Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

March 2016

Cm 9219

Investigatory Powers Bill: Government Response to Pre-Legislative Scrutiny

Presented to Parliament
by the Secretary of State for the Home Department
by Command of Her Majesty

March 2016

Cm 9219

This publication is available at www.gov.uk/government/publications

Any enquiries regarding this publication should be sent to us at investigatorypowers@homeoffice.gsi.gov.uk.

Print ISBN 9781474129534
Web ISBN 9781474129541

ID 26021601 03/15 54575 19585

Printed on paper containing 75% recycled fibre content minimum

Printed in the UK by the Williams Lea Group on behalf of the Controller of Her Majesty's Stationery Office

INVESTIGATORY POWERS BILL: GOVERNMENT RESPONSE TO PRE-LEGISLATIVE SCRUTINY

CONTENTS

Foreword from the Home Secretary

1 March 2016

INVESTIGATORY POWERS BILL: GOVERNMENT RESPONSE TO PRE-LEGISLATIVE SCRUTINY

Today I am introducing the Investigatory Powers Bill in the House of Commons. It will transform the law relating to the use of investigatory powers by law enforcement and the security and intelligence agencies, and it will strengthen safeguards and introduce world-leading oversight arrangements.

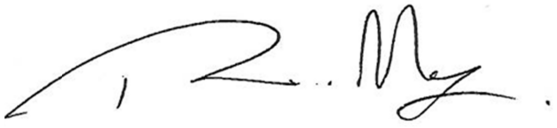
In November 2015 the Government published a draft Bill for pre-legislative scrutiny. The provisions in the draft Bill were considered by the House of Commons Science and Technology Committee, the Intelligence and Security Committee of Parliament and by a Joint Committee of both Houses of Parliament convened to scrutinise the draft Bill.

Between them, those Committees received over 1500 pages of evidence and took oral evidence from Government, industry, civil liberties groups and many others. The tables included in this document set out how the Government has responded to each of their reports.

I am pleased to say that the revised Bill, along with the supporting material that we are publishing alongside it, give effect to the vast majority of the recommendations made by the three Committees. Where we have not been able to accept the Committees' recommendations the tables explain the good reasons for not accepting them.

This Bill ensures that the security and intelligence agencies and law enforcement continue to have the powers they need to keep us safe – and no more. The Bill also provides the public and Parliament with greater confidence that there are robust measures in place to ensure that the powers are subject to appropriate safeguards.

The new legislation needs to be in force by 31 December 2016 in order to ensure that powers which are essential to counter the threat from criminals and terrorists do not lapse. By introducing it now, we have ensured that this important piece of legislation will be subject to full and thorough scrutiny by both Houses of Parliament, following the normal Parliamentary timetable.



Rt Hon Theresa May MP

INVESTIGATORY POWERS BILL: GUIDE TO POWERS AND PRIVACY SAFEGUARDS

Revised on introduction of the Bill in the House of Commons

March 2016

GUIDE TO POWERS AND PRIVACY SAFEGUARDS: CONTENTS

CONTEXT

1. The Investigatory Powers Bill will govern the use and oversight of investigatory powers by the law enforcement and security and intelligence agencies and by other specified public authorities. It builds on the work of three comprehensive reviews undertaken in the last two years. Those reviews, carried out by David Anderson QC, the Independent Reviewer of Terrorism Legislation, the Intelligence and Security Committee of Parliament (ISC), and a panel convened by the Royal United Services Institute (RUSI), between them made 198 recommendations.

2. All three reviews agreed that the use of these powers will remain vital to the work of the law enforcement and security and intelligence agencies in the future. Collectively, they proposed reforms to the way these powers are overseen and recommended the introduction of stronger safeguards and greater openness.

3. In November 2015 the Government published a draft Bill for pre-legislative scrutiny. The provisions in the draft Bill were considered by the House of Commons Science and Technology Committee, the Intelligence and Security Committee of Parliament and by a Joint Committee of both Houses of Parliament convened to scrutinise the draft Bill.

4. Between them, those Committees received around 200 submissions and held a number of evidence sessions with the Government, industry, civil liberties groups and other bodies. In response to their recommendations, the Government introduced a revised Bill to Parliament on 1 March, alongside further explanatory material.

5. The Government has accepted the vast majority of the Committees' recommendations and the revised Bill reflects this. More detail is provided in the following pages. In addition, the Government is – in line with the Committees' recommendations – publishing six draft Codes of Practice alongside the Bill to provide greater detail on the operation of the powers contained in the Bill and the oversight arrangements that will govern them.

6. The Government is also publishing a detailed operational case for the use of the bulk powers and has revised the previously published operational case for the retention of internet connection records.

7. The Investigatory Powers Bill will transform the law relating to the use and oversight of these powers. It will strengthen safeguards and introduce world-leading oversight arrangements. The Bill will do three things:

- First, it will bring together powers already available to law enforcement and the security and intelligence agencies to obtain communications and data about communications. It will ensure that these powers – and the safeguards that apply to them – are clear and understandable.

- Second, the Bill will radically overhaul the way these powers are authorised and overseen. It will introduce a 'double-lock' for interception warrants, so that these – and other warrants – cannot be issued by the Secretary of State until they have been approved by a judge. And it will create a powerful new Investigatory Powers Commissioner (IPC) to oversee how these powers are

used.

- Third, it will make sure powers are fit for the digital age. The Bill will make provision for the retention of internet connection records (ICRs) in order for law enforcement to identify the communications service to which a device has connected. This will restore capabilities that have been lost as a result of changes in the way people communicate.

8. This guide provides an overview of the key provisions in the Investigatory Powers Bill, including the key changes that have been made to the Bill following pre-legislative scrutiny. It should be read alongside the Bill and the accompanying Explanatory Notes, which have been published at the same time.

PRIVACY IN THE REVISED BILL

9. The Investigatory Powers Bill will protect both privacy and security. Part 1 of the Bill provides an overview of the privacy safeguards contained throughout the Bill. The revised Bill and the accompanying Codes of Practice make clear the strong privacy safeguards that apply to all of the powers in the Bill, in particular:

a. **Transparency:** the Bill makes more explicit the powers available to public authorities to obtain communications or communications data. In doing so, it puts on a clearer statutory footing some of the most sensitive powers and capabilities available to the security and intelligence agencies. Some powers will remain outside of the Bill. For example, in line with the recommendation made by David Anderson QC, the police will retain the ability to use overt search and seizure powers to obtain communications that have been stored on a device or a server, such as emails stored on a web-based server. The Bill also imposes requirements on the Investigatory Powers Commissioner to report to the public and to Parliament precisely how the powers in the Bill have been exercised.

b. **Authorisation:** The Bill overhauls the way the most sensitive powers available to law enforcement and the security and intelligence agencies are authorised. Under the Bill, warrants will be subject to a new 'double lock', so that they must be approved by a Judicial Commissioner before they can be issued by the Secretary of State. This will preserve democratic accountability and introduce a new element of judicial independence into the authorisation process. This powerful new safeguard was endorsed by the Joint Committee convened to scrutinise the draft Bill.

c. **Oversight:** The Bill creates a world-leading oversight regime, bringing together three existing commissioners and providing new powers and resources to an independent Investigatory Powers Commissioner (IPC). The Commissioner will hold, or have held, high judicial office and will oversee the use of the powers in the Bill by public authorities. The revised Bill strengthens the office of the IPC further. Where the IPC in the course of his or her investigations determines that a person has been the subject of a serious error, the IPC will have the ability to notify the individual concerned.

d. **Limited powers:** the Bill strictly limits the circumstances in which the powers it provides for can be used. In line with the recommendation made by the Intelligence and Security Committee in its 2015 Privacy and Security report, the revised Bill and the accompanying Codes of Practice make clear:

    i. <u>The purposes for which each of the powers in the Bill may be used</u>. Those powers that can be used to access the content of communications or other private documents, such as interception and equipment interference, may only be used for a very limited number of statutory purposes.

ii. The overarching human rights obligations which constrain the use of the powers in the Bill. This includes statutory obligations elsewhere in domestic and international law.

iii. Whether each of the powers in the Bill must be used in a targeted way or provides for the acquisition of data in bulk. The Bill also makes clear that a Secretary of State and a Judicial Commissioner (the 'double lock') must approve the purposes for which data obtained in bulk can be examined.

iv. The authorisation procedures that must be followed, including the review, inspection and oversight regime. This includes the introduction of a new 'double lock' for all warrants in the Bill.

v. Specific safeguards for certain sensitive professions or categories of information. This includes additional protections in the Bill and the statutory Codes of Practice for lawyers, Parliamentarians and journalists.

vi. Safeguards and obligations in respect of retention, storage and destruction of data. In addition, the Bill and the accompanying materials make clear the security obligations relating to retained data.

vii. Safeguards relating to sharing of material obtained under the powers in the Bill. These are set out on the face of the Bill and the accompanying Codes of Practice.

e. **Penalties for misuse:** the Bill sits alongside existing legislation such as the Computer Misuse Act 1990 to make clear the circumstances in which it is an offence to obtain communications or communications data without a lawful authorisation:

i. Interception: the Bill replicates the existing offence of unlawful interception, so that interception in the absence of a warrant may constitute a criminal offence.

ii. Communications data: The Bill creates a new offence for a person knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority.

iii. Equipment interference: The Bill preserves the offence in the Computer Misuse Act 1990, so that equipment interference in the absence of a warrant may constitute an offence.

OVERSIGHT

What happens now?

10. The UK's system of oversight for law enforcement and the security and intelligence agencies' use of investigatory powers is provided for in different Acts of Parliament. These include the Regulation of Investigatory Powers Act 2000 (RIPA), the Police Act 1997, and the Justice and Security Act 2013 (JSA). Oversight of the powers and their use is carried out by a number of different bodies.

11. Parliamentary oversight is carried out by the cross-party ISC, whose powers were strengthened by the JSA. Independent non-Parliamentary oversight is carried out by:

- The Interception of Communications Commissioner (IoCC), who oversees public authorities' use of interception and communications data powers under RIPA and powers under section 94 of the Telecommunications Act 1984 (which has been repealed in the Bill).

- The Chief Surveillance Commissioner (CSC), who oversees law enforcement agencies' use of covert surveillance powers and covert human intelligence sources under RIPA Part II and property interference powers under the Police Act 1997.

- The Intelligence Services Commissioner (ISCom), who oversees the intelligence agencies' use of the powers available to them under RIPA Part II (covert surveillance and covert human intelligence sources) and the Intelligence Services Act 1994.

Right of redress

12. The Investigatory Powers Tribunal (IPT) investigates complaints that law enforcement and the security and intelligence agencies have used their covert investigative techniques unlawfully, or claims that the intelligence or law enforcement agencies have breached human rights legislation. It is an independent Tribunal comprised of judges and senior members of the legal profession.

Why does oversight need to change?

13. The reports published by David Anderson QC, the ISC and the RUSI panel all agreed that our oversight regime should be strengthened. The present system of three separate oversight bodies, with overlapping responsibilities and distinct identities, is more confusing than a single, authoritative body which is equipped with all the skills and resources it needs.

What will happen in the future?

14. The Bill will create a single new independent and more powerful Commissioner, the IPC. The Commissioner will be properly supported and will have a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee any aspect of law enforcement and the security and intelligence agencies' use of the powers available to them.

15. The IPC will hold or have held high judicial office and with his or her supporting staff will have three key roles. First, they will authorise and approve the use of investigatory powers. Judicial Commissioners, who will be serving or former High Court judges, will undertake this role. Secondly, they will be responsible for inspecting public authorities on their use of the powers contained in the Bill. The IPC will audit compliance and undertake independent investigations. Judicial Commissioners will undertake this role and will be supported by a team of expert inspectors.

16. Third, the Commissioner will have a clear mandate to inform Parliament and the public about the need for, and use of, investigatory powers. The Commissioner will report publicly and make recommendations on the findings that emerge in the course of his or her work. The Commissioner will also publish guidance, when it is required, on the use of investigatory powers. The Commissioner should have a high public profile and active media and online presence so that he or she is quickly established as an authoritative source of advice and information. To support these three roles, the Commissioner will also have dedicated legal, technical and communications support.

17. The Bill will also strengthen the right of redress by allowing a domestic right of appeal from the IPT.

What are the key provisions in the Bill?

- **The Bill will replace the IoCC, the CSC and the ISCom with a powerful new IPC**

- **The IPC will be supported by Judicial Commissioners, who will themselves be senior judges; they will be supported by staff with relevant expertise, both legal and technical**

- **The Judicial Commissioners will, for the first time, be responsible for approving the issue of interception, equipment interference and bulk warrants**

- **The Judicial Commissioners will also oversee the use of all the powers under the Bill and will be required to publish their findings in an annual report**

- **The IPC will have a power to inform individuals who have been the subject of serious errors by law enforcement, the security and intelligence agencies and other public authorities**

- **The IPT will be strengthened through the creation of a new domestic right of appeal**

What are the key changes following pre-legislative scrutiny?

- **Reducing the period of time within which urgent warrants must be reviewed by a judge.** The revised Bill reduces the period of time within which a Judicial Commissioner must review an urgent warrant for interception or equipment interference from five working days to three. This responds to recommendations made by the Joint Committee (recommendation 36) and the ISC (recommendation v)

while still ensuring that when a warrant is urgently required, there is no operational delay.

- **Providing for anyone to be able to share information in confidence with the Investigatory Powers Commissioner**. This provision will permit the ISC, or those using investigatory powers, or subject to any of the obligations within the Bill, to contact the IPC. This will also allow those with concerns over the misuse of the powers to inform the IPC without being at risk of prosecution for breaching the Official Secrets Act. The IPC will then have discretion as to whether to exercise his or her power to initiate an inquiry into the allegations. This gives effect to a recommendation of the Joint Committee (recommendation 61) and responds to the ISC (recommendation vi.).

- **Requirement for the Lord Chief Justice (LCJ) to be consulted before a person is appointed as a Judicial Commissioner or the IPC.** The revised Bill includes an additional requirement for the LCJ, and his or her equivalents in the Devolved Administrations, to be consulted on the appointment of the Judicial Commissioners. This follows a recommendation from the Joint Committee (recommendation 53).

- **Permitting the IPC to report errors to affected individuals without reference to the Investigatory Powers Tribunal.** The revised Bill includes provision to allow the IPC to inform people who have suffered as a result of a serious error by a public authority. This gives effect to a recommendation from the Joint Committee (recommendation 57).

- **Permitting the Judicial Commissioners to communicate directly with the Investigatory Powers Tribunal.** The Bill published in draft required Judicial Commissioners to consult the Home Secretary prior to providing advice and guidance to the IPT. This requirement has been removed from the revised Bill in response to the Joint Committee (recommendation 65).

- **Including reference to a Memorandum of Understanding that will govern the means by which the Scottish Government will be consulted on appointments to the Investigatory Powers Commission.** This provides for a formal agreement to be made between the United Kingdom Government and the Scottish Government setting out how the process of consultation with Scottish Ministers and appointments to the IPC will work in practice.

- **Altering the means by which a Judicial Commissioner can be removed from appointment.** A Judicial Commissioner can now only be removed from office by a resolution of Parliament or, in limited circumstances, by the Prime Minister, rather than by the IPC. This gives effect to a recommendation by the Joint Committee (recommendation 55).

