revised Bill".
ISC Recommendation E: The Committee recommends that the new legislation should require the Agencies to obtain a Targeted Equipment Interference warrant for an operation overseas whenever it is practical to do so.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny explains that the draft Code of Practice provides greater clarity on where is would not be operationally feasible for the security and intelligence agencies to seek a targeted EI warrant when conducting operations overseas and on the circumstances in which the agencies would be expected to seek an EI warrant.
S&T Recommendation 5: The Government states that the draft Bill introduces no substantive changes to the existing 'equipment interference' regime. It has made the practices more visible to the public and industry, however, and it remains to be seen whether this greater visibility affects the nature or extent of such activity in practice. Some sectors of the communications industry have concerns that equipment interference could jeopardise their business model; for example those producing and distributing open source data. They have a concern that because, as now, CSPs will not be permitted to reveal any equipment interference, their clients may assume that it is used. (Paragraph 50)	The response to pre-legislative scrutiny states that the draft Code of Practice explains the consultation process with CSPs and any impact on business will be considered as part of the necessity and proportionality determination.
S&T Recommendation 6: As ever, the fight against serious crime should be appropriately balanced with the requirement to protect and promote the UK's commercial competitiveness. We believe the industry case regarding public fear about 'equipment interference' is well founded. The Investigatory Powers Commissioner should carefully monitor public reaction to this power and the Government should stand ready to refine its approach to 'equipment interference' if these fears are realised. Taking into account security considerations, the Investigatory Powers Commissioner should report to the public on the extent to which such measures are used. (Paragraph 51)	The response to pre-legislative scrutiny indicates that the Government believes that the oversight arrangements in the Bill are sufficient to meet this recommendation.

6.3 What did the reports on investigatory powers say?

Anderson	ISC
Equipment interference (referred to as CNE) should be brought into the new law and made subject to equivalent conditions as those recommended in relation to interception and the acquisition of communications data.[89]	Consideration should be given to creating a specific authorisation regime in relation to the use of IT Operations against computers or networks in order to obtain intelligence.

6.4 Debate and comment

TechUK have criticised the Government's response to the Committees' recommendations on EI:

> Neither the face of the Bill nor the Codes of Practice acknowledge the dangers inherent within equipment interference provisions. In fact, the key recommendations by the Committees that attempted to safeguard the use of equipment interference have all been ignored and in some instances EI powers have been extended, rather than limited.
>
> For example, despite the draft Codes of Practice on Equipment Interference requiring EI warrants to include "an assessment of any risks to the security or integrity of systems or networks", this assessment on the face of it seems different to the Joint Committee's recommendation of a "detailed risk analysis of the possibilities of system damage and collateral intrusion and how such risks will be minimised".
>
> Furthermore, under provisions in the new Bill police officers will now be able to use EI for "threat to life" situations. The new Bill also provides for the Secretary of State to authorise bulk EI warrants in urgent circumstances. The concerns regarding bulk equipment interference, and the ISC recommendation that bulk equipment interference be removed from the Bill, have therefore been ignored.
>
> There are therefore no provisions within the Bill or Codes of Practice relating to the importance of network integrity and cyber security. Neither is there a requirement for agencies to inform companies of vulnerabilities that may be exploited by other actors. It is important that EI does not introduce new vulnerabilities into systems and the detailed risk analyses that the Joint Committee recommended would help any assessment of proportionality.[90]

Clause 96 has attracted some more specific comment. Subsection (2) contains a new provision that would provide for an additional basis on which law enforcement agencies could obtain equipment interference warrants. In the draft Bill targeted EI warrants could only be used by law

[89] Recommendations 6 and 21

[90] techUK Briefing and Response to New investigatory Powers Bill, 2 March 2016, techUK.org

enforcement agencies for the purpose of preventing or detecting serious crime. This would not have provided for law enforcement to use equipment interference to save a life or to locate a vulnerable person.

Currently, "property interference" powers for law enforcement agencies, under which equipment interference is carried out, are provided for by section 93 of the *Police Act 1997*.[91] This provides that an authorising officer may authorise "the taking of such action, in respect of such property in the relevant area, as he may specify" where the authorising officer believes it is necessary for the purpose of preventing or detecting serious crime.

According to the Home Office, law enforcement agencies currently use property interference for "threat to life" purposes in exceptional circumstances. The use of property interference in this way is not provided for in legislation but is overseen by the Office of Surveillance Commissioners, who are content that law enforcement agencies should be able to authorise this conduct in limited exceptional circumstances.

The Guardian noted in relation to this change that

> [F]ar from climbing down over her proposals, [Theresa May] intends to expand the scope of its most controversial new powers – the collection and storage for 12 months of everyone's web browsing history, known as internet connection records – and state powers to hack into computers and smartphones.
>
> …
>
> [The Bill] will extend the use of state remote computer hacking from the security services to the police in cases involving a "threat to life" or missing persons. This can include cases involving "damage to somebody's mental health", but will be restricted to use by the National Crime Agency and a small number of major police forces.
>
> …
>
> Documents published alongside the bill today describe the position as having changed as it was not referenced in the draft bill. However it reflects current police practice. The fact that it was not included in the draft bill was an omission that is being corrected in the final bill.
>
> The Home Office said the hacking powers dated from the 1997 Police Act and would most likely only be used in "exceptional circumstances" such as finding missing people. They would require a "double-lock" warrant with ministerial authorisation and judicial approval.
>
> …
>
> The Home Office's claim that the legalised hacking powers had been missed out of the original draft bill and so escaped the process of pre-legislative scrutiny was greeted with scepticism by at least one member of the scrutiny committee.[92]

The Telegraph also picked up on this change:

---

[91] According to the Home Office Factsheet: Targeted Equipment Interference

[92] Snooper's charter: wider police powers to hack phones and access web history, *The Guardian*, 1 March 2016

> [I]t has emerged that [the police] also already have the power to covertly glean personal data for the purposes of "preventing death or injury or damage to a person's physical or mental health".
>
> It raises the prospect police could have been accessing communications data for common investigations such as assaults, missing persons or suicide risks. So-called "equipment interference" can include remotely hacking in to phones or computers, or by-passing security on seized equipment.[93]

[93] Snoopers': charter: Police have been able to hack into phones and computers for routine investigations for years, The Telegraph, 1 March 2016

7. Part 6: Bulk warrants

7.1 What does the Bill do?

Chapter 1: Bulk interception warrants

Clauses 119-137 deal with bulk interception warrants. Bulk interception warrants would allow for the collection of a volume of communications of persons who are outside the British Islands.[94] This would be followed by the selection of specific communications to be read, looked at or listened to.

Bulk interception warrants are currently provided for by section 8(4) of RIPA. This would be repealed

Warrants would only be available where the main purpose was to obtain overseas related communications or secondary data on specific grouds, one of which must be national security.

Warrants could only be applied for by or on behalf of the heads of the intelligence services and must be issued personally by the Secretary of State, subject to the approval of a Judicial Commissioner. Warrants should specify the operational purposes for which any content or secondary data obtained would be selected for examination.

Clause 122 provides that where a warrant is likely to require the cooperation of an overseas CSP, the Secretary of State should consult with the CSP before issuing the warrant, and must consider a number of factors, including the costs and technical feasibility of complying.

Clauses 128 and 129 provide that major modifications to warrants should be made by the Secretary of State and approved by a Judicial Commissioner, except in urgent cases, where the Judicial Commissioner would have five working days to approve or refuse the modification.

Provisions for implementation and safeguards replicate those relating to targeted interception warrants.

Clause 134 provides for safeguards relating to the examination of intercepted content and secondary data which has been acquired under a bulk interception warrant. Material could only be examined where necessary for the operational purposes stated in the warrant and proportionate. A targeted examination warrant would be required to examine material relating to a person known to be in the British Islands, subject to approval by a Judicial Commissioner.

Clause 135 would provide additional safeguards in relation to material subject to legal privilege. Where the purpose of selecting intercepted material for examination was to identify items subject to legal privilege, it would only be possible to select that content with the approval of a senior official appointed by the Secretary of State. The senior official could only give approval if there were sufficient safeguards in place in respect of handling the material, and if there were exceptional and compelling circumstances making it necessary. The Investigatory Powers Commissioner should also be informed if such items were retained.

[94] "Overseas-related communications" are communications that are sent or received by individuals outside the British Islands.

Chapter 2: Bulk acquisition warrants

Clauses 138-153 relate to the acquisition of communications data in bulk.

Bulk acquisition of communications data is currently provided for by section 94 of the Telecommunications Act 1984, which will be repealed.

Many of the same provisions apply as to bulk interception warrants. Bulk acquisition warrants may only be sought by the intelligence agencies where national security is one of the purposes for which it is required. They would be granted by the Secretary of State, subject to approval by a Judicial Commissioner.

One key difference with bulk interception warrants is that bulk acquisition warrants would be available in respect of domestic, as well as overseas, communications.

CSPs may be required to disclose specified communications data in their possession or to obtain and disclose data not in their possession, and warrants may be issued on a forward looking basis.

The Secretary of State would be required to ensure arrangements are in place to limit the disclosure of data, and that data is held securely and destroyed when there were no longer grounds for retaining it.

Chapter 3: Bulk equipment interference warrants

Clauses 154-173 deal with bulk equipment interference warrants. Bulk equipment interference collects data relating to a number of devises; it is not targeted against particular persons, organisations or locations, or equipment that is being used for particular activities.

Bulk equipment interference is currently provided for by the Intelligence Services Act 1994 and the Police Act 1997

Bulk equipment interference warrants are aimed at obtaining overseas related communications, private information or equipment data. Provisions relating to the procedures for the issue and approval of warrants, implementation and safeguards are similar to those for the other bulk warrants, and in particular, bulk interception warrants. As with bulk interception, a targeted examination warrant is required in order to examine material of any person within the British Islands.

By contrast with the other bulk warrants, the Bill provides for the issue of bulk EI warrants in urgent cases without the need for approval by a Judicial Commissioner. A Judicial Commissioner would be required to approve the warrant within three working days, otherwise it would cease to have effect.

7.2 Changes following pre-legislative scrutiny

Key changes in the Bill and relevant recommendations

Clause 134 (previously 119) has been amended by the addition of a new subsection (8). Subsection (8) provides that the Secretary of State should be informed when a person whose communications have been intercepted under a bulk warrant and subsequently selected for examination, enters the UK unexpectedly or for a short period.	**ISC Recommendation J(iv):** Where GCHQ has collected UK material through Bulk Interception, the draft Bill allows a 'grace period' of five working days during which GCHQ can continue to examine the material without a specific warrant (solely with the authorisation of a senior official). This is the only scenario in which interception of a person known to be in the UK may take place without a warrant: it is therefore essential that additional safeguards are included in the new legislation - for example, through mandatory retrospective scrutiny by the Judicial Commissioners.
New **clause 158** provides for the approval of bulk EI warrants in urgent cases. As with other urgent warrants, a Judicial Commissioner would have three days within which to approve or refuse an urgent warrant issued by the Secretary of State	
Clause 164 (previously 143) provides that the Secretary of State would be able to make modifications to the conduct authorised by a warrant, or the operational purposes for which material acquired may be examined, in urgent cases. This would be subject to approval by a Judicial Commissioner within five working days.	

Other relevant recommendations and responses

Recommendation	Response
JC Recommendation 23: We recommend that the Government should publish a fuller justification for each of the bulk powers alongside the Bill. We further recommend that the examples of the value of the bulk powers provided should be assessed by an independent body, such as the [ISC] or Interception of Communications Commissioner.	**The Government accepted this recommendation**. An Operational Case for Bulk Powers document was published alongside the Bill.
JC Recommendation 24: We recognise that, given the global nature of the internet, the limitation of the bulk powers to "overseas-related" communications may make little difference in practice to the data that could be gathered under these powers. We recommend that the Government should explain the value of including this language in the Bill	Paragraph 6.8 of the Operational Case for Bulk Powers provides information about the global nature of communications traffic in order to illustrate why it would not be possible to avoid on occasion acquiring data relating to people in the UK. It further explains that the Bill provides additional protection for the content of such communications, in the form of a targeted examination warrant.
JC Recommendation 25: We recommend that the investigatory Powers Commissioner, within two years of appointment, should produce a report to Parliament considering the safeguards that exist [for bulk powers] and making recommendations if required	This recommendation was not aimed at the Government. This would be within the IPC's remit.

ISC Recommendation J (ii): The draft Bill provides that all Bulk warrants must specify the 'operational purpose' for which the material collected is being examined; however, no detail is provided as to what these operational purposes may be. The Committee considers this completely unsatisfactory: it contradicts the primary purpose of the draft Bill, to provide some much needed transparency in this area. The Committee therefore recommends that some detail on the 'specified operational purposes' for which material obtained under a Bulk warrant can be examined should be published – only then can Parliament properly evaluate the provisions of the new legislation in this area. We recognise, however, that it may not be possible to publish full details of the specified operational purposes. In such circumstances, this Committee would expect to be able to examine the secret material on behalf of Parliament, and to provide assurances or recommendations, as appropriate, to our parliamentary colleagues and to the public. However, the Committee has been told that the list of operational purposes has not yet been finalised by Government, and that it will not be finalised until after the Bill itself has been passed. The Committee is therefore unable to provide any reassurance that these 'operational purposes' are appropriate. We fail to see how Parliament is expected to approve any legislation when a key component, on which much of it rests, has not been agreed, let alone scrutinised by an independent body.	The response to pre-legislative states that a list of draft operational purposes has been provided to the ISC in advance of publication of the Bill. The ISC has not made further comment as to the sufficiency of this information.
ISC Recommendation J(iii): The draft Bill provides that, where the communications of a person known to be in the UK have been obtained via Bulk Interception or Bulk Equipment Interference, the Agencies require a Targeted Examination warrant before they can examine it. The draft Bill appears to suggest that Targeted Interception and Targeted Examination warrants are very similar. For the sake of clarity, further thought should therefore be given to creating a single warrant covering the content of the communications of a person in the UK, thereby ensuring that the same safeguards and authorisation procedures apply, irrespective of the way in which the material was obtained.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that although the processes for authorising the two categories of warrant are essentially the same, the fact that they authorise different activity means that they could not be brought together without adding significant complexity to the Bill.

7.3 What did the reports on investigatory powers say?

Anderson	ISC	ISR
There should be two types of bulk warrant: bulk interception warrants and bulk communication data warrants. A bulk interception warrant should never be applied for, approved or authorised when a bulk communications data warrant would suffice.[95]	Existing bulk interception is not indiscriminate, but involves a degree of targeting and filtering. It is essential that the Agencies can 'discover' unknown threats. Targeted techniques only work on known threats; bulk techniques are essential to enable the Agencies to discover those threats. Existing capabilities should remain available, provided that they are tightly controlled and subject to safeguards.[96]	The capability of the security and intelligence agencies to collect and analyse bulk data should be maintained with stronger safeguards as set out in the Anderson Report. Warrants should be subject to judicial authorisation.[97]
Bulk interception warrants should be targeted at communications of persons believed to be outside the UK. Consideration should be given to whether an analogous restriction is necessary or desirable in relation to bulk communications data. [98]	The Government should clarify the definition of 'external communications' –where at least one end is overseas - under RIPA in relation to internet communications, to make clear which communications are included.[99] Searching for and examining the communications of a person known to be in the UK, or a UK national who is overseas, should require a specific warrant authorised by the Secretary of State.	
As with intercept warrants, where the purpose relates to national security, the Secretary of State should certify that it is necessary for that purpose. Otherwise authorisation should be given by a Judicial Commissioner.[100]	The current arrangements in the Telecommunications Act 1984 lack clarity and transparency, and should be clearly set out in law, including safeguards and statutory oversight arrangements.[101]	

7.4 Debate and comment

The use of bulk powers has been contentious, with commentators and privacy campaigners describing the practice as 'blanket surveillance' or 'mass surveillance'. These are not characterisations the Government would recognise in respect of these activities.