- **Providing for the oversight of the use of Telecommunications Restriction Order Regulations 2016.** This provides that the IPC will oversee the use of powers

to prevent or restrict the use of communication devices, including unauthorised mobile phones, in prisons. This will ensure the use of such powers is subject to formal statutory oversight.

- **Ensuring that either an interim decision or a final determination from the IPT can be appealed.** This makes clear that an interim decision (e.g. on a specific point of law that arises in the course of a challenge) could be challenged, as well as a final determination. The Bill gives effect to a recommendation made by the Joint Committee (recommendation 71) that either stage can be appealed, as opposed to only the final determination. This broadens the opportunities in which an appeal can be made from the IPT.

- **Oversight of technical systems.** The revised Bill makes clear that Judicial Commissioners have an explicit legal mandate to access all relevant technical systems required to ensure effective oversight of the powers contained in the Bill. This gives effect to a recommendation by the Joint Committee (recommendation 63).

- **Making clear that in all circumstances, warrants are subject to the 'double-lock'.** The draft Bill made clear that the Judicial Commissioner review would apply to renewals of urgent warrants, but did not provide that the original decision to issue an urgent warrant must also be subject to the double-lock soon afterwards. The Bill has, therefore, been revised so that the decision to issue all urgent warrants must be reviewed by a Judicial Commissioner after three working days. If he or she does not approve the decision, all activity must cease and the Judicial Commissioner can direct that any collected material must be destroyed.

INTERCEPTION

What is it?

18. Interception is the obtaining of 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. Interception is used to collect valuable intelligence against terrorists and serious criminals, which can inform law enforcement and national security investigations as well as support military operations.

Why do we need it?

19. Warranted interception is used only for intelligence purposes. It is a vital tool which helps the law enforcement and security and intelligence agencies to prevent and detect serious or organised crime, and to protect national security.

What happens now?

20. Warranted interception is governed by RIPA. It allows for the security and intelligence agencies, the armed forces and a small number of law enforcement agencies to seek warrants when it is necessary and proportionate to do so for one of three statutory purposes: in the interests of national security; for the prevention and detection of serious crime; or in the interests of the economic well-being of the UK where it is connected to national security. Separate provision for interception of wireless telegraphy (such as military radio communications) is made under the Wireless Telegraphy Act 2006.

What will happen in the future?

21. The Investigatory Powers Bill will provide a new and more transparent statutory basis for the existing nine intercepting authorities to seek interception warrants in very limited circumstances. It will replace the provisions in RIPA and the Wireless Telegraphy Act. The Bill will enhance the safeguards that apply to the acquisition of intercept material, building on the recommendations made by David Anderson QC, the ISC and the RUSI panel.

What will the safeguards be?

22. In line with the recommendations made by David Anderson QC, RUSI and the ISC, the Bill will limit warranted interception powers to the existing nine intercepting authorities. Warrants may only be sought and issued for one of the current three statutory purposes.

23. Interception warrants must currently be authorised personally by the Secretary of State or, in the case of Scotland-related serious crime warrants, a Scottish Minister. The Bill responds to recommendations made by David Anderson QC and the RUSI panel by requiring that a Judicial Commissioner will in future need to approve decisions by the Secretary of State (or a Scottish Minister) to issue warrants before they can be issued. This will provide for a ‘double-lock’ of Executive and judicial approval for the use of interception.

24. The IPC will oversee intercepting authorities’ use of this power, ensuring that the detailed safeguards set out in legislation are stringently applied and that appropriate

arrangements are in place to handle the sensitive material that is obtained through interception. The Commissioner will audit how the authorities use the power and publish the findings annually.

What are the key provisions in the Bill?

- **The Bill will bring together all interception powers currently under RIPA and the Wireless Telegraphy Act 2006**

- **The Bill will limit the ability to seek interception warrants to the existing nine intercepting authorities and existing three statutory purposes**

- **It will introduce a new safeguard requiring that Judicial Commissioners approve warrants before they can be issued**

- **Applications for targeted interception warrants will need to specify a particular person, premises or operation**

What are the key changes following pre-legislative scrutiny?

- **Making explicit the protections for intelligence sharing.** The revised Bill makes clear that a warrant must be in place before asking an international partner to undertake activity in the UK on behalf of a public authority. This responds to recommendations from the Joint Committee (recommendation 43) and the ISC (recommendation xii).

- **Making changes to the handling of intercept material in inquests and public inquiries.** The revised Bill:
  - provides for Counsel and the solicitor to an inquest to view intercept material;
  - allows the solicitor to a public inquiry to view intercept material;
  - permits relevant intercept material to be considered where a retired judge has been appointed to lead an inquest (to extend the cadre of judges available to deal with these instances); and
  - allows for intercept material to be used and examined when it is relevant to a public inquiry.

  These changes address the recommendation from the Joint Committee (recommendation 79).

- **Making explicit provision for intercept material to be disclosed to the Independent Police Complaints Commission (IPCC) where it is relevant to its investigation.** This will clarify the circumstances in which it is permitted to inform the IPCC of intercept material that is relevant to an investigation they are conducting for the purpose of carrying out their statutory functions.

- **Providing that the interception of postal items in immigration centres in accordance with statutory rules is authorised for the purposes of the Bill.** This allows for the opening and examination of mail – as is currently the case – either for reasons of security, safety (to prevent weapons, drugs or other illicit items from being

sent to detainees) or where there is reason to believe that the contents of the mail could help in establishing the receiving detainee's identity, nationality or citizenship, to facilitate his or her removal from the UK.

- **Preserving law enforcement authorisation levels for minor modifications to warrants to reflect current practice.** The revised Bill preserves the position under existing legislation.

- **Providing for urgent modifications.** This makes clear the provisions in RIPA that allow for intercepting agencies to make major modifications to warrants in urgent circumstances. This power is used under existing legislation, in the case of thematic warrants, to add new individuals to the warrant where they are clearly caught by the scope of the warrant. In fast-moving situations (such as kidnaps, or drug importations arranged by organised crime groups) adding the names of new individuals to a thematic warrant is essential. The revised Bill clarifies this.

- **Replacing the term "related communications data" with "secondary data".** The Bill renames data, other than content, that can be obtained under a targeted or bulk interception warrant as "secondary data". The Bill sets out the definition of secondary data, making clear that it is broader than communications data. This clarifies the distinction between this type of data and the narrower class of data available under a communications data authorisation.

- **Creation of central definitions of systems data and identifying data.** This change ensures consistency when the same data is being referred to in different contexts.

Interception Case Study: Serious Crime Investigation

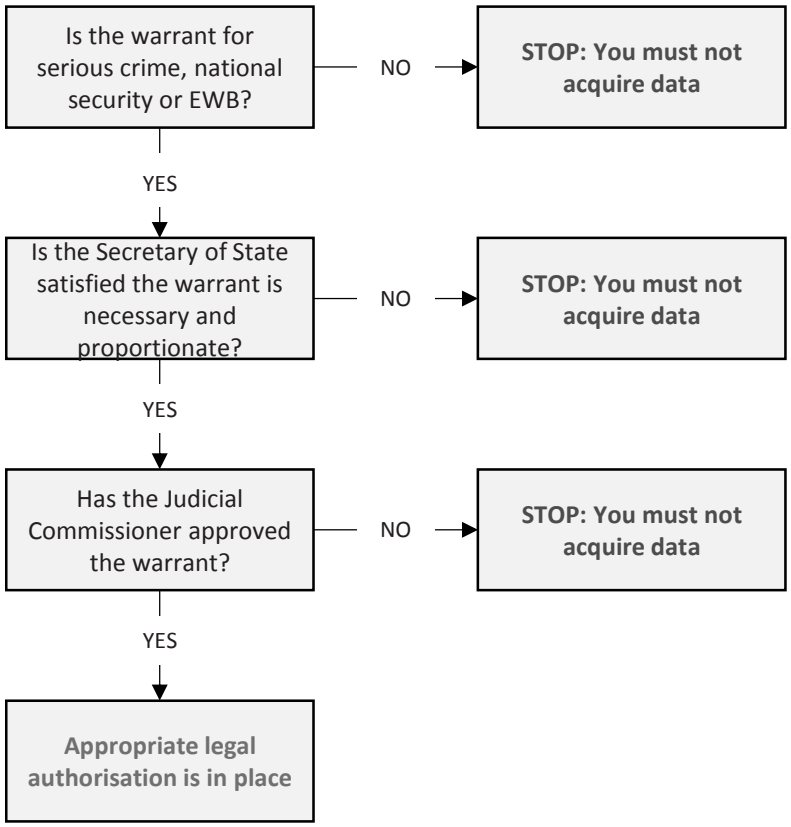
A criminal investigation was underway and was monitoring a pattern of escalating violence between a number of rival organised crime groups, including street gangs linked to the London drug economy, operating across the capital.

Intelligence derived from interception indicated a conflict between the organised crime groups as each sought to control a greater section of the drugs market, and intelligence suggested the use of firearms by the groups. This prompted immediate steps to tackle the groups, with the intention of dismantling the network, preventing further loss of life, disrupting the supply of Class A drugs, and arresting those involved.

Intercepted material identified the individual co-ordinating the sale of significant amounts of Class A drugs, led to the location of his safe storage premises, and identified senior gang members involved in the supply chain. It also enabled junior gang members to be identified as couriers of the drugs to numerous locations across London, the Home Counties and beyond, including the method and timing of transport. Interception also revealed that the head of the organised crime group was conspiring with others to shoot a rival. This led to the subject of interest being arrested while he was en-route to the hit location. He was found to be in possession of a loaded firearm.

The operation led to the collapse of the network operating across London and a number of other counties. During the course of the operation, intelligence from interception led to the seizure of over 40 firearms, in excess of 200kg of Class A drugs, the seizure of over £500,000 of cash as well as over 100 arrests.

IP Bill: Interception Authorisations



COMMUNICATIONS DATA

What is it?

25. Communications data is information about communications: the 'who', 'where', 'when', 'how' and 'with whom' of a communication but not what was written or said. It includes information such as the subscriber to a telephone service. Law enforcement, the security and intelligence agencies and other specified public authorities may acquire this data from Communications Service Providers (CSPs) who may be required to retain it.

Why do we need it?

26. Communications data is an essential tool for the full range of law enforcement activity and national security investigations. Requests may be made for data in order to identify the location of a missing person or to establish a link (through call records) between a suspect and a victim. It is used to investigate crime, keep children safe, support or disprove alibis and tie a suspect to a particular crime scene, among many other things. Sometimes communications data is the only way to identify offenders, particularly where offences are committed online, such as child sexual exploitation or fraud.

What happens now?

27. When necessary and proportionate, CSPs can be required to keep certain types of communications data for up to 12 months under the Data Retention and Investigatory Powers Act 2014 (DRIPA). Law enforcement and the security and intelligence agencies may acquire that data and any other communications data held by CSPs for business purposes under RIPA. Requests must be for a specific statutory purpose. Other than in exceptional circumstances, they must be independently authorised. Safeguards are set out in two statutory Codes of Practice. The Government keeps the number of public bodies which can acquire communications data under constant review; only organisations which can demonstrate a continuing and compelling need are provided with the power. Police requests that are intended to identify journalists' sources must be authorised by a judge. Local authorities can only apply for communications data for the purpose of the prevention and detection of crime and local authorities' applications must be approved by a magistrate.

What will happen in the future?

28. The Investigatory Powers Bill will create a new statutory basis for the retention and acquisition of communications data. The Bill will enhance the safeguards that apply to communications data acquisition, building on the recommendations made by David Anderson QC. The Bill will close the growing capability gap that limits the ability of law enforcement to identify the sender of online communications or the internet services being used by a suspect or a missing person (see following section on ICRs).

What safeguards will there be?

29. Authorisations will have to set out why accessing the communications data in question is necessary in a specific investigation for a particular statutory purpose, and how it is proportionate to what is sought to be achieved. All authorisations will go through a Single Point of Contact (SPoC). The SPoC's role is to ensure effective co-operation

between law enforcement bodies, the security and intelligence agencies, other specified public authorities and CSPs and to facilitate lawful acquisition of communications data. They also play a quality control role, ensuring that applications meet the required standards.

30. Once it has gone through the SPoC, the authorisation will be signed off by a Designated Senior Officer (DSO), who is independent of the investigation for which the communications data is needed. The Bill will provide a power that can ensure public authorities which access communications data infrequently will have to go through a shared SPoC (for example, by making use of the SPoC function within the National Anti-Fraud Network, as recommended by David Anderson QC). This will help to ensure that all applications are consistent and of sufficient quality.

31. The IPC will oversee how all law enforcement and the security and intelligence agencies use these powers. The Commissioner will audit how the authorities use them and report publicly on what they find.

What are the key provisions in the Bill?

- **Communications data retention and acquisition powers will be brought within a single, clear piece of legislation**

- **Other powers for acquiring communications data, such as those in the Health and Safety at Work Act 1974, will be repealed**

- **A new criminal offence of knowingly or recklessly acquiring communications data will be provided for as a firm check against abuse**

- **Bodies that make a small number of communications data requests can be required to share Single Points of Contact (SPoCs) to ensure requests meet accepted and consistent standards**

- **The definitions of communications data have been reviewed and are being updated to reflect changes in the way people communicate**

- **CSPs will only be required to retain internet connection records when served with a notice requiring them to do so. Access to this information will be limited, targeted and strictly controlled**

What are the key changes following pre-legislative scrutiny?

- **Permitting disclosures of the existence of a data retention notice in specified circumstances.** CSPs are prohibited from disclosing the existence of a retention notice, technical capability notice, or national security notice, to any person. As is currently the case, CSPs will be able to discuss their obligations with systems suppliers, oversight bodies and other companies subject to retention obligations. The Bill has been revised to ensure that CSPs can disclose the existence and contents of such notices with the permission of the Secretary of State, giving effect to a recommendation from the Joint Committee (recommendation 15).

- **Requiring the security and intelligence agencies to seek judicial authorisation for acquiring communications data to identify a journalistic source.** The revised Bill removes an exemption for the security and intelligence agencies and responds to a recommendation of the ISC (recommendation B). It will bring the security and intelligence agencies into line with law enforcement and other public authorities.

- **Dual reporting of communications data acquisition errors.** The revised Bill includes an amendment to the Privacy and Electronic Communications Regulations 2003 so that personal data breaches that follow from communications data requests are not required to be reported twice, to both the IPC and Information Commissioner, by CSPs. The new Codes of Practice will require such errors to be reported to the IPC, who can report relevant errors to the Information Commissioner. This simplification of reporting arrangements responds in part to a recommendation from the Joint Committee (recommendation 76).

- **Making clearer when the offence of knowingly or recklessly obtaining communications data applies.** The revised Bill provides a defence where a person in a public authority believed they had the appropriate authorisation in place. The offence is intended to prevent the misuse of the communications data powers, this change has been made in order to limit the risk that genuine mistakes become a criminal offence.

- **Relevant authorities for CD.** The revised Bill adds Food Standards Scotland to the list of public authorities that can acquire communications data. This provides for consistency between Scottish and English bodies.

- **Changes to regulation making powers in relation to relevant authorities**. The revised Bill responds to a recommendation from the Joint Committee (recommendation 41) by requiring that certain changes to authorisation levels for access to CD are subject to enhanced Parliamentary scrutiny.