In evidence to the Joint Committee on the Draft Bill, the Home Secretary said:

> The UK does not undertake mass surveillance. We have not undertaken, and we do not undertake, mass surveillance. That is not what the Investigatory Powers Bill is about … I would wish to

[95] Recommendation 42
[96] Annex A, paras F-M
[97] Recommendation 8
[98] Recommendation 44
[99] Ibid, para O
[100] Recommendations 46-48
[101] Ibid, para VV

> be very clear that mass surveillance is not what we are talking about.[102]

The Intelligence and Security Committee (ISC) considered the suggestion, stemming from the Snowden revelations, that government agencies were engaged in blanket surveillance of the internet in their 2015 *Privacy and Security* report (which, as is normal practice, has been redacted at various points):

> 57. The allegation arising from the NSA leaks is that GCHQ 'hoover up' and collect all internet communications. Some of those who gave evidence to this Inquiry said 'the Agencies are monitoring the whole stream all the time', referring to the 'apparent ubiquity of surveillance'.
>
> 58. We have explored whether this is the case. It is clear that both for legal reasons and due to resource constraints it is not: GCHQ cannot conduct indiscriminate blanket interception of all communications. It would be unlawful for them to do so, since it would not be necessary or proportionate, as required by RIPA.[50] Moreover, GCHQ do not have the capacity to do so and can only cover a fraction of internet communications:
>
> - Of the 100,000 'bearers' which make up the core infrastructure of the internet, GCHQ could theoretically access communications traffic from a small percentage (***). These are chosen on the basis of the possible intelligence value of the traffic they carry.
> - However, the resources required to process the vast quantity of data involved mean that, at any one time, GCHQ access only a fraction of the bearers that they have the ability to access – around ***. (Again, these are chosen exclusively on the basis of the possible intelligence value of the traffic they carry.)
> - In practice, GCHQ therefore access only a very small percentage (around ***%) of the internet bearers at any time.
> - Even then, this does not mean that GCHQ are collecting and storing all of the communications carried on these bearers – the processes by which GCHQ select which communications to collect are covered in the next section.
>
> 59. The proportion of bearers making up the internet that are accessed by GCHQ's 'bulk interception' systems is very small – and certainly far from the 'blanket' coverage of all communications that some are concerned is happening. Nevertheless, the volume of communications flowing across these bearers, and the number of people those communications relate to, is still extremely large. We therefore consider that 'bulk' remains an appropriate term to use when describing this capability.

[102] Q 271, cited in Draft Investigatory Powers Bill Report, para 329

…

> F. GCHQ's bulk interception capability is used either to investigate the communications of individuals already known to pose a threat, or to generate new intelligence leads, for example to find terrorist plots, cyber attacks or other threats to national security. It has been alleged – inaccurately – that this capability allows GCHQ to monitor all of the communications carried over the internet. GCHQ could theoretically access a small percentage (***%) of the 100,000 bearers which make up the internet, but in practice they access only a fraction of these (***%) – we detail below the volume of communications collected from these bearers. GCHQ do not therefore have 'blanket coverage' of all internet communications, as has been alleged – they have neither the legal authority, the technical capacity nor the resources to do so.

However, the term 'blanket surveillance' has been used to describe these activities by various organisations advocating the need for greater privacy protection. For example, in evidence to the ISC, Isabella Sankey of Liberty said that bulk interception was objectionable in principle:

> The objection is to both – the collection and interrogation without an appropriate framework. There is nothing passive about GCHQ collecting millions and millions of communications of people in this country… even if human beings are not processing those communications and it is being done by machines, that is a physical interception – a privacy infringement – and a model of blanket interception that we have not traditionally followed in this country.[103]

Liberty's evidence to the Joint Committee was also critical of the provisions covering bulk powers:

> Part 6 of the Draft Bill places the breathtakingly broad mass surveillance powers revealed by Edward Snowden and additional bulk surveillance practices on an explicit statutory footing. New powers to intercept, in bulk, 'external' communications (including vast swathes of domestic communications) and to acquire records of the entire nation's communications data are supplemented by powers permitting "industrial scale exploitation" (GCHQ's own words) of electronic devices and networks. Part 7 further extends blanket surveillance powers away from a focus on the population's communications and towards the acquisition and linking of all public and private sector personal data databases.[104]

In a blog responding to the publication of the draft Bill, Amnesty's Technology and Human Rights adviser Carly Nyst said:

> Blanket, indiscriminate interception and retention of people's communications by any other name is still mass surveillance and it can never be proportionate. If adopted in its current form, the IP Bill will authorise the intelligence services to intercept, in bulk, all email, text and internet communications in and out of the UK; demand phone and internet companies hand over entire databases full of records about what their customers do online and on their phones; acquire databases of other personal information from other companies and government departments, and hack into whole networks and millions of smartphones

---

[103] Cited at para 92

[104] Liberty's written evidence on the Draft investigatory Powers Bill, December 2015, liberty-human-rights.org.uk [accessed 11 March 2016]

> consecutively, rummaging through individuals' most private thoughts and records.[105]

Following publication of the Bill, the Open Rights Group said of the provisions on bulk powers:

> The final Bill does not contain any fundamental changes and the wholesale tapping of fibre optic cables revealed by Snowden will continue as before. The agencies will also continue to obtain the phone records of everyone in the UK, plus soon our full internet histories. The final bill ensures that nothing is out of bounds by using more general words to refer to the intercepted content and data, now referring to "anything obtained under the warrant". The agencies also gain more flexibility to modify warrants, separating the obtention of content and data, which can be changed without judicial approval during emergencies. [106]

The Joint Committee accepted the principle that bulk powers should be an additional resource to the agencies, and that they would not seek them if they did not believe they would be effective.[107] The Committee did acknowledge though that:

> It is possible that the bulk interception and equipment interference powers contained in the draft Bill could be exercised in a way that does not comply with the requirements of Article 8 as defined by the Strasbourg court. It will be incumbent upon the Secretary of State and judicial commissioners authorising warrants, and the Investigatory Powers Commissioner's oversight of such warrants, to ensure that their usage is compliant with Article 8.[108]

---

[105] Mass surveillance by another name, amnesty.org.uk
[106] The revised Investigatory Powers Bill: what has changed, 2 March 2016, Jim Killock, Pam Cowburn & Javier Ruiz, openrightsgroup.org [accessed 10 March 2-16]
[107] Report of the Joint Committee on the Draft Investigatory Powers Bill, para 340
[108] Para 331

8. Part 7: Bulk personal datasets

8.1 What does the Bill do?

The acquisition of **Bulk Personal Datasets** is currently governed by the Security Services Act 1989 and the Intelligence Services Act 1994

Clauses 174 - 193 would provide for bulk personal dataset (BPD) warrants. A BPD is a dataset containing information about a wide range of people, most of whom are not of interest to the security and intelligence agencies. Examples provided by the Home Office include lists of people who have a passport or firearms license.[109]

The intelligence services would only be able to retain or examine a BPD with a warrant, unless the material is governed by another regime contained in the Bill.

Two types of warrant would be available:

- A class warrant – authorises the intelligence services to retain or examine BPDs that fall within a class described in the warrant. According to the explanatory notes, datasets can be said to fall into a class because they are of a similar type and raise similar considerations (for instance in relation to the degree of intrusion and sensitivity and the proportionality of using the data).
- A specific warrant – authorises the intelligence services to retain and examine a BPD described in the warrant. These warrants are relevant where the dataset concerned does not fall within a class described by an existing BPD warrant, for example where a new or novel dataset is to be retained, or where the dataset may raise issues of sensitivity such that it would be appropriate for the Secretary of State to issue a specific warrant.

Both types of warrant would be subject to authorisation by the Secretary of State. She or he would need to believe that the warrant was necessary on the grounds of national security, serious crime or economic well-being where also relevant to national security, proportionate, and that satisfactory handling arrangements were in place. This would be subject to approval by a Judicial Commissioner.

As with other warrants in the Bill, the decision to issue must be made personally by the Secretary of State, and a procedure is prescribed for the issue of warrants in urgent cases. The duration, renewal, modification and cancellation of BPD warrants are also provided for, consistent with the rest of the Bill.