CD Case Study: Child Sexual Exploitation

Operation GLOBE was a South Wales Police investigation in late 2012, into the sexual offences against children by Ian Watkins, lead singer of rock band *Lostprophets*. The investigation went on to show that Watkins was engaged in serious sexual offences against children, including the babies of two female co-defendants.

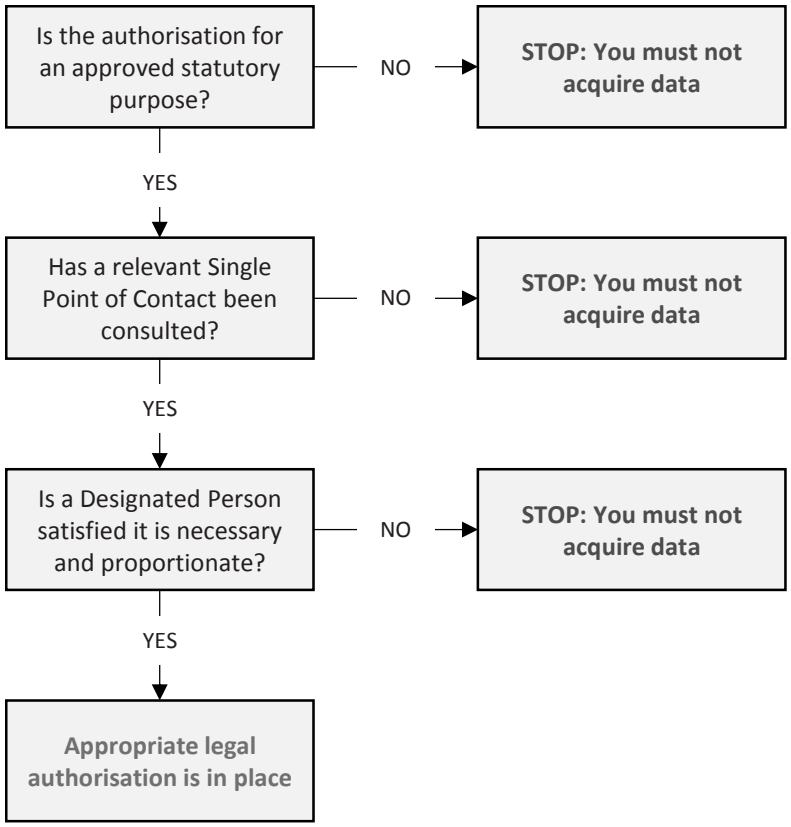
In the early stages of the inquiry, neither child had any physical injuries consistent with sexual abuse; there were no witnesses and no substantive evidence to support charges for the serious sexual offences that were suspected. Communications data was used alongside other investigative techniques which identified a clear conspiracy between all three defendants to abuse children sexually.

During the course of the investigation, officers seized electronic devices belonging to Watkins and recovered emails that contained indecent images of children. In one case, communications data was used to identify the sender of emails containing child abuse images and to establish the physical address of one of the co-defendants, who was subsequently arrested and her 16-month old daughter taken into care.

At court, the prosecution case relied on evidence of phone contacts, movements and messaging between five key mobile telephone numbers. Subscriber checks had been made against these numbers to establish names and links. Historic communications data was also used to demonstrate the movement of devices attributed to the defendants and show that they were consistent with conversations that took place between them.

Watkins pleaded guilty and in December 2013 was sentenced to 35 years. Two co-defendants, who were mothers of babies sexually abused by Watkins, also pleaded guilty and received sentences of 17 years and 14 years. Their identities have not been revealed as the names of the child victims are protected by law and, consequently, so are the mothers.

IP Bill: Communications Data Authorisations



EQUIPMENT INTERFERENCE

What is it?

32. Equipment interference allows the security and intelligence agencies, law enforcement and the armed forces to interfere with electronic equipment such as computers and smartphones in order to obtain data, such as communications, from a device. Equipment interference encompasses a wide range of activity, from remote access to computers to downloading covertly the contents of a mobile phone during a search.

Why do we need it?

33. Where necessary and proportionate the security and intelligence agencies, law enforcement and the armed forces need to be able to access communications or other information held on computers, in order to gain valuable intelligence in national security and serious crime investigations and to help gather evidence for use in criminal prosecutions. Equipment interference plays an important role in mitigating the loss of intelligence that may no longer be obtained through other techniques, such as interception, as a result of sophisticated encryption. It can sometimes be the only method by which to acquire the data. The armed forces use this technique in some situations to gather data in support of military operations.

What happens now?

34. Equipment interference is currently used by law enforcement agencies and the security and intelligence agencies; more sensitive and intrusive techniques are generally available only to the security and intelligence agencies and a small number of law enforcement agencies, including the National Crime Agency. Equipment interference is currently provided for under property interference powers in the Intelligence Services Act 1994 and covert use of the power is provided to law enforcement agencies in the Police Act 1997. A draft Code of Practice was published last year and governs the use of equipment interference powers by the security and intelligence agencies.

What will happen in the future?

35. Building on recommendations made by David Anderson QC, the ISC, the Joint Committee on the draft Investigatory Powers Bill and the Science and Technology Committee, the Bill will provide for a new, more explicit equipment interference regime that will govern the use of these techniques by law enforcement agencies, the security and intelligence agencies and the armed forces. The use of this power will be limited to the same statutory purposes as interception. Law enforcement agencies' use of equipment interference will be permitted for the prevention and detection of serious crime and emergencies only.

What safeguards are there?

36. Use of these powers by the security and intelligence agencies or the armed forces currently requires a warrant to be issued by the Secretary of State. Property interference authorisations for law enforcement agencies may be issued by an appropriate law enforcement chief. The Investigatory Powers Bill will strengthen authorisation safeguards

so that the issue of warrants will in future also be subject to approval by a Judicial Commissioner.

37. The IPC will oversee the use of equipment interference powers by law enforcement agencies, the security and intelligence agencies, and the armed forces. They will ensure that the detailed safeguards set out in the legislation and accompanying Code of Practice are stringently applied and that appropriate arrangements are in place to handle the sensitive material obtained. The Commissioner will audit how the authorities use the power and publish the findings.

What are the key provisions in the Bill?

- **The Bill will build on the recommendations made by David Anderson QC, the ISC, the Joint Committee on the draft Investigatory Powers Bill and the Science and Technology Committee by creating a new, specific equipment interference regime**

- **It will strengthen the authorisation regime so that warrants will be subject to the double-lock authorisation safeguard**

- **It will limit the use of this technique to the same statutory purposes as interception; law enforcement agency warrants will only be issued for serious crime or when there is an urgent threat to life that may be prevented**

- **As some equipment interference techniques are used by all law enforcement agencies, the Bill will permit all police forces to undertake equipment interference; a Code of Practice will outline the limitations and regulate the use of more sensitive and intrusive techniques**

- **The Bill will create a new obligation on domestic CSPs to assist in giving effect to equipment interference warrants**

What are the key changes following pre-legislative scrutiny?

- **Permitting the use of equipment interference powers by law enforcement agencies for 'threat to life' situations.** In the draft Bill, targeted EI warrants could only be used by law enforcement agencies for the purpose of preventing or detecting serious crime. This would potentially prohibit law enforcement from using equipment interference to save a life or to locate a vulnerable person or missing child. The revised Bill provides for this and also reflects the Joint Committee's recommendation on the purposes for which access to communications data should be permitted (recommendation 4).

- **Providing for urgent modifications.** The Bill makes clear that security and intelligence agencies, law enforcement agencies and the armed forces are able urgently to modify both targeted and bulk equipment interference warrants, providing them with the operational agility that they require. In fast-moving situations (such as kidnaps, or unfolding terrorist attacks) adding the names of new targets to a warrant,

when relevant to an existing warrant, is essential. The revised Bill provides appropriately robust authorisation for this process.

- **Preserving the equipment interference powers of certain public authorities.** Immigration officers, British Transport Police, the Competition and Markets Authority and the Police Investigations and Review Commissioner currently have equipment interference powers under the Police Act 1997. The revised Bill preserves their ability to use these powers in the same way as provided for in existing legislation.

- **Creation of central definitions of systems data and identifying data.** This change ensures consistency when the same data is being referred to in different contexts.

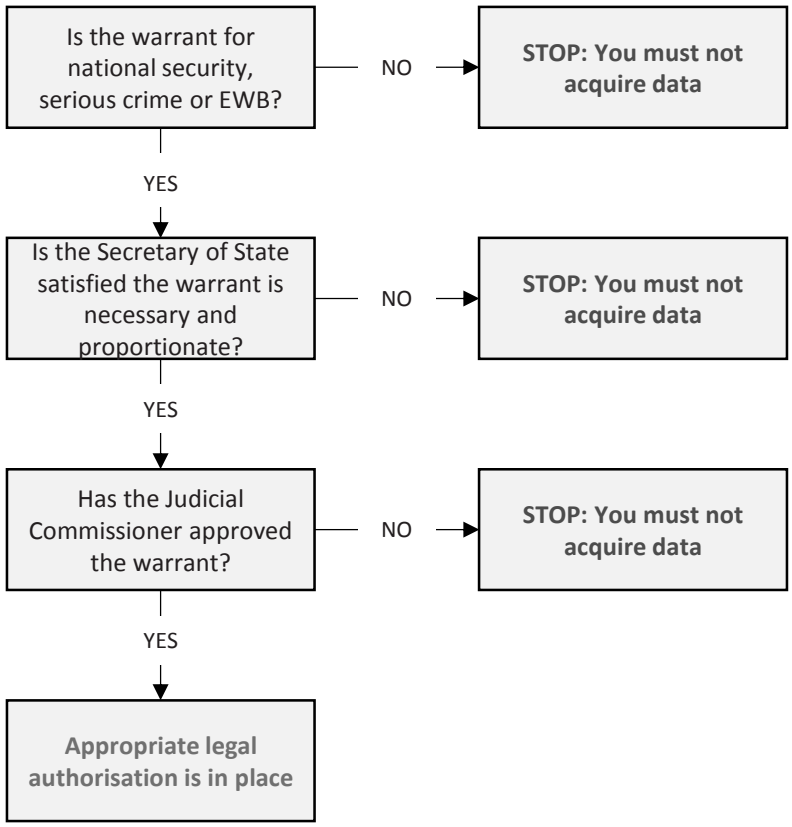
- **Updated the duty not to make unauthorised disclosures of material derived from equipment interference.** The Bill now ensures that the prohibition against the unauthorised disclosure of information relating to an equipment interference warrant applies to a broader range of individuals, such as police officers and members of the security and intelligence agencies. This will add to the safeguards applied to any sensitive material acquired through the use of this power.

EI Case Study: Attempted Murder

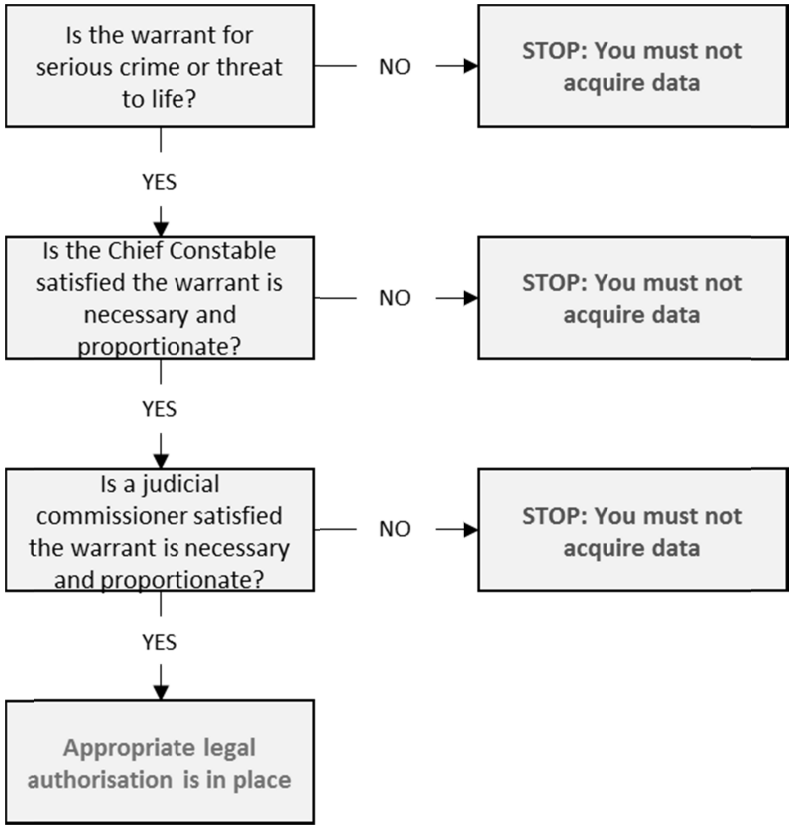
Equipment interference, when used with other intelligence-gathering techniques, is vital in time-limited cases of threat-to-life when the police need to act quickly.

In one example, intelligence was received that several suspects were at large after being involved in an attempted murder. Equipment interference and other intelligence gathering techniques were used to identify and locate the suspects leading to their arrest before further offences could be committed. Due to the intelligence acquired through equipment interference, the suspects were arrested within hours of receiving the initial intelligence. Without the use of equipment interference it would not have been possible to arrest the suspects simultaneously which was critical to preserving the evidence.

IP Bill: Equipment Interference Authorisations – MI5, SIS, GCHQ and armed forces



IP Bill: Equipment Interference Authorisations – Law Enforcement



BULK POWERS

What are they?

38. Access to bulk data is crucial in enabling the security and intelligence agencies to investigate known, high-priority threats and to identify emerging threats from individuals not previously known to them. The law provides for the use of interception, communications data and equipment interference powers in bulk. These can be used to obtain large volumes of data that are likely to include communications or other data relating to terrorists and serious criminals. Robust safeguards govern access to this data to ensure it is only examined where it is necessary and proportionate to do so.

Why do we need them?

39. The security and intelligence agencies frequently have only small fragments of intelligence or early unformed leads about people overseas who pose a threat to the UK. Equally, terrorists, criminals and hostile foreign intelligence services are increasingly sophisticated at evading detection by traditional means. Access to bulk data enables the security and intelligence agencies to:

- Obtain intelligence on overseas subjects of interest, including threats to UK citizens and our armed forces;
- Identify threats here in the UK, sometimes from fragments of intelligence;
- Establish and investigate links between known subjects of interest, at pace, in complex investigations;
- Understand known suspects' behaviour and communications methods to identify potential attack planning;
- Verify information obtained about subjects of interest through other sources (e.g. agents); and
- Resolve sometimes anonymous online personae to real world identities

40. Bulk powers are used to advance investigations both in the UK and overseas. They are integral to the work of the security and intelligence agencies.

What happens now?

41. Current legislation provides for investigatory powers to be used to acquire data in bulk:

a. **Bulk Interception** – currently provided for under RIPA, this allows for the interception of large volumes of communications in order to acquire the communications of terrorists and serious criminals that would not otherwise be available.

b. **Bulk Communications Data Acquisition** – currently provided for under section 94 of the Telecommunications Act 1984, this is used to identify subjects of interest within the UK and overseas, and to understand

relationships between suspects in a way that would not be possible using only targeted communications data powers.

c. **Bulk Equipment Interference** – currently provided for under the Intelligence Services Act 1994, equipment interference is used increasingly to mitigate the inability to acquire intelligence through conventional bulk interception and to access data from computers which may never otherwise have been obtainable.