[109] Home Office Factsheet – Bulk Personal Datasets

8.2 Changes following pre-legislative scrutiny

Key changes to the Bill

New **clause 187** would provide for a procedure for the approval of major modifications – affecting the operational purposes – to BPD warrants, in urgent cases. Such modifications would be subject to approval by a Judicial Commissioner within five working days.	
Clause 189 (previously 164) has been amended to provide that where a BPD warrant ceases to have effect because it expires or is cancelled, SIA must apply for a new warrant within three months in order to continue to retain and examine the dataset.	**ISC Recommendation J(ix)**: Clause 164 of the draft Bill states that when a Class BPD warrant is not renewed, or is cancelled, the Secretary of State may (with the approval of a Judicial Commissioner) authorise the retention or examination of any of the material. This appears to circumvent the warrantry process: if the Agencies wish to retain and use information contained within a BPD, they should seek a new warrant. The Committee recommends that, in circumstances where a Class BPD warrant is not renewed, or is cancelled, and the Agencies wish to continue retaining or examining any of the material, a new Specific BPD warrant must be sought. The Committee therefore recommends that the Government amend this Clause accordingly.
Clause 190 now specifies time limits for the initial examination of the datasets. UK-originated dataset must be examined within three months, and a foreign-originated dataset must be examined within six months; in both cases, if the dataset is to be retained and is not already covered by an existing class BPD warrant, a specific BPD warrant must be applied for as soon as reasonably practicable and in any event within the specified time limit.[110]	**ISC Recommendation G**: Whilst it is reasonable to allow the Agencies a period of grace in which to apply for a Specific Bulk Personal Dataset warrant where a Bulk Personal Dataset has been obtained opportunistically, that period should be specified on the face of the new legislation to ensure that no Bulk Personal Dataset can be held without authorisation for an undue length of time. The Committee recommends that a time limit of one month is introduced for the Agencies to hold a UK-sourced Bulk Personal Dataset without a warrant temporarily whilst a specific warrant application is made and determined. In the case of overseas-sourced Bulk Personal Datasets, this time limit should be six months.

Other key recommendations and responses

Recommendation	Response
JC Recommendation 28: We recommend that the Home Office should produce its case for bulk personal datasets (BPDs) when the Bill is published.	**The Government accepted this recommendation.** The Government has published an operational case for bulk powers, including BPDs.
JC Recommendation 30: We believe that a draft Code of Practice on BPDs should be published when the Bill is introduced to provide greater clarity on the handling of BPDs, not least in relation to the provisions of the Data Protection Act 1998. To the greatest extent possible, the safeguards that appear in the Data Protection Act 1988 should also apply to personal data held by the security and intelligence agencies.	**The Government accepted this recommendation**. The Government has published a draft Code of Practice on BPDs. Chapters 4, 5 and 7 deals with safeguards.

[110] Previously, under clause 152(2) of the draft Bill, an agency was exempted from the requirement under clause 151(2) to obtain a warrant in order to retain a dataset, while an application for a dataset was made and determined. There was however no time limit to this state of affairs.

JC Recommendation 31: We also agree that existing powers for acquiring BPDs should be consolidated in this Bill and that any other powers for the security and intelligence agencies to acquire BPDs should be repealed.	**The Government did not accept this recommendation**. The response to pre-legislative scrutiny states: "The provisions in the Bill do not provide a power to acquire BPDs but instead apply robust, consistent safeguards to the handling of BPDs acquired by the security and intelligence agencies, including through the introduction of a new 'double lock', so that warrants authorised by the Secretary of State must be approved by a Judicial Commissioner. BPDs can be collected by a range of means, including through the use of other investigatory powers and through voluntary disclosures. The primary bases in law for the acquisition of bulk personal datasets are sections 2(2)(a) of the Security Service Act 1989 and 2(2)(a) and 4(2)(a) of the Intelligence Services Act 1994, sometimes referred to as the information gateway provisions. To separate acquisition of this type of data from other types when there is an existing framework for data acquisition would add undue complexity to the Bill and would risk undermining the existing information gateway provisions. Retaining the ability to obtain BPD under these provisions in law does not exempt the agencies from applying the strict safeguards in the Bill."
JC Recommendation 42: The Committee recommends that authorisations for bulk personal datasets should be required to be specific and provisions for class authorisations should be removed from the Bill. The provision relating to replacement datasets (Clause 154(6)) should also be removed.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states: "Class BPD warrants provide an appropriate means of authorising the retention and use of datasets that are similar in nature and in the level of intrusiveness. … The decision to issue a warrant for a particular class of data would be subject to approval by a Judicial Commissioner before being issued. … The provision for a replacement dataset would only be relevant where a specific BPD warrant has been authorised and is already in place. This is a pragmatic and sensible approach to situations where a dataset is regularly or continually updated… ."
ISC Recommendation F: The Committee considers that the acquisition, retention and examination of any Bulk Personal Dataset is sufficiently intrusive that it should require a specific warrant. We therefore recommend that Class Bulk Personal Dataset warrants are removed from the new legislation.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that Class BPD warrants are an appropriate way of authorising the retention of datasets that are similar in nature and in the degree of intrusiveness. The draft Code of Practice provides guidance on the factors relevant to deciding when to use a class warrant, and on reviewing the necessity of retaining individual datasets.

8.3 What did the reports on investigatory powers say?

Anderson	ISC
The existing audit and inspection functions of the current Commissioners should be transferred to the Independent Surveillance and Intelligence Commission, including the audit of the use by security and intelligence agencies of their holdings of bulk personal datasets[111]	Bulk datasets are an increasingly important investigative tool for the Agencies. In the interests of transparency, this capability should be clearly acknowledged and put on a specific statutory footing, along with provision for oversight.[112]

8.4 Debate and comment

The Joint Committee noted that many of their witnesses argued that it was not apparent from the draft Bill what information the Bulk Personal Datasets might include. The Information Commissioner's Office suggested that the examples provided by the Home Office were not helpful because they were already available to the security and intelligence agencies under pre-existing legislation. Suggestions from witnesses as to the kind of data that might be covered included medical records, immigration histories, tax returns, flight data, and financial data.

A number of witnesses suggested that certain types of dataset should be explicitly excluded, the common suggestion being medical records.[113]

The Committee acknowledged the case made by the Home Office for not providing detailed information as to the contents of bulk personal datasets, but concluded that the lack of that detail makes it hard for Parliament to give the power sufficient scrutiny.

[111] Recommendation 89
[112] Annex A, paras X & Y
[113] Report of the Joint Committee on the Draft Investigatory Powers Bill, paras 392-399

9. Part 8: Oversight arrangements

9.1 What does the Bill do?

Chapter 1: Investigatory Powers Commissioner and other Judicial Commissioners

Clauses 194 - 206 make provision for a new oversight framework.
Clause 194 would establish the office of the Investigatory Powers Commissioner, to be supported by a number of other Judicial Commissioners, all of whom must hold or have held high judicial office (together known as the Judicial Commissioners).

The Judicial Commissioners would be appointed by the Prime Minister following consultation with the Lord Chief Justice of England and Wales, the Lord President of Scotland, the Lord Chief Justice of Northern Ireland, the Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland.

The Investigatory Powers Commissioner would replace the existing Intelligence Services Commissioner, Surveillance Commissioner, and Interception of Communications Commissioner, and would have a broad remit to keep under review the use of investigatory powers.

The IPC would report annually to the Prime Minister, and would be able to report on other matters as he or she deemed necessary, or as requested by the Prime Minister.

Clause 198 would provide for a process whereby individuals can be informed of serious errors in the use of investigatory powers. A serious error would be a failure by a public authority to comply with a requirement over which the IPC has oversight which caused significant prejudice to the person concerned. In these circumstances the person concerned would be informed of their right to bring a case to the Investigatory Powers Tribunal (IPT).

Public authorities and CSPs would be subject to a requirement to provide the IPC with any information, documents or assistance required to carry out oversight functions.

Clause 203 would allow people to provide information to the Investigatory Powers Commissioner, regardless of any other legal restrictions that might exist in relation to that information.

Chapter 2: Other arrangements

Clause 207 provides for the Secretary of State to issue Codes of Practice governing the use of powers contained in the Bill, as set out in Schedule 7. These must include provision for the protection of journalistic sources and legally privileged or confidential material.

Clause 208 provides for a right of appeal from the IPT to the Court of Appeal on a point of law.

Clause 211 provides for the retention of a Technical Advisory Board and its composition.

9.2 What has changed following pre-legislative scrutiny?

Key changes to the Bill and relevant recommendations

Change	JC	ISC
Clause 194 (previously 167) has been amended to include a requirement that the Prime Minister consults with the Lord Chief Justice (LCJ) of England and Wales and his or her counterparts in Scotland and Northern Ireland before appointing Judicial Commissioners.	**Recommendation 53**: The LCJ should be responsible for appointing Judicial Commissioners.	
Clause 195 (previously 168) has been amended by the removal of subsections (6) and (7), which would have provided for a Judicial Commissioner to be removed from office on the grounds of inability, misbehaviour or a breach of the terms and conditions of appointment, by the IPC in consultation with the Prime Minister. However, clause 195 still provides that the Prime Minister would be able to remove a Judicial Commissioner from office in a range of circumstances.	**Recommendation 55:** We believe that the broad powers of dismissal contained in the draft Bill significantly impair the independence of the Judicial Commissioners. We therefore recommend that the Judicial Commissioners be subject to the same dismissal and suspension procedures as those applicable to serving senior judges: removal from office following a resolution of both Houses of Parliament and suspension and other disciplinary measures exercised by the Lord Chief Justice and Lord Chancellor.	
Clause 198 (previously 171) has been amended so that the Investigatory Powers Commissioner is able to report errors in the use of investigatory powers to individuals directly, rather than via the IPT	**Recommendation 57**: Clause 171 changes the existing powers of the relevant commissioners to report errors in the use of surveillance powers to the individuals affected by raising the applicable test and requiring the involvement of the Investigatory Powers Tribunal in making the decision. … We recommend that the Investigatory Powers Commissioner exercise the error-reporting power alone, without reference to the Investigatory Powers Tribunal.	
Clause 199 (previously 172) has been amended to make clear that the Judicial Commissioners can communicate with the IPT without reference to the Home Secretary	**Recommendation 65**: The Judicial Commissioners should be able to communicate with the Investigatory Powers Tribunal on a point of law without consulting the Home Secretary. Clause 172(3) should be redrafted to reflect this.	

Clause 201 (previously 174) has been amended to make clear that the Investigatory Powers Commissioner must include in an annual report, information about the results and extent of the use of the powers in the Bill.	**Recommendation 67**: The Investigatory Powers Commissioner's annual report must include information about the impact, results and extent of the use of powers in the Bill so effective public and parliamentary scrutiny of the results of the powers can take place.	
Clause 202 (previously 175) has been amended in order to make it clear that Judicial Commissioners have the power to initiate investigations.	**Recommendation 52**: The Judicial Commissioners or Commission should have the power to instigate investigations on their or its own initiative. This is vital in order to ensure effective and independent oversight. The current provisions in the draft Bill on the powers of the Judicial Commissioners do not make it clear that they have this power. We recommend that a power to initiate investigations should appear on the face of the Bill.	
Clause 202 has been amended to make clear that Judicial Commissioners would have access to all relevant technical systems where necessary for them to provide oversight	**Recommendation 63**: We recommend that the Judicial Commissioners should have a legal mandate to access all relevant technical systems required to ensure effective oversight of the powers contained in the Bill. This mandate should appear on the face of the Bill.	
New **Clause 203** would provide a route for CSPs and public authorities to refer complaints or concerns to the Judicial Commissioners, without breaching any restriction on the disclosure of information	**Recommendation 60:** We recommend the Bill should contain an explicit provision for Communication Service Providers and staff in public authorities to refer directly to the Judicial Commissioners any complaint or concern they may have with the use of the powers under the Bill or any request for clarification on the use of those powers. Where clarification is provided the Judicial Commissioners will need to have the power to make that information public should it be appropriate in the circumstances. This will enable better compliance with the provisions of the Bill and will help to reduce costs. **Recommendation 61:** We recommend that members of the intelligence services should be able to contact the Investigatory Powers Commissioner with concerns over the misuse of surveillance powers without being at risk of prosecution for breaching the Official Secrets	**Recommendation J(vi):** While the draft Bill contains some much-needed reforms of the current Commissioners which should increase the current limited oversight, there is one further addition which the Committee considers necessary. At present, when this Committee is informed of matters that would more appropriately fall to the Commissioners or the Investigatory Powers Tribunal, there is no mechanism through which these can be formally referred to them for investigation. It would therefore be sensible for this Committee – on behalf of Parliament – to be given such a power.

	Act. The Investigatory Powers Commissioner should then have discretion whether to exercise his or her power to initiate an inquiry into the allegations.	
Clause 208 has been amended to provide for the possibility of an appeal from the IPT on a point of law against a preliminary determination.	**Recommendation 71:** We recommend that rulings in the Investigatory Powers Tribunal should be subject to an interim right of appeal on the grounds of an error of law to save time and costs.	
Clause 208 has been amended to make the appeal route from the IPT clear for Northern Ireland and Scotland	**Recommendation 72:** We recommend the appeal route for Scotland and Northern Ireland should appear on the face of the Bill. It is unclear to us why there is not a specified route of appeal in Scotland and Northern Ireland nor what appellants in those parts of the United Kingdom are expected to do before the Home Secretary issues regulations on this issue.	

Other key recommendations and responses

JC Recommendation 50: It is unclear to us why the Home Office chose to create a group of Judicial Commissioners rather than creating an Independent Intelligence and Surveillance Commission as recommended by David Anderson QC … . The evidence we have heard is that the work of the oversight body will be significantly enhanced by the creation of a Commission with a clear legal mandate. We recommend that such a Commission should become the oversight body in the Bill.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states that such a body would incur significantly higher costs, without having any additional powers or independence.
JC Recommendation 53: We recommend the Lord Chief Justice should have the power to appoint Judicial Commissioners following consultation with his judicial counterparts in Scotland and Northern Ireland and with the Prime Minister, Scottish Ministers, and the First Minister and deputy First Minister in Northern Ireland. This will ensure public confidence in the independence and impartiality of the Judicial Commissioners. It will also enhance political confidence in them. …The Judicial Appointments Commission must also be consulted to ensure that the appointments procedure is fair and transparent.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states: "It is an important principle that the Judiciary are as independent from each other as they are from the executive, to avoid accusations of a system of patronage. Similarly although the Lord Chief Justice may consult his counterparts, he would have no authority to make appointments relating to the deployment of Scottish or Northern Irish judges; agreement in principle from the Scottish Government to bring the relevant legislative consent motions is contingent on Scottish Ministers having a role in appointments of Judicial Commissioners and the IPC."

JC Recommendation 54: The Government should reconsider both the length of terms of appointment and whether they should be renewable. ... It may be that three-year terms with an option for renewal is the most workable solution but we recommend that there should be careful reconsideration of these provisions in consultation with the Lord Chief Justice, Judicial Appointments Commission, the current surveillance Commissioners and other interested parties to ensure the benefits and disadvantages of the different approaches have been thoroughly examined.	**The Government accepted this recommendation** but published the Bill before any review was undertaken.
JC recommendation 56: We believe it is inappropriate for the Home Secretary alone to determine the budget of the public body which is monitoring her exercise of surveillance powers. The Government may want to consider a role for Parliament in determining the budget.	The Government has agreed to consider whether there is a role for the ISC in determining the Judicial Commissioners' budget
JC recommendation 58: We recommend that the Government should review the error-reporting threshold in light of the points made by witnesses	The Government agreed to review the threshold but also emphasised the importance of national security and the wider public interest, suggesting that it is unlikely to be lowered
JC recommendation 59: It should be made clear in the duties laid on the Judicial Commissioners in sub-clauses 169(5) and (6) (now 196(5) and (6)) that they must comply with those duties in a proportionate manner. The sub-clauses are drafted in very broad and uncertain terms which have the potential to impact upon the work of Judicial Commissioners in unintended ways. Public confidence in the independence of the Judicial Commissioners requires clarity and transparency in both powers and duties. We recommend Clauses 169(5) and (6) should be re-drafted to protect the Judicial Commissioners' independence and to ensure the Judicial Commissioners are not constrained from providing effective oversight.[114]	Clause 196 subsection (5) has been amended in response to recommendation 59. Subsection (5) places a requirement on Judicial Commissioners not to act in a manner that is contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime, or the economic well-being of the UK. As a result of the amendment, this is now a matter of subjective judgment on the part of the Judicial Commissioner.
JC recommendation 62: We agree with the Independent Reviewer of Terrorism that Judicial Commissioners must have access to both in-house legal expertise and, on request, security-cleared independent counsel to assist them in both the authorisation and oversight functions of their role.	According to the response to pre-legislative scrutiny, the Government intends that the IPC will have both an in-house legal adviser, and a budget for the appointment of independent counsel.
JC recommendation 64: We recommend that the Judicial Commissioners should have access to technical expertise to assist them in fulfilling their authorisation and oversight functions.	According to the response to pre-legislative scrutiny, the Government intends that the Commissioners will have a range of specialist inspectors to assist them, and a budget for the appointment of external consultants.