42. The responsibility for authorising bulk warrants (or in the case of the Telecommunications Act 1984, issuing directions) currently rests with the Secretary of State. Additional safeguards, including robust internal safeguards, apply in relation to the accessing of material acquired under such warrants and directions. The security and intelligence agencies' handling arrangements for data acquired under section 94 of the Telecommunications Act 1984 were published alongside the draft Bill in November 2015.

What will happen in the future?

43. David Anderson QC, the Intelligence and Security Committee of Parliament and the panel convened by RUSI all concluded that new legislation should make explicit provision for bulk powers. The Investigatory Powers Bill provides a clear statutory framework for all of the bulk powers available to the security and intelligence agencies and introduces robust, consistent safeguards across all of those powers.

What safeguards will there be?

44. The Bill will limit the ability to apply for a bulk warrant to the security and intelligence agencies. All bulk interception, communications data and equipment interference warrants must be necessary in the interests of national security. Warrants will be issued by the Secretary of State but must first be approved by a Judicial Commissioner.

45. The Bill will require that bulk interception and bulk equipment interference warrants may only be issued where the main purpose of the activity is to acquire intelligence relating to individuals outside the UK. Conduct within the UK or interference with the privacy of persons in the UK will be permitted only to the extent that it is necessary for that purpose.

46. At the moment, a certificate authorised alongside the warrant limits the purposes for which content may be selected for examination under a bulk interception warrant; the same limitations do not apply to secondary data that may be acquired under a bulk interception warrant. The Bill will introduce new, enhanced safeguards before data obtained under bulk warrants may be accessed. Before accessing data, analysts will need to ensure that it is necessary to do so for a specific Operational Purpose authorised by the Secretary of State and approved by the Judicial Commissioner when the warrant is issued. An example of a possible operational purpose might be "To detect and disrupt direct threats to the UK and allied interests overseas from Daesh and its affiliates".

47. Additional protections will apply to content acquired under bulk interception and bulk equipment interference powers, such as the contents of an email or a photograph saved on a mobile device. Where an analyst wishes to examine the content of a UK person's data acquired incidentally under foreign-focused bulk interception or equipment interference

warrants, he or she will need to seek a new targeted examination warrant from the Secretary of State, which must be approved by a Judicial Commissioner.

48. The Bill builds on recommendations made by David Anderson QC and the RUSI panel allowing the Secretary of State to issue a bulk warrant authorising the obtaining of Secondary Data (data that can be acquired under an interception warrant but that does not communicate the meaning of the communication).

What are the key provisions in the Bill?

- **The Bill will provide a clear statutory framework for the issue of bulk interception, communications data and equipment interference authorisations**

- **The ability to seek bulk warrants will be limited to the security and intelligence agencies**

- **A bulk warrant can only be issued if it is necessary in the interests of national security**

- **Bulk interception and bulk equipment interference warrants must be focused on obtaining data relating to persons outside the UK**

- **The Secretary of State cannot issue a bulk warrant until it has been approved by a Judicial Commissioner.**

- **Access to any data obtained under a bulk warrant must be necessary for a specific Operational Purpose approved by the Secretary of State and a Judicial Commissioner**

- **A targeted warrant must be sought to look at or listen to content acquired under bulk interception and bulk equipment interference warrants relating to persons in the UK**

What are the key changes following pre-legislative scrutiny?

- **Alongside the Bill, the Government has published an operational case for the bulk powers in the Bill.** This provides greater information about the bulk powers in the Bill, how they are used and why they remain essential. This gives effect to the recommendations from the Joint Committee (recommendations 23, 28), which was also covered by the ISC (recommendation D). The security and intelligence agencies have also made available to the ISC further classified information on the necessity of bulk powers.

- **Permitting Scottish Ministers to issue examination warrants for equipment interference for serious crime in Scotland.** The revised Bill provides that examination warrants for serious crime in Scotland will be authorised by a Scottish Minister, providing consistency with the targeted EI regime.

- **Providing for urgent examination warrants.** The revised Bill provides for targeted examination warrants to be sought in urgent circumstances.

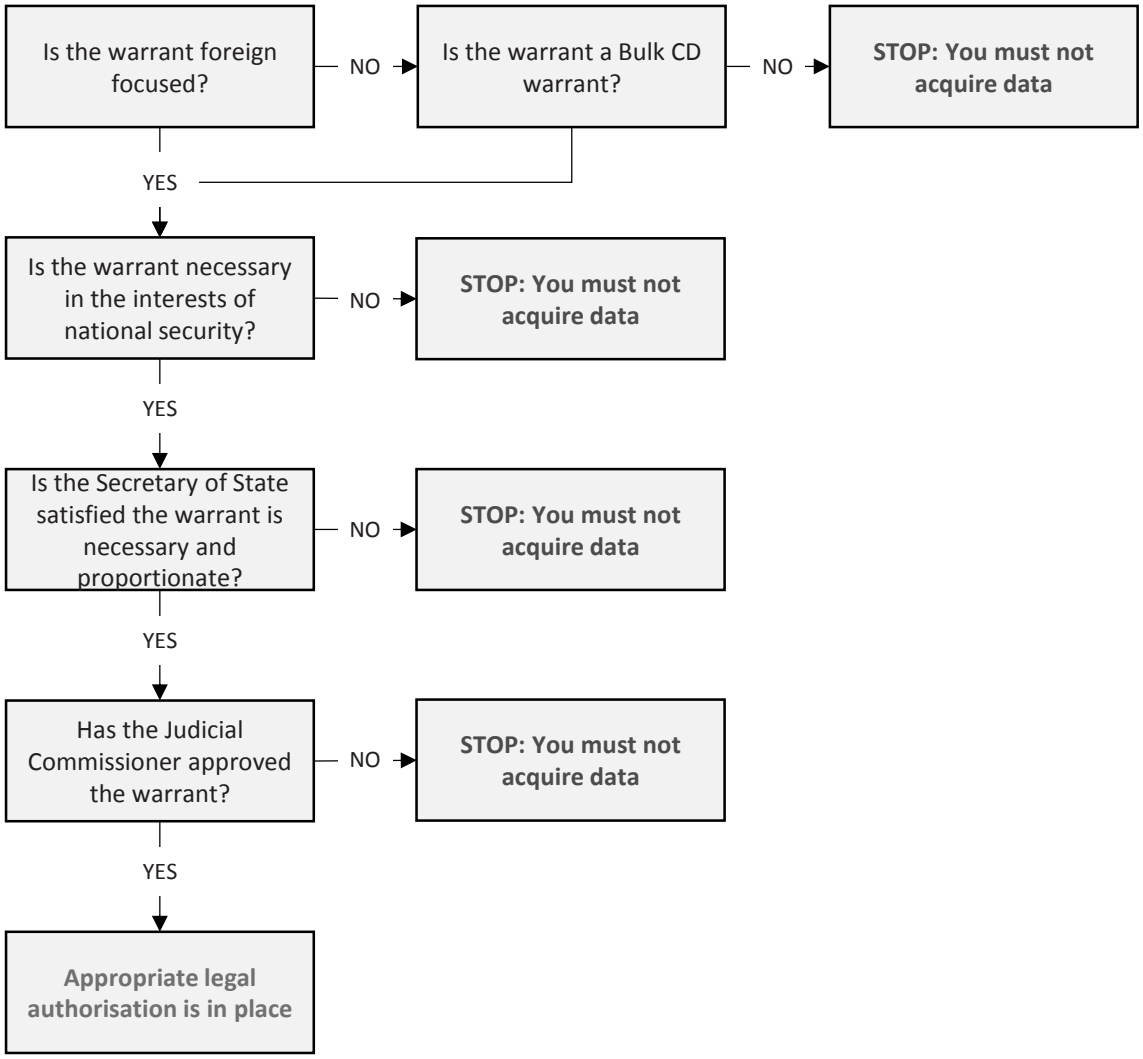
- **Providing for urgent modifications to Operational Purposes.** The revised Bill allows for the Secretary of State to amend the operational purposes for which material acquired under a bulk warrant may be examined in urgent circumstances. Such modifications must be approved by a Judicial Commissioner within five working days. This will not allow the conduct authorised by the warrant to be modified. This

will allow the security and intelligence agencies to examine data that has been acquired under existing warrants in relation to new or emerging threats.

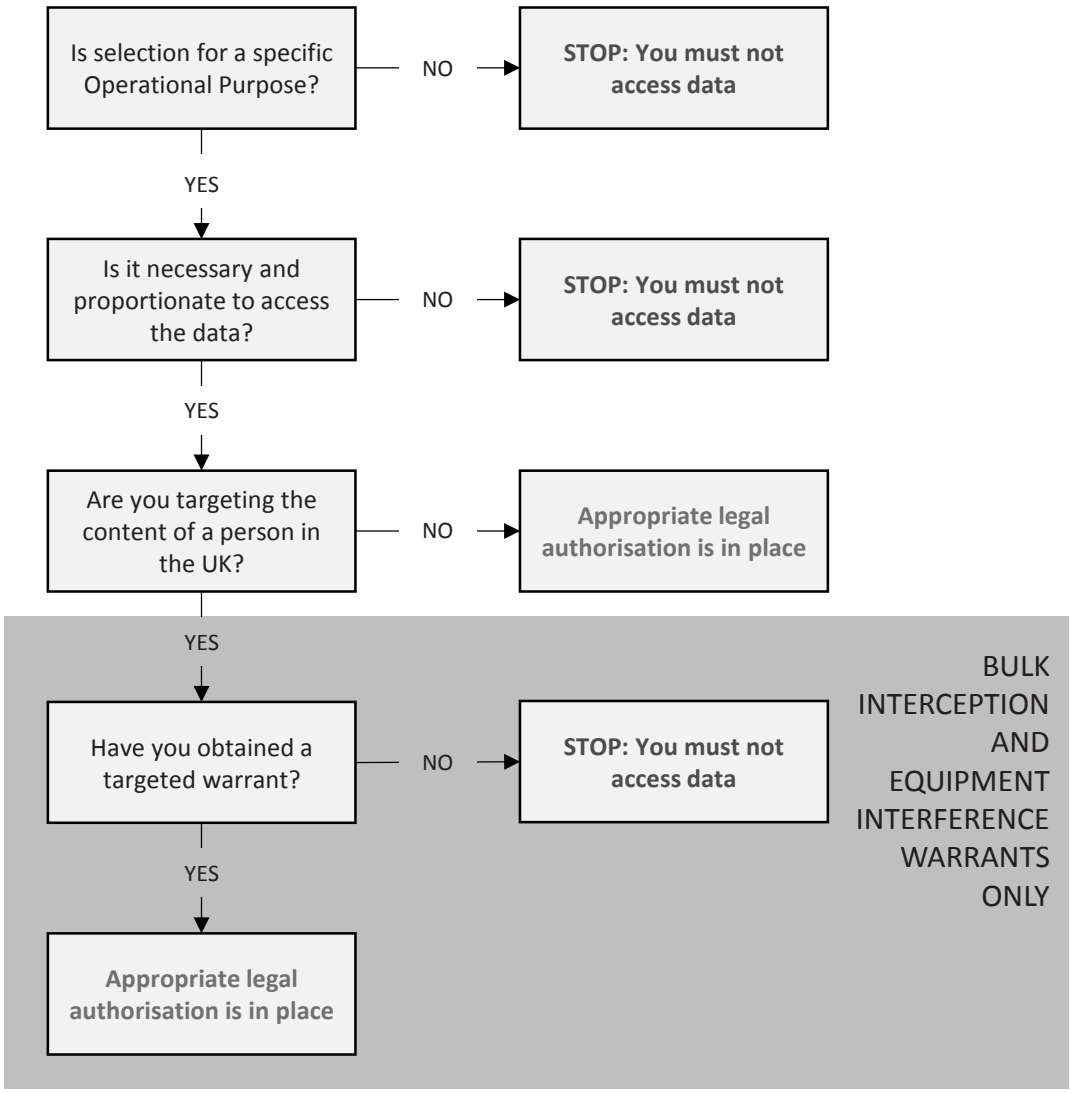
- **Providing for urgent bulk equipment interference warrants.** The Bill provides for the Secretary of State to authorise bulk equipment interference warrants in urgent circumstances. This will provide the security and intelligence agencies the ability to deploy equipment interference powers rapidly in response to fast moving events, such as a foreign cyber-attack on UK infrastructure or a terrorist attack overseas.

- **Providing for modifications to bulk equipment interference warrants, including urgent modifications.** The revised Bill provides for modification to the conduct authorised under a bulk equipment interference warrant to be made by the Secretary of State, with Judicial Commissioner approval. It also provides for the Secretary of State to authorise such modifications in urgent circumstances. This will provide the security and intelligence agencies with the ability to modify the conduct authorised under a warrant in order to respond in the most appropriate way to fast-moving events. Such modifications must be approved by a Judicial Commissioner within five working days.

IP Bill: Authorisation of Bulk Interception and Equipment Interference Warrants



IP Bill: Access to data obtained under Bulk Warrants



INTERNET CONNECTION RECORDS

What are they?

49. An internet connection record (ICR) is a record, comprised of a number of items of communications data, of an event about the service to which a customer has connected to on the internet, such as a website or instant messaging application. It is captured by the company providing access to the internet. Where available, this data may be acquired from CSPs by law enforcement and the security and intelligence agencies.

50. An ICR is not a person's full internet browsing history. It is a record of the services that they have connected to, which can provide vital investigative leads. It would not reveal every web page that they visit or anything that they do on that web page.

Why do we need them?

51. ICRs are vital to law enforcement investigations in a number of ways. For example:

- To assist in identifying who has sent a known communication online, which often involves a process referred to as internet protocol (IP) address resolution
- To establish what services a known suspect or victim has used to communicate online, allowing investigators to request more specific communications data
- To establish whether a known suspect has been involved in online criminality, for example sharing indecent images of children, accessing terrorist material or fraud
- To identify services a suspect has accessed which could help in an investigation including, for example, mapping services

What happens now?

52. There is no current requirement in law for CSPs to keep ICRs and this information may therefore be unavailable to law enforcement agencies meaning that often they can only paint a fragmented intelligence picture of a known suspect. Internet protocol (IP) address resolution identifies the sender of online communications which is provided for under the Counter Terrorism and Security Act 2015 (CTSA), but it is only possible in a limited range of cases. Because CSPs will often allocate the same IP address to many devices on their networks, it is often difficult for them to identify, in response to a request by law enforcement, which particular user or device uploaded an illegal image to a file sharing website. This is a significant problem for law enforcement. For example:

- From a sample of 6025 referrals to the Child Exploitation and Online Protection Command (CEOP) of the NCA, 862 (14%) could not be progressed and would require the ICR provisions in the Investigatory Powers Bill to have any prospect of being progressed.

- That is a minimum of 862 suspected paedophiles, involved in the distribution of indecent imagery of children, who cannot be identified or potentially prosecuted without this legislation.

53. This also means that in some cases law enforcement do not have access to essential data regarding an investigation as it has not been retained – this includes, for example, the identity of an individual suspected of sharing indecent images of children or the people with whom a missing person was last in contact.

What will happen in the future?