[114] The provisions in question state that the Judicial Commissioners must not exercise functions under the Act in a which would be contrary to the public interest or prejudicial to national security, the prevention of crime or the economic well-being of the country, and that Commissioners must not act in a way that would jeopardise or impede an operation or compromise the safety of those involved.

JC Recommendation 66: The Judicial Commissioners should be able to make a direct reference to the Investigatory Powers Tribunal where they have identified unlawful conduct following an inspection, audit, investigation or complaint.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny points to the fact that the IPT does not have the power to carry out investigations on its own initiative, and that it is a fundamental principle of the British justice system that courts and tribunals will not consider and determine legal issues without individual parties issuing a claim. However, the JC did not recommend that the IPT should be endowed with powers of investigation, but rather that Judicial Commissioners should have standing to challenge (potentially) unlawful conduct without the need to inform the individuals involved, where that would not be in the public interest.
JC Recommendation 68: The Investigatory Powers Commissioner should be able to inform the Intelligence and Security Committee if he is unhappy about the use of the Prime Minister's power to redact his annual report.	The Government have indicated that this will be included in a Memorandum of Understanding, however this has not yet been published.
JC Recommendation 69: We recommend that the Judicial Commissioners should have the power to develop guidance to public authorities to assist them in applications seeking to use investigatory powers. This will help applicant bodies to formulate focused applications saving time and resources. Where the constraints of national security allow, the guidance should be published in the interests of public transparency and foreseeability.	**The Government accepted this recommendation.** It is provided for in the draft Codes of Practice rather than on the face of the Bill.
JC Recommendation 70: We recommend that the right of appeal from the Investigatory Powers Tribunal in Clause 181 (now 208) should be amended to include cases where there has been an error of law to prevent injustice as a matter of public policy and to satisfy the rule of law.	**The Government did not accept this recommendation.** It remains the case that an appeal would have to raise an important point of principle or practice, or there would need to be another compelling reason for granting leave.
JC Recommendation 73: The Home Office should conduct a consultation and review of the powers and procedures of the Investigatory Powers Tribunal with the aim of improving openness, transparency and access to justice.	**The Government did not accept this recommendation.**
JC Recommendation 74: The Investigatory Powers Tribunal should have the power to decide whether its proceedings should be held in public. When making a decision on whether a hearing or part of a hearing should be open or not the Tribunal should apply a public interest test.	**The Government did not accept this recommendation.**
JC Recommendation 75: The Investigatory Powers Tribunal should be able to make a declaration of incompatibility under the Human Rights Act.	**The Government did not accept this recommendation.**

9.3 What did the reports on investigatory powers say?

Anderson	ISC	ISR
The Interception of Communications Commissioner's Office, the Office of the Surveillance Commissioners and intelligence Services Commissioner should be replaced by a new Independent Surveillance and Intelligence Commission (ISIC).[115]	The Commissioners should have increased oversight responsibilities, and all their functions should be put on a statutory footing.[116]	The existing Commissioners should be replaced by a new single body: a National Intelligence and Surveillance Office with four main areas of responsibility: inspection and audit; intelligence oversight; legal advice; and public engagement.
ISIC, through its Judicial Commissioners, should have the power to issue, renew and modify warrants. Judicial Commissioners should hold or have held high judicial office.[117]		
ISIC should have the power to inform a subject of an error on the part of a public authority or CSP, and of the right to lodge a complaint with the IPT.[118]		The judicial commissioners should be able to refer cases to the IPT where they find a material error, arguable illegality or disproportionate conduct.[119]
The jurisdiction of the IPT should be expanded to cover circumstances where it is a CSP rather than a public authority which was at fault.[120]		The IPT should find ways to be less opaque and should hold open hearings except where closed proceedings are necessary in the public interest.[121]
There should be a right of appeal to an appropriate court from rulings of the IPT on points of law.[122]	There should be a domestic right of appeal from the IPT.[123]	The IPT should have the ability to test secret evidence and there should be a domestic right of appeal.[124]
The IPT should have the same power as the High Court to make a declaration of incompatibility under section 4 of the Human Rights Act 1998.[125]		

[115] Recommendation 82
[116] Annex A. para II & JJ
[117] Recommendations 84 & 85
[118] Recommendation 99
[119] Recommendation 16
[120] Recommendation 113
[121] Recommendations 11 & 12
[122] Recommendation 114
[123] Ibid, para LL
[124] Recommendations 13 & 14
[125] Recommendation 115

10. Part 9: Miscellaneous and general provisions

10.1 What does the Bill do?

Chapter 1: Miscellaneous

Clause 212 introduces **Schedule 8**, which would make provision for the combination of targeted interception warrants or targeted equipment interference warrants with other warrants or authorisations.

Clause 213 would provide that CSPs must receive a contribution towards their compliance costs and **clause 214** enables the Secretary of State to put measures in place to facilitate compliance.

Clause 215 would amend the Intelligence Services Act 1994 in relation to certain functions of GCHQ and SIS. These changes would enable GCHQ to provide information assurance advice to external organisations. They would also enable GCHQ and SIS to engage in property interference where the property in question is in the UK, removing an existing restriction.

Clause 216 would provide that the Secretary of State may issue a "national security notice" requiring a CSP to take steps in the interests of national security. National security notices may only require conduct that the Secretary of State considers to be necessary and proportionate, for example the provision of services or facilities to assist an intelligence service to carry out its functions more effectively. A notice could not be used where the primary purpose was to authorise interference with privacy where warrant or authorisation would otherwise be required under the Act.

Clause 217 would allow the Secretary of State to use regulations to impose obligations on CSPs, via "technical capability notices", in order to facilitate assistance in relation to authorisations under Parts 2, 3, 5 and 6 of the Bill. Obligations may include obligations relating to the removal of electronic protection applied by a relevant operator to any communications or data, and obligations relating to the security of any postal or telecommunications services. Before making regulations under this clause the Secretary of State is obliged to consult the technical advisory board and the affected CSPs.[126]

Clauses 218 and 219 make further provision in relation to "national security notices" and "technical capability notices", including the matters that the Secretary of State should take into account before issuing a notice; the duty to comply; and the process for review of a notice prior to variation or revocation. Subsection 218(4) emphasises that the Secretary of State must take particular account of the technical feasibility and cost of compliance when considering giving a notice that would impose obligations relating to the removal of electronic protection.

[126] For further explanation on encryption see Box 4, below

Clause 220 would permit the recipient of a notice to refer it back to the Secretary of State for review. There would be no obligation to comply with the notice pending the outcome of the review. The Secretary of State would be required to consult the Technical Advisory Board and the Investigatory Powers Commissioner before reaching a decision as to whether to vary, revoke or confirm the notice.

Clause 221 would amend the Wireless Telegraphy Act 2006 to avoid duplication with the Bill in relation to interception powers.

Chapter 2: General

Clause 222 would provide for the Secretary of State to prepare a report on the operation of the Act after five years and six months. The Secretary of State would be required to take account of any report made by a Joint Committee of both Houses.

The remaining clauses deal with definitions, the procedure for making regulations, commencement, extent and other technical matters.