54. Communication service providers can be required to keep ICRs for a maximum period of 12 months. This will be invaluable to law enforcement for the prevention and detection of crime and protecting national security. The Bill will build on the provisions in the CTSA that provide for the resolution of IP addresses. Bringing the powers together in one place will ensure openness and that safeguards are applied consistently.

What safeguards will there be?

55. Applications to acquire ICRs can only be approved using the stringent application process for communications data requests and only for a limited set of statutory purposes and subject to strict controls. Local authorities will be prohibited from acquiring ICRs for any purpose.

What are the key changes following pre-legislative scrutiny?

- **Expanding the purposes for which internet connection records may be acquired.** This gives effect to a recommendation from the Joint Committee (recommendation 9). It will allow law enforcement to acquire internet connection records to identify the internet services that a person or device has accessed that are not related to communications services nor contain illegal material, provided that this is necessary and proportionate for a specific investigation.

- **Consistent definitions.** A single definition of an ICR has been created, ensuring consistency across parts 3 and 4 of the Bill, which provide for the acquisition and retention of communications data respectively. This responds to a recommendation by the Joint Committee (recommendation 7).

PROTECTIONS FOR COMMUNICATIONS INVOLVING SENSITIVE PROFESSIONS

56. Whilst everyone has a right to privacy, certain professions handle particularly sensitive or confidential information, which may attract additional protections. These professions include medical doctors, lawyers, journalists, Members of Parliament and the devolved legislatures, and Ministers of Religion.

Communications Data

57. Accessing the communications data of an individual does not disclose what that person wrote or said, rather when they communicated, where, how and with whom. Communications data does not therefore attract, for example, legal professional privilege in the same way as the content of a communication between lawyer and client. However, additional protections for sensitive professions are as a matter of policy applied to requests for communications data.

58. All applications for communications data known to be of a member of a sensitive profession must set out clearly any circumstances which could lead to an unusual amount of intrusion, invasion of privacy or infringement of a person's right to freedom of expression. In addition the DSO who signs off an authorisation to access the communications data of a member of a sensitive profession must consider whether obtaining the information is in the public interest.

59. The Interception of Communications Commissioner published a report on 4 February 2015 in respect of journalists' sources. Following this report law enforcement applications to find the source of information given to a journalist can currently only be granted if a court order is obtained from a judge under the Police and Criminal Evidence Act 1984 (PACE). This was an interim measure.

60. The Bill will put in statute a requirement for all applications to access the communications data for the purpose of identifying or confirming the identity of a journalist's source to be authorised by a Judicial Commissioner. The Bill will also require that statutory Codes of Practice issued in respect of communications data must make provision for additional safeguards that apply to sensitive professions.

Interception and Equipment Interference Warrants

61. Information obtained by interception or equipment interference can reveal the content of a communication and make clear what is being said or written. As a consequence it often involves a higher level of intrusion, specifically where particularly confidential or sensitive information is involved.

62. The Bill introduces a two stage authorisation process in which warrants must be issued personally by the Secretary of State, and only after being approved by a Judicial Commissioner.. Strict procedures will govern how any information collected under the warrant is used, kept and destroyed. In addition to these general safeguards, additional provision is made on the face of the Bill in respect of legally privileged material. These additional protections will ensure that when activity authorised by a warrant is intended to

obtain legally privileged material, it is only authorised in exceptional and compelling circumstances. Where activity authorised by a warrant is likely to obtain such material, the application for a warrant must make this clear. The Bill also makes clear that the IPC must be informed when legally privileged material has been intercepted or obtained under an equipment interference warrant, or examined and retained in relation to bulk collection.

63. In addition, the Codes of Practice will make clear that where the law enforcement agencies and security and intelligence agencies wish to obtain the communications of, or with, a member of one of the sensitive professions, particular consideration must be given where confidential information might be involved. They must make a compelling case to the Secretary of State explaining why it is necessary and proportionate to seek the warrant and what additional protections they will apply to any particularly sensitive material obtained.

64. More detail on the current protections afforded to confidential material is available in the updated Interception of Communications Code of Practice and Equipment Interference Code of Practice. Draft Codes of Practice have also been published alongside the Bill.

65. The Bill provides that, in addition to approval by a Judicial Commissioner, the Prime Minister must be consulted before the Secretary of State can decide to issue a warrant to intercept a Member of Parliament's communications. This will cover all warrants for targeted interception and equipment interference that is carried out by the security and intelligence agencies. It will also include a requirement for the Prime Minister to be consulted prior to the selection for examination of a Parliamentarian's communications collected under a bulk interception or equipment interference warrant. It will apply to MPs, members of the House of Lords, UK MEPs and members of the Scottish, Welsh and Northern Ireland Parliaments/Assemblies.

What are the key changes following pre-legislative scrutiny?

- **Requiring the security and intelligence agencies to seek independent authorisation for acquiring communications data to identify a journalistic source.** The revised Bill removes an exemption for the security and intelligence agencies and responds to a recommendation of the ISC (recommendation B). It will bring the security and intelligence agencies into line with law enforcement and other public authorities.

- **Providing protections for legally privileged communications on the face of the Bill.** The revised Bill includes explicit protections for legally privileged communications in relation to interception and equipment interference. This responds to recommendations by the Joint Committee (recommendation 46) and the ISC (recommendation B).

OBLIGATIONS ON COMMUNICATIONS SERVICE PROVIDERS

66. The use of investigatory powers relies heavily on the cooperation of CSPs in the UK and overseas. The assistance of CSPs is frequently required to obtain communications data relating to a person's use of a particular service or to intercept communications sent by that service. The assistance of CSPs may also be necessary in order to gain direct access to a suspect's device by using equipment interference powers.

CSP Obligations

67. The obligations on CSPs to provide assistance in relation to the use of investigatory powers are spread across a number of different laws:

a. DRIPA requires CSPs to retain certain types of communications data; additional retention requirements are provided under the CTSA.

b. RIPA requires CSPs to provide communications data when served with a notice, to assist in giving effect to interception warrants, and to maintain permanent interception capabilities, including maintaining the ability to remove any encryption applied by the CSP to whom the notice relates.

c. The Telecommunications Act 1984 requires CSPs to comply with directions issued by the Secretary of State in the interests of national security; this includes the acquisition of bulk communications data.

68. The Bill will bring together these obligations in a single, comprehensive piece of legislation. It will also provide an explicit obligation on CSPs to assist in giving effect to equipment interference warrants. Only those agencies that are able to apply for an interception warrant will have the ability to serve such warrants, which must be authorised by the Secretary of State and approved by a Judicial Commissioner. The Bill will not impose any additional requirements in relation to encryption over and above the existing obligations in RIPA.

69. The Bill will provide for the Secretary of State to require CSPs to maintain permanent capabilities relating to the powers under the Bill. This will replace the current obligation to maintain a permanent interception capability and will provide a clear basis in law for CSPs to maintain infrastructure and facilities to give effect to interception and other warrants.

70. CSPs may be required to provide assistance to law enforcement and the security and intelligence agencies in the interests of national security through a national security notice. This will replace the general power of direction under the Telecommunications Act 1984. The new power will be subject to strict safeguards that will prevent it from being used to authorise any activity for the purpose of interference with privacy, such as authorising or requiring the disclosure of communications data. More detail on the use of national security notices have been provided in the draft National Security Notice Code of Practice.

71. The ability for CSPs to appeal obligations will be strengthened through the Bill. The Bill will provide for the continued existence of the Technical Advisory Board (TAB), which

comprises industry and agency experts and provides advice to the Secretary of State on the cost and technical feasibility of implementing a particular obligation. In future, CSPs will be able to appeal obligations (including Data Retention Notices) directly to the Secretary of State, who will be obliged to take advice from the TAB and the IPC. The circumstances in which appeals will be permitted will be broadened to take account of CSPs' changes to services and infrastructure.

Overseas Companies

72. Interception and communications data powers rely on the support of overseas companies. The existing obligation in RIPA to comply with interception warrants (including for bulk interception) and communications data acquisition notices was clarified in 2014 through DRIPA. Other investigatory powers (such as data retention) may rely on the support of overseas companies.

73. The Bill places the same obligations on all companies providing services to the UK or in control of communications systems in the UK. However, the Bill only provides for those obligations to be enforced through the courts against overseas companies in respect of targeted communications data acquisition and (targeted and bulk) interception powers. The Bill will include explicit provision to require the Secretary of State to take account of any potential conflict of laws that overseas companies may face.

What are the key provisions in the Bill?

- **The Bill will bring together all of the existing obligations on CSPs in RIPA, DRIPA, CTSA and the Telecommunications Act 1984**

- **The Bill will provide for notices to be given to CSPs to maintain capabilities relating to the use of powers under the Bill and to take steps necessary for national security**

- **A notice will not authorise or require a CSP to disclose communications or communications data in the absence of a warrant or communications data acquisition notice**

- **Appeal routes will be strengthened by allowing for appeals directly to the Secretary of State, who will take advice from the TAB and the IPC**

- **Enforcement of obligations against overseas CSPs will be limited to interception and targeted CD acquisition powers**

What are the key changes following pre-legislative scrutiny?

- **Amending the language on encryption in the Bill on technical capability notices.** The revised Bill makes clear that obligations to remove encryption from communications only relate to electronic protections that have been applied by, or on behalf of, the company on whom the obligation has been placed and / or where the company is removing encryption for their own business purposes. The Bill has also been revised to make clear that where an obligation is placed on a CSP which

includes the removal of encryption, the technical feasibility, and likely cost of complying with those obligations must be taken into account. This responds to recommendations from the Joint Committee (recommendations 16 and 17) and the Science and Technology Committee (recommendations 3 and 4).

- **Making clear the process that must be followed when a CSP is introducing a new service which may be subject to obligations.** This responds to concerns from the CSPs that the process could be clearer, as could the circumstances in which a right of review is conferred.

- **Making clear that the obligations that could be imposed on CSPs with 10,000 customers or more, are only imposed if the Secretary of State serves a notice on the CSP.** The Bill now makes clear that the obligation is only imposed when a notice is served.

- **Making clear that a CSP can disclose the existence and content of a technical capability notice with the permission of the Secretary of State.** This responds to CSP calls for permission to discuss obligations, and the way in which they can be met, with third party providers or in industry fora where appropriate.

BULK PERSONAL DATASETS

What are they?

74. Bulk Personal Datasets (BPDs) are sets of personal information about a large number of individuals, the majority of whom will not be of any interest to the security and intelligence agencies. The datasets are held on electronic systems for the purpose of analysis by the security and intelligence agencies. Examples of these datasets include the electoral roll, telephone directories and travel-related data.

Why do we need them?

75. BPDs are essential in helping the security and intelligence agencies identify subjects of interest or individuals who surface during the course of an investigation, to establish links between individuals and groups, to understand better a subject of interest's behaviour and connections and quickly to exclude the innocent. In short, they enable the agencies to join the dots in an investigation and to focus their attention on individuals or organisations that threaten our national security.

What happens now?

76. The security and intelligence agencies have powers under the Security Service Act 1989 and the Intelligence Services Act 1994 to acquire and use BPDs to help them fulfil their statutory functions, including protecting national security. The use of BPD is subject to stringent internal handling arrangements and the regime is overseen by the Intelligence Services Commissioner. BPDs may be acquired using investigatory powers, from other public sector bodies or commercially from the private sector.

What will happen in the future?

77. The Bill will provide robust new safeguards that apply to the retention and examination of BPDs.

What safeguards will there be?

78. There will be two types of warrant – Class BPD warrants and Specific BPD warrants. Class BPD warrants will authorise the retention of a class of BPDs, such as certain kinds of travel data. Specific BPD warrants will authorise the retention of a specific dataset – this could be because the dataset is of a novel or unusual type of information so does not fall within an existing class BPD warrant, or because a dataset raises particular privacy concerns that should be considered separately. Both types of warrant last for six months. They will be issued by the Secretary of State, who must consider that the warrant is necessary and proportionate and adequate measures are in place to store the datasets securely. As will be the case for interception and equipment interference authorisations, a Judicial Commissioner must also approve the Secretary of State's decision to issue the warrant. The Bill provides for urgent specific BPD warrants that must be approved by a Judicial Commissioner three working days after they have been authorised by a Secretary of State.

79. A statutory Code of Practice will set out additional safeguards which apply to how the agencies access, store, destroy and disclose information contained in the BPDs.

80. The Investigatory Powers Commissioner will oversee how the agencies use these datasets. Supported by a team of Judicial Commissioners and technical and legal experts, the Commissioner will audit how the agencies use them and they will report publicly on what they find.

What are the key provisions in the Bill?

- **The Bill will provide for new safeguards in respect of the security and intelligence agencies' retention and use of BPDs**

- **Class or specific BPD warrants are subject to the 'double lock' authorisation safeguard**

- **The data can only be examined for the Operational Purposes specified on the warrant and agreed by the Secretary of State and Judicial Commissioner**

- **The Code of Practice will provide clear guidance on whether it is appropriate to seek a specific warrant for a particular BPD**

- **In considering whether a class warrant should be renewed, the Secretary of State will consider the datasets held under the warrant**

- **The Bill will place time limits on the initial examination of BPDs**

What are the key changes following pre-legislative scrutiny?

- **Alongside the Bill, the Government has published an operational case for the bulk powers in the Bill.** This provides greater information about the bulk powers in the Bill, how they are used and why they remain essential. This gives effect to the recommendations from the Joint Committee (recommendations 23, 28), which was also covered by the ISC (recommendation D). The security and intelligence agencies have also made available to the ISC further classified information on the necessity of bulk powers.

- **Providing for urgent modifications to Operational Purposes.** The revised Bill allows for the Secretary of State to amend the operational purposes for which material acquired under a BPD warrant may be examined in urgent circumstances.

- **Time limits for initial examination of BPDs and applying for warrants. The** revised Bill now specifies time limits for initial examination of BPDs. These are: as soon as reasonably practicable and in any event within a maximum of three months to undertake an initial examination of a UK-originated dataset and apply for a warrant; and as soon as reasonably practicable and in any event within a maximum of six months to undertake an initial examination of a foreign-originated dataset and apply for a warrant. This responds to a recommendation made by the ISC (recommendation G).

- **Requiring new warrants for material to be retained or examined after an existing warrant is cancelled or not renewed.** The revised Bill makes clear that if the Secretary of State authorises, with Judicial Commissioner approval, the retention or examination of some material held under a warrant that is cancelled or not renewed, the agency must apply for a new warrant as soon as reasonably practicable and in any event within a maximum of three months. This responds to a recommendation made by the ISC (recommendation ix).

BPD Case Study: Preventing Access to Firearms

The terrorist attacks in Mumbai in 2008 and the more recent shootings in Copenhagen and Paris in 2015, highlight the risk posed by terrorists gaining access to firearms. To help manage the risk of UK based subjects of interest accessing firearms, the intelligence agencies match data about individuals assessed to have access to firearms with records of known terrorists. To achieve this, the security and intelligence agencies acquired the details of all these individuals, even though the majority will not be involved in terrorism and therefore will not be of direct intelligence interest. This allowed the matching to be undertaken at scale and pace, and more comprehensively than individual requests could ever achieve. Completing such activities enabled the intelligence agencies to manage the associated risks to the public.

INVESTIGATORY POWERS AT A GLANCE

	Conduct authorised	Statutory bodies / purposes	Authorisation - Acquisition	Authorisation - Access	Oversight
Interception	Obtaining the content of a communication in the course of its transmission	MI5, GCHQ, SIS, Ministry of Defence and five law enforcement agencies Purposes: National security, serious crime and economic well-being of the UK	Secretary of State authorisation, subject to approval by a Judicial Commissioner before warrants come into force	N/A	Investigatory Powers Commission (IPC) replaces the Interception of Communications Commissioner Office (IOCCO), the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (IsCom) The judge-led IPC will have an extensive remit to oversee the use of all investigatory powers and will scrutinise those provided with these powers though inspections, investigations, audits and authorisations of warrants and internal practices Statutory Codes of Practice provide further details, and information of how the powers work in practice
Communications Data (CD)	Obtain CD, usually via Communications Service Providers (CSPs)	Public authorities set out on the face of the Bill and approved by Parliament. Statutory purposes are detailed in the Bill	Must be authorised by a designated senior officer (who must be independent from the investigation) following consultation with a single point of contact (SPOC). Only the SPOC can approach CSPs to request CD	N/A	
Equipment Interference (EI)	Obtaining communications, information and other data from computers and other equipment	MI5, GCHQ, SIS, law enforcement and the Ministry of Defence Purposes: National security, serious crime and economic well-being. Law enforcement may only seek warrants for serious crime or in certain circumstances to prevent death or harm	Security and intelligence agencies and MOD: Secretary of State authorisation, subject to approval by a Judicial Commissioner before warrants come into force Law enforcement agencies: Law enforcement chief authorisation. All warrants subject to approval by a Judicial Commissioner before warrants come into force	N/A	
Bulk Powers	Bulk interception, equipment interference and acquisition of communications data	MI5, GCHQ, SIS Purposes: Warrants must be necessary in the interests of national security; may also be authorised for serious crime and economic well-being when combined with national security	Secretary of State authorisation, subject to approval by a Judicial Commissioner before warrants come into force Interception and equipment interference warrants must be targeted at persons outside of the UK	Examination of any material must be necessary for a specific Operational Purpose, authorised by a Secretary of State and approved by a Judicial Commissioner Examination of content relating to persons in the UK requires a new separate targeted warrant	
Bulk Personal Datasets (BPD)	Additional safeguards for the retention and use of BPD	MI5, GCHQ, SIS Purposes: National security, serious crime and economic well-being	Authorisation to retain particular classes of BPD or specific BPDs issued by Secretary of State and subject to approval by a Judicial Commissioner before warrants come into force	Examination of any material must be necessary for a specific Operational Purpose, authorised by a Secretary of State and approved by a Judicial Commissioner	

Government response to the recommendations of the Joint Committee on the draft Investigatory Powers Bill

	Recommendation	Government response
1	We are grateful that the Government has provided further information on the interpretation of communications data and content. We have not had an opportunity to seek views as to whether the definitions are now sufficiently clear. Parliament will need to look again at this issue when the Bill is introduced. 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 Government recognises the importance of engagement with Communications Service Providers (CSPs) on the provisions in the Bill, and is committed to on-going, detailed consultation with companies that may be subject to obligations under the Bill. The Government appreciates the importance of clarity around definitions for CSPs, oversight bodies and others. The draft Codes of Practice published alongside the revised Bill provide further information on how the definitions in the Bill will work in practice. The Government invites comments on the draft Codes. New Codes of Practice will be published for formal consultation following Royal Assent of the Bill; they will require approval by Parliament and will have statutory force and these will be subject to full consultation with industry and with the public.
2	This definition of data in Clause 195 is unclear, unhelpful and recursive. The Government must provide a meaningful and comprehensible definition of data when the Bill is introduced.	Clause 225 of the revised Bill provides an updated definition of data. This makes clear that the term “data” in the revised Bill includes information which is not electronic information.
3	We recommend that Parliament should give further consideration to defining the purposes for which local authorities may be allowed to apply for communications data when the Bill is introduced.	Local authorities are responsible for investigating a range of serious offences such as scams to target the elderly, rogue traders, environmental offences such as dumping hazardous waste illegally and benefit fraud. Clause 64 provides that local authorities are only permitted to acquire communications data for the purpose of preventing or detecting crime or of preventing disorder. Local authority communications data requests must be signed off by a magistrate, and all local authority requests must be made by Single Points of Contact in an independent body. The Investigatory Powers Bill prohibits local authorities from having access to Internet Connection Records (ICRs). The Government looks forward to Parliament’s consideration of this issue during the Bill’s passage.

4	We believe that law enforcement should be able to apply for all types of communications data for the purposes of 'saving life'. We recommend that the Home Office should undertake further consultation with law enforcement to determine whether it is necessary to amend clause 46 (7) (g) to make this explicit on the face of the Bill.	The Government has amended Clause 46(7)(g) of the revised Bill now Clause 53 to remove the words 'in an emergency' to make it clear that law enforcement can always acquire communications data for the purpose of saving lives.
5	We recommend 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 has included a section relating to subject access requests in Chapter 11 of the draft Code of Practice on Communications Data, which has been published alongside the revised Bill.
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 on introduction provide further detail and address the points on the technical feasibility of ICRs which were raised with the Committee. The Government will continue to discuss ICRs with those service providers likely to be affected by the obligations in the Bill.
7	We recommend that the definition of Internet Connection Records 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'. We recommend that more effort should be made to reflect not only the policy aims but also the practical realities of how the internet works on a technical level.	The Government has made amendments to the Bill to ensure that it contains a single definition of ICRs – see Clause 54. Chapters 2 and 7 of the draft Code of Practice on Communications Data provide further information and guidance on the definition and uses of ICRs, including examples of 'internet services' and 'internet communications services' to assist with the interpretation of those terms.
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 welcomes the Committee's acknowledgement that there are important differences between the ICR proposal in the Bill and the system used in Denmark. The Government has published an assessment of those differences alongside introduction of the Bill.
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 this is necessary and proportionate for a specific investigation.	The Government has redrafted Clause 54 of the Bill to widen the purposes for which law enforcement may seek to access ICRs, including which internet service is being used. Further guidance on access to ICRs can be found in Chapter 7 of the draft Code of Practice on Communications Data.

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, which has recognised expertise in this area, to draw up a set of standards for CSPs [in the area of data retention security].	When setting out the steps that a CSP needs to take to meet its security obligations, the Government already draws upon a set of recognised security standards. Detailed guidance is contained in Chapter 16 of the draft Code of Practice on Communications Data. It is important that CSPs can put in place security safeguards that are appropriate to the nature of the data being retained. The Government will, however, consult the Information Commissioner's Office, the National Technical Assistance Centre and GCHQ with a view to being able to provide clear and consistent standards for CSPs retaining data under the obligations in the Bill.
11	As the communications data will be held for purposes that are not related to the CSP's own business purposes, we agree that the Government should provide CSPs with whatever technical and financial support is necessary to safeguard the security of the retained data. 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.	It would not be appropriate to commit future Governments to pay the full cost of compliance, as it would limit their discretion on this issue. The Government welcomes the Committee's conclusion on this point. In practice, the Government has a long-standing position of reimbursing 100% of the costs associated with data retention. There are no current plans to change that policy, which was confirmed by the Home Secretary on the floor of the House of Commons on 21 February 2016. Any retention notice must specify the level, or levels of contribution which the Secretary of State determines should apply in relation to that notice. Clause 80 of the Bill provides a clear route for CSPs to appeal to the Secretary of State should a company consider that the obligation placed on them would incur unreasonable costs. In considering their appeal, the Secretary of State must take advice from the Technical Advisory Board (TAB) on costs and technical feasibility and from the Investigatory Powers Commissioner (IPC) on proportionality.
12	Our view is that the Government should provide statutory guidance on the cost recovery models, and that with particular consideration should be given to how the Government will support smaller providers served with data retention notices.	Further guidance on costs is included in Chapter 19 of the draft Communications Data Code of Practice. This notes where the arrangements are of particular importance to smaller providers. The draft Codes of Practice relating to other powers in the Bill also provide detail on costs.
13	We agree with the Government's intention not to require	The Bill provides a definition of 'relevant communications data' in

	CSPs to retain third party data. The Bill should be amended to make that clear, either by defining or removing the term "relevant communications data".	Clause 78. If this term were removed, it would reduce the clarity regarding what data a CSP could be required to retain. Chapter 2 of the draft Communications Data Code of Practice also includes a clear restriction on third party data retention by CSPs.
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.	Further clarity on generation of data has been provided in Chapter 14 of the draft Communications Data Code of Practice.
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, perhaps through the Technical Advisory Board, is made available so that CSPs subject to such notices can share views on how best to comply with them.	Clause 84(4) of the Bill has been added to enable CSPs to disclose the existence and contents of a notice with permission of the Secretary of State. As set out in Chapter 18 of the draft Code of Practice on Communications Data, this will provide for disclosure to relevant oversight bodies and other CSPs served with a notice.
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.	Clauses 217 and 218 of the Bill have been amended to make clear the obligations that can be imposed on CSPs with regard to encryption. This explains what is meant by 'removing electronic protection' and makes clear that CSPs can only be required to remove protection that they themselves have applied, or that has been applied on their behalf. Other provisions in the Bill at Clause 218 set out the considerations that must be taken into account when considering whether it is necessary and proportionate to issue a technical capability notice. The relevant draft Codes of Practice provide detailed information on technical capability notices and the obligations that can be imposed on CSPs.
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 decrypted copies of those communications if it is not practicable for them to do so. We recommend that a draft Code of Practice should be published alongside the Bill for Parliament to consider.	
18	We recommend that the Government should produce a Code of Practice on Equipment Interference to cover the activities both of the security and intelligence agencies and of law enforcement.	A draft Code of Practice on Equipment Interference, covering both the security and intelligence agencies (SIAs), and law enforcement agencies (LEAs), has been published alongside the Bill at introduction. This builds on the existing Code of Practice for the use of Equipment Interference, which was approved by Parliament in January 2016 and which provides for the SIAs' use of EI.

		GCHQ's use of equipment interference and the safeguards in place have recently been subject to litigation. The Investigatory Powers Tribunal (IPT) handed down their judgment in the case of Privacy International and Greennet & Others (IPT 14/85/CH, IPT 14/120-126/CH) on 12 February 2016. The IPT supported the lawfulness of the current EI regime, including the safeguards provided in the existing Code of Practice.
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 on Equipment Interference provides further information on the key terms to ensure greater clarity.
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.	Clause 112 of the revised Bill requires the Secretary of State to ensure that there are arrangements in place for the security and protection of data acquired under EI. Chapter 6 of the draft Equipment Interference Code of Practice provides further information on data protection both in regard to agency systems and those systems which may be interfered with when using EI capabilities.
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 documentation produced in support of the Bill makes clear that CSPs will not be in breach of their data protection obligations in giving effect to an EI warrant, as all activity carried out under a warrant is lawful. Chapter 6 of the draft Equipment Interference Code of Practice provides further information on the impact of the Data Protection Act.
22	We agree that material acquired through targeted equipment interference warrants should be admissible in court, though we share the concerns of witnesses about the risks involved. We believe that law enforcement and the security and intelligence agencies will need detailed codes of practice and appropriate procedures to ensure that evidence is not inadvertently compromised. We urge	Chapters 2 and 8 of the draft Equipment Interference Code of Practice provides guidance on this matter for law enforcement agencies. Further advice and operational guidance will continue to be provided by relevant oversight and governance bodies, including the Investigatory Powers Commissioner (IPC). The Government will also continue to work with law enforcement agencies, the College of Policing and the Crown Prosecution

	the Government to consider how it will reconcile the understandable desire of law enforcement and the security and intelligence agencies to keep their techniques secret with the need for evidential use and disclosure regimes in legal proceedings.	Service to consider how the guidance and training provided in relation to using EI-derived information in court can be developed further.
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 Intelligence and Security Committee or the Interception of Communications Commissioner.	An operational case for the use of bulk powers has been published alongside introduction of the revised Bill. Further classified documentation has been provided to the Intelligence and Security Committee (ISC), the Interception of Communications Commissioner and the Intelligence Services Commissioner in parallel.
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.	Limiting the bulk interception and equipment interference powers to overseas-related communications provides an important safeguard, and ensures that these powers are not directed at individuals in the UK. The operational case for bulk powers provides further examples of how they are used to gather overseas-related communications. The communications or data of individuals in the UK may only be intercepted or obtained in so far as that is necessary to do what is expressly authorised by a bulk interception or bulk equipment interference warrant. Examination of the content of a UK person's data acquired by these means will require a targeted examination warrant issued by the Secretary of State and approved by a Judicial Commissioner.
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 for improvements if required.	Clause 201 of the revised Bill provides for the IPC to make both annual and ad hoc reports. The Government would expect the IPC to report in detail as to whether the bulk safeguards were operating effectively and to make any recommendations as appropriate.
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	Considerations of such risks will be integral to the determination of the proportionality of any warrant application. Chapter 3, 4 and 5 of the draft Equipment Interference Code of Practice provides further guidance on how collateral intrusion should be

	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.	considered in any decision to issue a warrant, and Chapter 3 elaborates on the considerations that should be made in regards to the security of networks and systems.
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.	Chapter 6 of the draft Equipment Interference Code of Practice provides guidance on this issue. This explains the process that any agency should adhere to when requiring assistance from a CSP in effecting an EI warrant, including the consultation that should take place before any such interference begins.
28	We recommend that the Home Office should produce its case for bulk personal datasets (BPDs) when the Bill is published.	An operational case for bulk powers, including bulk personal datasets, has been published alongside introduction of the revised Bill. Further classified information has also been provided to the ISC.
29	We recommend that the Intelligence and Security Committee, in their analysis of BPDs, should assess the extent to which the concerns expressed by witnesses are justified.	The Government has provided further information to the ISC on the BPD provisions in the Bill and will provide the Committee with any further information it requires.
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.	A detailed draft Code of Practice on the security and intelligence agencies' retention and use of Bulk Personal Datasets has been published alongside the revised Bill. Chapters 4, 5 and 7 include guidance relating to safeguards. Each of the security and intelligence agencies is a data controller in relation to all the personal data that it holds. Accordingly, the agencies are in general required by section 4(4) of the Data Protection Act 1998 (DPA) to comply with the Data Protection Principles in Part I of Schedule 1 to the DPA. That obligation is subject to sections 27(1) and 28(1) of the DPA, which exempt personal data from (among other things) the Data Protection Principles if the exemption 'is required for the purpose of safeguarding national security'. By virtue of section 28(2) of the DPA, a Minister may certify that exemption from the Data Protection Principles is so required. Ministerial Certificates have been issued for each of the security and intelligence agencies. Those Certificates certify that

		personal data that are processed in performance of their functions are exempt from the First, Second and Eighth Data Protection Principles (and are also exempt in part from the Sixth Data Protection Principle). The Certificates do not exempt the SIA from their obligation to comply with the Fifth and Seventh Data Protection Principles, which provide: '5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. '7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.'
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 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.