10.2 Changes following pre-legislative scrutiny

Key changes in the Bill and relevant recommendations

Change	JC	ISC	S&T
The definition of "data" in **clause 225** (previously 195) has been revised	**Recommendation 2** – The Government must provide a meaningful and comprehensible definition of data when the Bill is introduced		**Recommendation 2**: The Government, in seeking to future-proof the proposed legislation, has produced definitions of internet connection records and other terms which have led to significant confusion on the part of communications service providers and others. Terms such as "telecommunications service", "relevant communications data", "communications content", "equipment interference", "technical feasibility" and "reasonably practicable" need to be clarified as a matter of urgency.

Clauses 217 and 218 (previously 189 and 190) have been revised. The Government's response to pre-legislative scrutiny states that they now explain what is meant by 'removing electronic protection' and make clear that CSPs can only be required to remove protection that they themselves have applied, or has been applied on their behalf.	**Recommendation 16**: We agree with the intention of the Government's policy to seek access to protected communications and data when required by a warrant, while not requiring encryption keys to be compromised or backdoors installed on to systems. The drafting of the Bill should be amended to make this clear. **Recommendation 17:** The Government still needs to make explicit on the face of the Bill that CSPs offering end-to-end encrypted communication or other un-decryptable communication services will not be expected to provide copies of those communications if it is not practicable for them to do so.	**Recommendation J(x)**: The draft Bill imposes several obligations on CSPs to assist the Agencies. For example, Clause 189 states that the Secretary of State may make *"technical capability"* regulations. Some CSPs have expressed serious concern as to this seemingly open-ended and unconstrained power, suggesting that this may lead to banning end-to-end encryption. The Home Office must ensure that the legislation provides clarity as to the nature and scale of these obligations.	**Recommendation 3:** In tightly prescribed circumstances, law enforcement and security services should be able to seek to obtain unencrypted data from communications service providers. They should only seek such information where it is clearly feasible, and reasonably practicable, and where its provision would be consistent with the right to privacy in UK and EU law. The obligations on potential providers of such data should be clarified in the proposed Codes of Practice to be published in draft alongside the Bill later this year. (Paragraph 42)
Clause 222 has been added to the Bill to require the Secretary of State to prepare a report on the operation of the Act within six years of the Bill being enacted. This must take account of any report on the operation of the Act by a Select Committee of either House.	**Recommendation 86:** We recommend that a provision be added to the face of the Bill for post-legislative scrutiny by a committee of the two Houses within six months of the end of the fifth year after the Bill is enacted.		

Other key recommendations

Recommendation	Response
JC recommendation 1: We urge the Government to undertake further consultation with communications service providers, oversight bodies and others to ascertain whether the definitions are sufficiently clear to those who will have to utilise them.	The response to pre-legislative scrutiny states: "the draft Codes of Practice published alongside the Bill provide further information on how the definitions in the Bill will work in practice. New Codes of Practice will be published for formal consultation following Royal Assent; they will require approval by Parliament and will have statutory force and will be subject to full consultation with industry and the public. The draft Code of Practice on Communications Data includes Chapter 2 on scope and definitions."

JC Recommendation 82: The Committee recommends that the Bill includes a definition of national security in order to provide clarity to the circumstances in which these warrants can be issued.	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny states: "It has been the policy of successive governments not to define national security in statute. Threats to national security are constantly evolving and difficult to predict, and it is vital that legislation should not constrain the ability of the security and intelligence agencies to protect the UK from new and emerging threats."
JC Recommendation 83: The Committee recommends that the Bill includes a definition of economic well-being in order to provide clarity to the circumstances in which these warrants can be issued.	**The Government did not accept this recommendation.**
S&T Recommendation 2: The Government, in seeking to future-proof the proposed legislation, has produced definitions of internet connection records and other terms which have led to significant confusion on the part of communications service providers and others. Terms such as "telecommunications service", "relevant communications data", "communications content", "equipment interference", "technical feasibility" and "reasonably practicable" need to be clarified as a matter of urgency. The Government should review the draft Bill to ensure that the obligations it is creating on industry are both clear and proportionate. Furthermore, the proposed draft Codes of Practice should include the helpful, detailed examples that the Home Office have provided to us.	In addition to the revision of clause 225, the response to pre-legislative scrutiny states that the draft Codes of Practice provide further examples of definitions, and information about obligations that can be placed on a CSP and compliance.
S&T Recommendation 4: There is some confusion about how the draft Bill would affect end-to-end encrypted communications, where decryption might not be possible by a communications provider that had not added the original encryption. The Government should clarify and state clearly in the Codes of Practice that it will not be seeking unencrypted content in such cases, in line with the way existing legislation is currently applied. (Paragraph 43)	The response to pre-legislative scrutiny states that the relevant draft Codes of Practice contain further detail on the factors that will be relevant to a determination as to whether it is necessary and proportionate to impose an obligation on a CSP. The extent to which encryption has been applied, and the nature of that encryption will be part of the necessity and proportionality consideration. The revision of clause 217 also makes clear that obligations to remove encryption may only relate to protections applied by or on behalf of the CSP on whom the obligation is placed.
S&T Recommendation 10: Detailed Codes of Practice will be needed to provide a more effective means of assisting compliance, and retaining business confidence in the feasibility of investigatory powers provisions, and their regular updating should be an explicit requirement in the Bill when it is introduced. Specifically, the Bill should require that at regular set intervals (perhaps yearly) the Technical Advisory Board is consulted about keeping the Codes of Practice up to date—a new role we propose for that body—and allowing both the Government and business representatives to bring forward amendments. (Paragraph 72)	**The Government did not accept the recommendation** to make it a requirement on the face of the Bill that the Technical Advisory Board are consulted at set intervals about keeping Codes of Practice up to date. However, Schedule 7, paragraph 5 provides for the Secretary of State to revise the Codes.

S&T Recommendation 13: The Government should review the composition of the Technical Advisory Board to ensure that it will have members from industry who will be able to give proper consideration, not just to the technical aspects of appeals submitted to it from CSPs concerned about ICR or other interception or 'interference' notices, but also any concerns raised about costs. The Government should also produce an explicit framework for how mediation of disputes and challenge will be resolved. The Government should consider whether the Board will need stronger legal expertise in light of the new investigatory powers that it will have to deal with. Membership of the Board should also more generally reflect a wide range of internet industries and expertise, and be able to co-opt individuals from individual businesses likely to be directly affected.(Paragraph 80)	The response to pre-legislative scrutiny indicated that these matters will be addressed in secondary legislation, to be published during the Bill's passage.
S&T Recommendation 14: The Government did not set up the 'Advisory Council for Digital Technology and Engineering' advocated by the Royal United Services Institute. It should nevertheless add to the remit of the Technical Advisory Board a role it envisaged for that Council—to keep under review the domestic and international implications of the evolution of the internet, digital technology and infrastructure. (Paragraph 81)	**The Government did not accept this recommendation.** The response to pre-legislative scrutiny indicates that the Government did not believe it was necessary, in light of existing arrangements

10.3 Debate and comment

Encryption

Clauses 217 and 218 would provide the means for the Secretary of State to impose "technical capability notices" on CSPs in order to facilitate assistance in relation to authorisations under the Bill. This may include obligations relating to the removal of electronic protection, including encryption. Before imposing a notice the Secretary of State must consult affected CSPs and the Technical Advisory Board.

Clause 189(4)(c) of the draft Bill provided that notices could impose obligations relating to the "removal of electronic protection applied by a relevant operator to any communication or data". Clause 217(4)(c) now provides that a notice may impose "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communication or data". This would appear to clarify the point that a CSP can only be required to remove encryption that it has applied itself, or that has been applied by a third party on its behalf.

Clause 218(4) contains a new requirement that, where the relevant notice would impose obligations relating to the removal of electronic protections, the Secretary of State must take particular account of the technical feasibility and cost of compliance. Cost and technical feasibility are already listed as matters to be taken into account in clause 218 (3), as they were in the previous clause 190(3).

Box 4: Encryption

Encryption is the process of converting information ('plaintext') into an encrypted form ('ciphertext') which is only intelligible to someone who knows how to 'decrypt' it to obtain the information. It is commonly used to protect the confidentiality of digital data stored on electronic devices or transmitted over an unsecured network, such as the internet. It also underpins systems for user authentication and for verifying the integrity of data.