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.	Clause 30 of the Bill provides that a Secretary of State must be notified of major modifications to a targeted interception warrant. All such modifications will be subject to retrospective oversight by the IPC. To require authorisation by a Judicial Commissioner for each such modification would drastically reduce the operational agility of the agencies. Currently the law (RIPA) allows for major modifications to be made to thematic targeted interception warrants. This ability is a key feature in the effective operation of the warrantry system. Such warrants are used for fast moving and urgent events – for example, when a person has been kidnapped and his life is in imminent danger. Being able to have a single targeted warrant against the group of kidnappers, without needing to seek separate authorisations for each of the kidnappers as their identities become known has significant operational benefits. Thematic warrants are not, though, just important for urgent situations. If, for example, a law enforcement agency wished to intercept the users of a paedophile file sharing website, they would be likely to use a thematic warrant because it would not be possible to identify each individual user beforehand. It would be permissible to use a thematic warrant in such a case because there would be a clear link between the group and the necessity and proportionality considerations for the interception of each suspected paedophile could be properly considered by the Secretary of State. In his March 2015 annual report, the Interception of Communications Commissioner's, Sir Anthony May, agreed that such warrants comply with the law '*so long as they sufficiently name or describe the combination or association of persons'*. The Investigatory Powers Tribunal (IPT) considered the issue in the context of GCHQ's use of equipment interference powers and found it lawful (see response to recommendation 18). The IPT made clear that in order for a thematic warrant to be

		granted, the description of the interference needed to be sufficiently foreseeable for the Secretary of State to be able effectively to consider necessity and proportionality. The draft Codes of Practice for Interception and Equipment Interference set out these requirements. The Investigatory Powers Bill preserves this essential ability for major modifications to be made, but only where they are necessary and proportionate and within the boundaries of the original Secretary of State / Judicial Commissioner approved warrant. As an additional safeguard, the Bill requires such major modifications to be notified to the Secretary of State. The Investigatory Powers Commissioner also provides retrospective oversight of all modifications. Where targeted interception or equipment interference warrants relate to more than one person, to a group or to an operation, the Bill requires that those persons are named or described wherever it is reasonably practicable to do so. This is to ensure the Secretary of State and the Judicial Commissioner have the fullest possible picture when approving the warrant.
33	The omission of a reference to the Mental Health (Care and Treatment) (Scotland) Act appears to us to be an oversight, which we agree could lead to the creation of conflicting authorisation regimes for the use of interception in psychiatric hospitals in Scotland. The Committee recommends that this apparent oversight be addressed in the revised Bill.	Provision relating to this Act is now included in the revised Bill, at Clause 43.
34	We recommend that the Home Office should further review its list of investigatory powers in other legislation to ensure that nothing else has been overlooked.	The Government has undertaken a further review of other statutes that remain available to intercept communications and acquire communications data and believes that, where necessary, they are provided for in the Bill. One clarification that has been identified is the interception of postal communications in immigration centres provided for in

		rules issued under the Immigration and Asylum Act 1999. This is now provided for at Clause 44.
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 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. Equipment interference warrants for the security and intelligence agencies are issued by the Secretary of State. When modifications are required the Secretary of State, or a senior official reporting to the Secretary of State, can authorise any such modification (if the modification is considered necessary and proportionate). If the modification is made by a senior official the Secretary of State must be informed. This ensures that modifications are overseen by the original issuing authority. Equipment interference warrants for law enforcement agencies are issued by the respective law enforcement chief, rather than the Secretary of State. Modifications can be made by either the law enforcement chief or an appropriate delegate. In the absence of judicial oversight, this would mean that modifications could be made without any external or independent consideration. The Government therefore feels that it is appropriate to require a Judicial Commissioner to review any modifications by law enforcement chiefs/delegates, in order to maintain a robust authorisation process.
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.	Clause 22 of the revised Bill now provide that urgent warrants must be approved by a Judicial Commissioner within three working days of authorisation by a Secretary of State. They will continue to last for five working days before, if appropriate, they must be renewed.

		The Government believes that this will provide sufficient time for the Judicial Commissioner to be presented with the facts of the case and to reach a decision on the necessity and proportionality of the warrant.
37	The Committee recommends the inclusion of a definition of the word 'urgent' for the purposes of authorising urgent warrants.	The relevant draft Codes of Practice published alongside the draft Bill make clear that urgent warrants should fall into at least one of the following three categories: • Imminent threat to life or serious harm - for example, if an individual has been kidnapped and it is assessed that his life is in imminent danger; • An intelligence gathering opportunity which is significant because of the nature of the potential intelligence, the operational need for the intelligence is significant, or the opportunity to gain the intelligence is rare or fleeting – for example, a group of terrorists is about to meet to make final preparations to travel overseas; • A significant investigative opportunity - for example, a consignment of Class A drugs is about to enter the UK and law enforcement agencies want to have coverage of the serious criminals in order to effect arrests.
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.	Clause 30 of the Bill provides that a Secretary of State must be notified of major modifications to a targeted interception warrant. All such modifications will be subject to retrospective oversight by the IPC. To require authorisation by a Judicial Commissioner for each such modification would drastically reduce the operational agility of the agencies. Currently the law (RIPA) allows for major modifications to be made to thematic targeted interception warrants. This ability is a

		key feature in the effective operation of the warrantry system. Such warrants are used for fast moving and urgent events – for example, when a person has been kidnapped and his life is in imminent danger. Being able to have a single targeted warrant against the group of kidnappers, without needing to seek separate authorisations for each of the kidnappers as their identities become known has significant operational benefits. Thematic warrants are not, though, just important for urgent situations. If, for example, a law enforcement agency wished to intercept the users of a paedophile file sharing website, they would be likely to use a thematic warrant because it would not be possible to identify each individual user beforehand. It would be permissible to use a thematic warrant in such a case because there would be a clear link between the group and the necessity and proportionality considerations for the interception of each suspected paedophile could be properly considered by the Secretary of State. In his March 2015 annual report, the Interception of Communications Commissioner's, Sir Anthony May, agreed that such warrants comply with the law '*so long as they sufficiently name or describe the combination or association of persons'*. The Investigatory Powers Tribunal (IPT) considered the issue in the context of GCHQ's use of equipment interference powers and found it lawful (see response to recommendation 18). The IPT made clear that in order for a thematic warrant to be granted, the description of the interference needed to be sufficiently foreseeable for the Secretary of State to be able effectively to consider necessity and proportionality. The draft Codes of Practice for Interception and Equipment Interference set out these requirements. The Investigatory Powers Bill preserves this essential ability for major modifications to be made, but only where they are necessary and proportionate and within the boundaries of the

		original Secretary of State / Judicial Commissioner approved warrant. As an additional safeguard, the Bill requires such major modifications to be notified to the Secretary of State. The Investigatory Powers Commissioner also provides retrospective oversight of all modifications. Where targeted interception or equipment interference warrants relate to more than one person, to a group or to an operation, the Bill requires that those persons are named or described wherever it is reasonably practicable to do so. This is to ensure the Secretary of State and the Judicial Commissioner have the fullest possible picture when approving the warrant.
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.	The Bill and Chapter 6 of the associated draft Communications Data Code of Practice address recommendations made by the Interception of Communications Commissioner and by David Anderson in 'A Question of Trust' with regards to the acquisition of communications data for the purposes of identifying journalistic sources, and provide clear guidance on the additional considerations that apply when seeking to obtain data in relation to any person who handles privileged or otherwise confidential information. In addition Chapter 6 in the draft Code of Practice also now provides for 'novel or contentious' requests to be referred to the IPC for consideration, and includes information on the special considerations that must be made in respect of sensitive professions.
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 welcomes the Committee's recognition of the importance of the SPOC process. The draft Code of Practice on Communications Data makes clear the steps public authorities should take to ensure a SPOC is available. However, there may be circumstances where, despite the best efforts of the public authority, a SPOC is not available. In very limited circumstances it is important that an emergency process is available to, for example, avoid loss of life. More details on the limitations of this

		provision can be found in Chapter 4 of the Communications Data Code of Practice. The Home Office will work with public authorities and CSPs to put in place clear processes so that a CSP can validate the authenticity of requests not made through a SPOC. The IPC will be notified whenever these procedures are used, to ensure retrospective oversight.
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.	The Government has amended Clause 63 so that the enhanced affirmative procedure is required for any change to the list of ranks and offices which must be held by a designated officer 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.
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.	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. This would, for example, allow the Secretary of State to authorise a class of dataset relating to travel where these conditions were met, such as for datasets that are similar in nature but refer to different travel routes or are provided by different sources. 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 draft Code of Practice provides clear guidance on the factors that the security and intelligence agencies will need to consider in determining whether it is appropriate to use a class warrant or whether it may be more appropriate to apply for a specific BPD warrant. These factors include whether the nature or the provenance of the dataset raises particularly novel or contentious issues; whether it contains a significant component of intrusive data; and whether it contains a significant component

		of confidential information relating to members of sensitive professions. The draft Code of Practice published alongside the revised Bill also sets out detailed requirements about how the security and intelligence agencies must keep under review the ongoing necessity of holding individual datasets, including those retained under a class warrant. In considering whether a class warrant should be renewed, the Secretary of State will consider whether continued retention of datasets held under the warrant remains necessary and proportionate. This decision will be subject to review by a Judicial Commissioner. 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 – there may be a particular dataset that is, for example, updated on a weekly or monthly basis. In these cases the necessity and proportionality case and operational purposes would not alter within these timeframes. To require repeated new warrants in this scenario would not be proportionate; the notion of a replacement warrant simply allows the agencies to use this amended data in line with the existing authorisation.
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.	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, as set out in the new Clause 47 in the revised Bill. This reflects the fact that the legal systems and protections that apply in other jurisdictions may not be exactly the same as those in the UK. The revised Bill makes clear in Clause 113 that this applies to EI material as well as that derived from interception. The draft Codes of Practice on Interception of Communications

		and Equipment Interference also provide more information on the safeguards associated with sharing intercept and equipment interference material with international partners at Chapters 9 and 8.
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 7 of the revised Bill has been amended to make sure that an overseas agency cannot be tasked to undertake interception on behalf of a UK authority, in respect of an individual in the UK, without a targeted interception warrant or a targeted examination warrant being in place. The draft Code of Practice on Interception of Communications describes how those agencies that undertake bulk interception may request unanalysed intercepted content or secondary data from another government, where a relevant interception warrant has already been issued, or where it does not amount to a deliberate circumvention of the Act. The draft Code of Practice also makes clear that any information obtained by these means is subject to the same internal rules and safeguards that would apply to information intercepted by the agency under the Bill.
45	We recommend that the Government should give more careful consideration to the consequences of enforcing extraterritoriality. The Government should re-double its efforts to implement Sir Nigel Sheinwald's recommendations.	As the Prime Minister and Home Secretary have previously stated, the Government is engaging in preliminary discussions with international partners on how a new international framework for access to data across jurisdictions might operate in principle. This would be based on strong, human rights-compliant domestic regulatory oversight.
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.	Clauses 25 and 100 of the revised Bill contain additional safeguards for items subject to legal privilege that have been acquired by targeted interception or equipment interference, and Clauses 135 and 171 set out on the face of the Bill the safeguards that apply before content that contains legally privileged material can be selected for examination. The Law Society and Bar Council have been consulted on these clauses. Schedule 7 of the revised Bill makes clear that the Codes of

		Practice accompanying the Bill must contain particular provision in relation to journalistic information, and members of professions who hold material that is subject to legal privilege or confidential material. Information on this issue is provided in Chapter 9 of the draft Interception of Communications Code of Practice, Chapter 6 of the draft Communications Data Code of Practice, Chapter 8 of the draft Equipment Interference Code of Practice, Chapter 9 of the draft Bulk Acquisition Code of Practice and Chapters 4 and 7 of the draft Code of Practice on the security and intelligence agencies' retention and use of Bulk Personal Datasets.
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	A memorandum on the ECHR and other human rights issues has been published alongside the introduction of the Bill, which makes clear how the provisions in the Bill meet the requirements of Article 8 and relevant case law.
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.	The Government is satisfied that the additional protections set out in the new draft Codes of Practice which have been published alongside the revised Bill are appropriate in relation to journalistic material. This reflects the fact that it is much harder to define in law what constitutes a journalist (as opposed to legally privileged material), as seen during the Joint Committee's evidence sessions on this issue. However, Schedule 7 of the revised Bill now makes clear that all the Codes of Practice accompanying the Bill must contain particular provision in relation to journalistic information. The draft Bill and associated draft Communications Data Code of Practice address the recommendations made by the Interception of Communications Commissioner and by David Anderson in 'A Question of Trust' with regards to acquisition of communications data for the purposes of identifying journalistic sources. PACE and the Terrorism Act 2000 provides appropriate mechanisms for law enforcement bodies to obtain journalistic

		material from journalists. RIPA, and now the revised Bill, is the appropriate mechanism for acquisition of communications data from CSPs. This does not require advance notification to be provided to a journalist of a communications data request. In many cases such notification would alert the subject under investigation to the ongoing investigation, to the detriment of the case. In addition no other applications for communications data require prior notification, nor do applications made to a court by the police for comparable data, for example banking records, or for other police powers such as applications for covert surveillance. Further information on this issue is provided in: • Chapter 9 of the draft Interception of Communications Code of Practice • Chapter 6 of the draft Communications Data Code of Practice • Chapter 8 of the draft Equipment Interference Code of Practice • Chapter 9 of the draft Bulk Acquisition Code of Practice • Chapters 4 and 7 of the draft security and intelligence agencies' retention and use of Bulk Personal Datasets Code of Practice
49	The Committee recommends that if Clause 61 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.	PACE and the Terrorism Act 2000 provide appropriate mechanisms for law enforcement bodies to obtain journalistic material from journalists themselves. RIPA, and in future the Investigatory Powers Bill, is the appropriate mechanism for acquisition of communications data from CSPs. The Bill makes it clear that requests for communications data must be made through the powers outlined in the Bill. This does not require advance notification to be provided to a journalist of a communications data request. In many cases such notification would alert the subject under investigation to the ongoing investigation, to the detriment of the case. In addition no other

		applications for communications data require prior notification, nor do applications made to a court by the police for comparable data, for example banking records, or for other police powers such as applications for covert surveillance. In addition, the Interception of Communications Commissioner conducted a detailed investigation into this issue and in his report published in 2015 he clearly rejected the claim that public authorities have utilised RIPA "to avoid the use of PACE".
50	The Home Office should review Clause 61 to ensure that it meets the requirements of Article 10 ECHR.	The previous Clause 61, now Clause 68, which has been amended to remove the exemption for the security and intelligence agencies, remains Article 10 compliant. In December 2015, the IPT delivered its judgment in the complaint brought by News Group Newspapers Ltd against the Metropolitan Police Service about access to communications data in Operation Alice. The IPT found that the then legal regime was deficient as it did not contain effective safeguards to protect Article 10 (freedom of expression) rights "in a case in which the authorisations had the purpose of obtaining disclosure of the identity of a journalist's source". It states that "Our decision is confined to such a case". It also notes that the March 2015 amended Code of Practice, which requires law enforcement to obtain independent authorisation through the use of PACE in such cases, "cures this incompatibility" and that the Bill will require judicial approval of requests for communications data to determine the identity of a journalist's source. The use of PACE for such requests has always been regarded as a stop gap until the provisions in Clause 61, now Clause 68 can be brought into force. The recognition by the Courts of the steps that the Government has taken, and is taking, to rectify the gap in our law is welcome.
51	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, a recommendation	The Government is committed to creating a new oversight body which simplifies the current oversight landscape, provides a more visible single body, and one with greater powers and resources. This will be achieved without the need for a new

	endorsed by the knowledgeable and experienced Interception of Communications Commissioner's Office. The benefits of having a senior independent judicial figure in the Investigatory Powers Commissioner would not be lost by putting the IPC at the head of a Commission. 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.	statutory body to be created. Creating an Investigatory Powers Commission as a statutory body would significantly increase its running costs, as it would have increased reporting and corporate / administrative responsibilities and so require extra staff and the appointment of Non-Executive Directors. The Government anticipates that it would cost an extra £0.5m p/a. However, it would have no additional powers and would not, in practice, be any more independent.
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.	The Government has amended the Bill at Clause 202 to make it explicit that Judicial Commissioners have the power to initiate investigations.
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 Lord Chief Justice will also be able to assess the impact of appointments on the work of the High Court and the Court of Appeal, which must not be impaired by the creation of the Judicial Commissioners. The Judicial Appointments Commission must also be consulted to ensure that the appointments procedure is fair and transparent.	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. The Government considers that the LCJ and his or her devolved equivalents should be consulted in the appointment process. A requirement for the Prime Minister to consult the Lord Chief Justice has been provided for in Clause 194 of the revised Bill. The Government will consult with the Judicial Appointments Commission on these provisions.