Encryption is routinely used by Communications Service Providers (CSPs) and social media applications (such as instant messaging) to protect data in transit across a wide range of communications networks; not just the internet but also private computer networks, wireless networks, and mobile networks. Encryption is used to protect data in a wide range of transactions, from personal emails to ATM transactions, online purchases and more. Encryption is increasingly implemented by service providers themselves, although encryption software is also freely available over the internet. Users can download it and apply their own encryption for added privacy.

Data is encrypted using an encryption algorithm (a set of mathematical instructions) and an encryption key. For example, in one of the oldest known examples of encryption, the Caesar cipher, messages were encrypted according to the algorithm "replace each letter with the letter N spaces to the right of it in the alphabet", where N is the key. Modern encryption algorithms operate on electronic data (strings of 1s and 0s) with keys that are themselves strings of 1 and 0s, but the principle is much the same.

There are two types of encryption, symmetric or secret key and asymmetric or public key:

- Symmetric encryption uses the same 'key' for both encrypting and decrypting data. In symmetric encryption both sides—the encrypter, and the decrypter—need access to the same key. Thus the sender of data must exchange the key used to encrypt the data with the recipient before it can be decrypted.
- Asymmetric encryption (also known as public-key cryptography) is where each party has a pair of keys – a public key and a private key. A user takes plaintext and encrypts it using the public key of their recipient. The recipient then decrypts it using their private key. The private key never needs to be exchanged. Asymmetric algorithms are designed such that a private key cannot easily be deduced from the corresponding public key.

Typically a symmetric algorithm would be used to efficiently encrypt data, and an asymmetric algorithm used to exchange the symmetric or secret key.

End-to-end encryption

In recent years there has been a drive towards increased data security and consumer privacy, driven in part by claims that government agencies were routinely monitoring communications. In many cases – for example web based email - data may not be encrypted at every stage of the path between sender and receiver, rendering it vulnerable to a third party. This is one reason why companies increasingly offer end to end encryption where data is encrypted along the entire path between sender and recipient. End to end encryption software can also be downloaded over the Internet-for example the freely available software PGP ("pretty good privacy"). With end-to-end encryption, the only people who have access to the keys required to decrypt the data are the two people communicating. This means that third-parties cannot easily tap into communicatons while they are transferred from one end system or device to another—not even a company that runs the messaging service. However, there are concerns in the cybersecurity community that if CSPs were asked to provide security services with 'backdoors' to such applications the applications' security would be weakened, for example unauthorised parties could obtain knowledge of the 'backdoor'and exploit it for unlawful purposes

Encryption 'backdoors'

In practice encryption cannot be guaranteed to be 100% secure. Often, software contains errors that are not picked up until in widespread circulation. Another common source of vulnerability is the way that keys are managed (i.e. generated, distributed and stored). For example, keys are often protected with a password set by the user. A weak password would render the key vulnerable. (For this reason there is an increasing trend towards privacy enhancing measures, for example limiting the number of allowed password attempts before access to a system is denied)

The term "encryption backdoor" is often used in current debate to describe mechanisms by which law enforcement could obtain access to keys required to decrypt data, or to the decrypted data itself. A "backdoor" might be based on a vulnerability known only to law enforcement - for example, a hidden bug in computer code. In practice however, security experts say it would be difficult to prevent such vulnerabilities from becoming more widely known, and they would therefore introduce a security risk. Moreover, users might simply migrate to other applications that did not contain "backdoors".

Another option that has been suggested is to make copies of keys required to decrypt data, for example via third party escrow, where copies of all keys are held by a trusted third party who could then hand over keys in response to warrants. Key escrow already takes place on a small scale within individual organisations. However, applying such mechanisms at a larger scale would raise many technical, logistical and legal challenges.

The Home Office stated in evidence that the Bill replicates the existing position under RIPA, and pointed to the recommendation in the Anderson Report that no-go areas for law enforcement should be minimised, in support of the provision's inclusion in the draft Bill.[127]

However, many witnesses who engaged in the pre-legislative scrutiny process raised concerns about the equivalent provisions in the draft Bill.[128] The Information Commissioner's Office suggested in evidence to the Joint Committee that it was unclear from the Bill how the requirement will be applied in practice. TechUK considered that it was unclear whether the requirement has any implications for encryption methods such as end-to-end encryption, where only the users of the services have access to the keys required to decrypt data. They expressed concern that, if it did affect end-to-end encryption, this would limit companies' ability to deploy the necessary security to safeguard their customers' privacy and security, thereby compelling companies to weaken the security of their products.

Privacy and civil liberties campaigners including Big Brother Watch, Article 19, Human Rights Watch and Liberty expressed concerns that the provision may undermine encryption, for example by requiring companies to insert 'backdoors' into their products in order to facilitate government access. Similar concerns were expressed by technology companies, including Apple, Facebook, Google, Microsoft, Twitter, Yahoo and Mozilla. Cybersecurity company F-Secure suggested the Bill might have implications for end-to-end encryption where the service provider might not have the capability to decrypt the contents of a communication passing across its system, by creating the possibility that such systems could be banned. Apple stated in evidence:

> Although it is not explicit in the draft bill, our understanding of the government's intention is that this would require us to remove end-to-end encryption if that was necessary to give effect to the warrant and considered proportionate.[129]

Several witnesses also suggested that the provision would have a negative economic impact by damaging the competitiveness of UK tech businesses or encouraging them to relocate outside the UK.

The Science and Technology Committee also heard evidence of concerns about the Bill's implications for encryption.[130] TechUK told the Committee that although the Government had been at pains to stress that it is not restricting or weakening encryption, and that the requirements under clause 189 are already provided for in existing legislation, further scrutiny is needed. They suggested that the test for whether it is technically feasible to remove electronic protection should include consideration of whether it is "reasonable and proportionate",

---

[127] Report of the Joint Committee on the Draft Investigatory Powers Bill, para 249
[128] Paras 250-260
[129] Cited at para 257 of the Report
[130] Investigatory Powers Bill: technology issues, Science and Technology Committee, HC 573, February 2016

encompassing time, cost, knock-on effects and change in customer relationships.[131]

The Institute for Human Rights and Business suggested that while the Bill might not eliminate end-to-end encryption, it could prevent companies served with a technical capability notice from offering end-to-end encryption as part of their services.

Mozilla expressed concern that software developers such as themselves could be compelled under the Bill to ship hostile software to a user or users without notice.

Other witnesses suggested that knowledge of such powers might encourage wrong-doers to use anonymity tools in order to circumvent the provisions.

Box 5: Apple v FBI

These issues are currently being debated in the USA in the context of a dispute between **Apple and the FBI**. The dispute arose following the San Bernardino shooting. The FBI discovered an IPhone belonging to one of the attackers. The FBI has permission to search the phone but has so far been unable to guess the passcode to unlock it. In iOS devices, 1 most files are encrypted using a combination of a secret key stored on the device, and the user's passcode. Data may be wiped after too many incorrect attempts at getting the passcode. The FBI has therefore made a request for technical assistance through a court order to Apple to enable it to make an unlimited number of passcode guesses. Apple are resisting on the basis that helping the FBI in this context would set a dangerous legal precedent, as well as undermining the security of their products, leaving customers vulnerable to interference for unlawful purposes.

Since publication of the revised Bill, there has been some limited reaction to the drafting changes.

The Internet Service Providers Association expressed disappointment at the speed with which the Bill has been introduced, and suggested that "there are still questions to be answered about technical capability notices". [132]

TechUK have suggested that more detail could have been provided in the Codes of Practice regarding the procedure to be followed when the Home Secretary disagrees with a CSP as to the technical feasibility of a technical capability notice, and that decisions as to costs and feasibility of compliance should be made by a Judicial Commissioner rather than the Secretary of State.[133]

---

[131] For discussion of technical aspects of encryption, see POSTbrief 19 *Data Encryption*

[132] Internet industry disappointed with Fast-tracking of Investigatory Powers Bill, 1 March 2016, ipsa.org.uk

[133] techUK Briefing and Response to New investigatory Powers Bill, 2 March 2016, techUK.org

BRIEFING PAPER
Number 7518, 11 March 2016