54	The Government should reconsider both the length of terms of appointment and whether they should be renewable. Terms need to be long enough for Judicial Commissioners to build expertise but should not be so long that they have a negative impact on a serving judge's career. 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 will carefully review the appointment provisions with the stakeholders that the Committee have suggested.
55	Maintaining public confidence in the Judicial Commissioners may occasionally require that a Commissioner is removed from the role because he or she has behaved in a manner incompatible with what is, in effect, high judicial office. Public confidence also requires that the power to remove from office does not damage the public perception of the Judicial Commissioners' independence from the executive or the freedom of the Judicial Commissioners to make decisions that may be unpopular with the Government. 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.	The Government has amended Clause 195 to make clear that Judicial Commissioners are subject to the same dismissal and suspension procedures as those applicable to serving senior judges.
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	The Government will consider whether there is a role for Parliament, e.g. the Intelligence and Security Committee (ISC), to play in determining, or reporting on the adequacy of, the

	Government may want to consider a role for Parliament in determining the budget.	budget of the IPC.
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. This approach is cumbersome and unnecessary given there are no concerns over the way the current oversight bodies have used their powers of error-reporting. We recommend that the Investigatory Powers Commissioner exercise the error-reporting power alone, without reference to the Investigatory Powers Tribunal.	The Government has amended Clause 198 of the Bill accordingly. This will now allow the Investigatory Powers Commissioner to inform an individual directly if they have been subject to a serious error.
58	We recommend that the Government should review the error-reporting threshold in light of the points made by witnesses.	The Government will review the threshold for error reporting. However it is vital that national security and the wider public interest is not compromised as a result of individuals being informed that they have been affected by an error which is inconsequential or has had a very minimal or imperceptible impact upon their lives.
59	It should be made clear in the duties laid on the Judicial Commissioners in sub-clauses 169(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.	The Government is committed to ensuring the independence and effectiveness of the Judicial Commissioners. The Government has amended Clauses 199 to make it clearer that the Judicial Commissioners will not be unduly constrained in performing their duties. As the current oversight commissioners recognise, and the Judicial Commissioners will undoubtedly accept, it is important that in carrying out their work they do so in a way that does not jeopardise national security or the effectiveness of operations.
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	Clause 203 of the revised Bill now provides a route for CSPs and public authorities to refer complaints and concerns, or requests for clarification, directly to the Judicial Commissioners.

	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.	Furthermore, there is a separate route for CSPs to refer notices to the Secretary of State who must consult both the IPC and the TAB as part of his or her deliberations.
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 Act. The Investigatory Powers Commissioner should then have discretion whether to exercise his or her power to initiate an inquiry into the allegations. We recognise that there may be wider concerns over the role of whistle-blowers in this area. This is a matter which requires consultation and therefore this is not the appropriate Bill in which those wider concerns should be taken forward.	Clause 203 has been amended to make clear that the public authorities who can exercise the powers contained in the Bill can discuss any concerns with the IPC. It will be for the IPC to determine what further action may be appropriate.
62	The law in this area is complex and developing. Judicial Commissioners will have to make decisions without the benefit of adversarial argument. 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.	It is the Government's clear intention that the IPC will have an in-house legal adviser. The Commissioner will also have budget provision for Counsel to be consulted and appointed when the Commissioner feels it is necessary. The Impact Assessments published alongside the draft Bill make it clear that this is being budgeted for.
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.	Clause 202 of the Bill has been amended explicitly to provide Judicial Commissioners with access to all relevant technical systems where necessary for them to provide effective oversight.
64	We recommend that the Judicial Commissioners should have access to technical expertise to assist them in fulfilling their authorisation and oversight functions.	The Government agrees with the Committee on the importance of access to technical expertise. It is our clear intention that not only will the Judicial Commissioners have a range of specialist inspectors to assist them, they will also have budgetary provision

		to consult additional technical experts and advisers when they feel it is necessary and appropriate. The Impact Assessments published alongside the draft Bill make it clear that this is being budgeted for.
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.	The Government has revised Clause 172(3) now Clause 199 to make it clear that the Judicial Commissioners can communicate with the IPT without consulting the Secretary of State.
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.	Courts and tribunals generally, including the IPT, do not have the power to carry out investigations into alleged unlawful conduct on their own initiative. It is a fundamental principle of our justice system that courts and tribunals will not consider and determine legal issues without individual parties having first issued a claim or initiated proceedings. If Judicial Commissioners were to notify the IPT that they had identified unlawful conduct, there would be no meaningful action that the IPT could take. In order for the IPT to be capable of assuming jurisdiction, it would be necessary to extend the IPT's jurisdiction and empower the Judicial Commissioners to bring claims or complaints against public authorities in the IPT, making the Commissioners party to proceedings. The Government does not consider that it would be appropriate to extend the IPT's jurisdiction in this way. However, if the Judicial Commissioners had concerns about unlawful conduct then they would be able to make a direct report to the Prime Minister and the Government would ensure that remedial action was taken as a matter of urgency. If the IPC considered that their concerns were not being adequately responded to it would be open to them to bring an action for Judicial Review in respect of the Government's failure to act.
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	The Government had envisaged that this information would be included in the Commissioner's annual report, and has amended Clause 201 to make clear that he or she must report on these

	and parliamentary scrutiny of the results of the powers can take place.	topics.
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.	This will be included in the Memorandum of Understanding establishing the IPC's operation and ways of working.
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 agrees that the Judicial Commissioners should have this function. It is now clear in the draft Codes of Practice, specifically: • Chapter 13 of the Interception of Communications Code of Practice • Chapter 22 of the Communications Data Code of Practice • Chapter 10 of the Equipment Interference Code of Practice • Chapter 12 of the Bulk Acquisition Code of Practice • Chapters 4 and 6 of the security and intelligence agencies' retention and use of Bulk Personal Datasets Code of Practice
70	We recommend that the right of appeal from the Investigatory Powers Tribunal in Clause 181 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.	As the Committee recognised, the test for any appeal from the IPT is consistent with the appeal route found elsewhere. The Bill provides in Clause 208 for appeals on any point of law, giving the IPT or appellate court significant discretion. They are able to give permission to appeal not only where there is an 'important point of principle', but also where they conclude there is another 'compelling reason' for granting leave. The Government believes this should provide enough flexibility for the court to ensure that all points of law which merit an appeal (suitably significant) are able to proceed.
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.	The Government has amended the Bill to provide for this in the new Clause 208.
72	We recommend the appeal route for Scotland and Northern Ireland should appear on the face of the Bill. It is	The Government has amended Clause 208 of the Bill to make the appeal route for Scotland and Northern Ireland clear.

	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.	
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 believes that the three recent scrutiny reports have provided a thorough review of the IPT's powers and procedures. The IPT is also subject to Triennial Reviews in line with Cabinet Office requirements.
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.	Rule 9 of the Tribunal Rules (SI 2000/2665) makes provision for how the IPT should hear a complaint. It gives the IPT discretion on whether or not to hold an oral hearing. In the vast majority of cases, the IPT will not hold an oral hearing, reflecting that most cases can be dealt with on the papers.
75	The Investigatory Powers Tribunal should be able to make a declaration of incompatibility under the Human Rights Act.	There is a domestic route of appeal from the IPT to the Court of Appeal which, as a senior court, already has the power to make a declaration of incompatibility.
76	We have heard evidence that there is potential for the further simplification of the oversight landscape. This would improve transparency, reduce overlaps and ensure consistency of decision-making which would all contribute to ensuring oversight of the powers contained in the Bill comply with international law standards. We recommend that the Home Office should carry out a review to identify areas in which further simplification of oversight could occur.	The Government believes that the oversight landscape has already been sufficiently reviewed by the three reports in this area. Similarly, regular (triennial) reviews are already undertaken of all Government bodies, to ensure that they are still performing unique and necessary functions. The Government does not consider that it would be appropriate to remove the oversight function performed by the Information Commissioner's Office (ICO) which, would undermine data security protections. However, the Government has made clear in Chapter 21 of the draft Communications Data Code of Practice that where a CSP is required to report an error to the IPC, it should not also be obliged to report that error to the ICO.
77	We call on the Government to outline its plans for the establishment of the Privacy and Civil Liberties Board.	As the Committee notes, the Government legislated, through the Counter-Terrorism and Security Act 2015, to provide the Secretary of State with a power to establish a Privacy and Civil Liberties Board in regulations, to support the Independent Reviewer of Terrorism Legislation, David Anderson QC. Having been informed by a public consultation and David Anderson's views on the Board's creation, the Government has since

		decided that in the interests of supporting the Reviewer to discharge his statutory functions in the most effective manner, it would instead provide him with assistants in the form that he recommended in his July 2014 Annual Report. The Government is currently working closely with David Anderson to ensure that the individuals he has identified to assist him in his role are suitably cleared to access sensitive material, enabling them to provide the specialist support required.
78	The Committee recommends that the Government keeps the issue of the inadmissibility of intercept material as evidence under review and takes note of the significant perceived benefits of using such material as evidence.	Eight reviews have been undertaken of the issue since 1993. The most recent review, overseen and endorsed by a cross-Party group of Privy Counsellors, published its findings in 2014. The 2014 review went further than any previous review by considering the costs and benefits of an intercept as evidence regime. The Government continues to keep the issue under review.
79	The Committee recommends that the Government considers the Chief Coroner's proposals and engages further with him to come to a satisfactory agreement about which judges can be included in the list in Schedule 3.	The Government will consider the Chief Coroner's proposals and discuss them with him further to determine how best to address his concerns.
80	We agree with this conclusion of the DPRRC on the power in Clause 201 (2) to make consequential provision and recommend the deletion of powers to amend future enactments.	It is necessary to retain the power to amend future enactments, although it is anticipated that there will be very limited circumstances in which the power will be exercised in this way. Legislation going through Parliament at the same time as the Bill (for example the Policing and Crime Bill and the Northern Ireland (Stormont Agreement and Implementation Plan) Bill) may require to be amended in consequence of the Investigatory Powers Bill, and it is impossible to anticipate how such Bills may be amended in Parliament or which Bill may receive Royal Assent first. The power is, however, limited by the fact that any amendment to legislation must be in consequence of this Act, so it is not an unrestricted power.
81	The Committee agrees with the DPRRC that the negative procedure for these powers is inappropriate and recommend that any modifications to primary legislation be subject to the super-affirmative resolution procedure	It remains the Government's position that it is not possible to define the circumstances in which a non-textual modification of legislation should attract the affirmative rather than the negative procedure, and that to attempt to do so would lead to legal

		uncertainty. The Government has committed that any significant non-textual amendments will be made by way of legislation subject to the affirmative procedure.
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.	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.
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 Bill provides for warrants to be sought in the interests of the economic-well-being of the United Kingdom so far as also relevant to national security. This replicates the current statutory purpose for which interception warrants may be authorised and which is contained in RIPA, replicates language in the e-privacy directive, and is consistent with the statutory functions of GCHQ and the Secret Intelligence Service. 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. The UK's National Security Strategy and Strategic Defence and Security Review 2015 highlighted economic security as a separate issue that is closely related to national security, and reflected the long-term shifts in the balance of global economic and military power and the emergence of more powerful non-state actors. It would not be appropriate to hinder the ability of the security and intelligence agencies to undertake investigative activity into issues where the primary risk is to economic security, which has an effect on national security. Such issues might include instability in parts of the world or unexpected crises which may undermine British markets and other economic interests, or create difficulties in the

		continued supply of a commodity on which our economic security depended. Such issues would also have a national security impact but their primary effect would be on economic well-being.
84	The Codes of Practice will provide essential further details on how the powers in the draft Bill will be used in practice. We recommend that all of them should be published when the Bill itself is introduced to allow both Houses to conduct full scrutiny of their contents.	To assist Parliament in scrutinising the Bill, the Government has published drafts of six statutory Codes of Practice that will be made under the Bill. These codes include details of implementation and technical application. The Government invites comments on the draft Codes of Practice. The new Codes of Practice will be published for formal consultation following Royal Assent of the Bill. They will require approval by Parliament and will have statutory force.
85	We urge the Investigatory Powers Commissioner to scrutinise the automated analysis of bulk datasets conducted by the security and intelligence agencies to ensure that they are conducted appropriately and proportionately and with regard to privacy and data protection requirements.	The Government is committed to ensuring that the IPC has the powers, resources and access to specialist knowledge to effectively and visibly oversee the security and intelligence agencies and the use of investigatory powers in the Bill. The Government cannot dictate how the independent IPC must undertake their scrutiny. We expect, and would welcome, though, the IPC scrutinising the automated analysis of bulk datasets. The Bill has been amended to make clear that the IPC has access to software and systems. The Government agrees that this would be part of the IPC's role.
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.	The Government is committed to post-legislative scrutiny of the Bill. Clause 222 requires the Secretary of State to prepare a report on the operation of the Investigatory Powers Act within six years of the Bill being enacted. This is in anticipation of a Select Committee of either House of Parliament (whether acting alone or jointly) undertaking a review of the powers in the Bill within five years and six months of Royal Assent.

Government response to the recommendations of the Intelligence and Security Committee of Parliament on the draft Investigatory Powers Bill

Recommendation		Government response
A	The new legislation should include a single additional Part that addresses privacy safeguards and clearly sets out universal privacy protections which apply across the full range of investigatory powers.	The Investigatory Powers Bill will protect both the privacy and the security of people in the UK. Part 1 of the Bill provides an overview of the privacy safeguards contained throughout the Bill. The revised Bill and the accompanying documents make clear the strong privacy safeguards that apply to all of the powers in the Bill. The revised Bill and the accompanying Codes of Practice make clear: • The purposes for which each of the powers in the Bill may be used • The requirement that each exercise of the power must be necessary and proportionate • The overarching human rights obligations which constrain the use of the powers in the Bill • Whether each of the powers in the Bill must be used in a targeted way or provides for the acquisition of data in bulk • The authorisation procedures that must be followed, including the review, inspection and oversight regime • Specific safeguards for certain sensitive professions or categories of information • Additional safeguards and obligations in respect of retention, storage and destruction of data • Safeguards relating to sharing of material obtained under the powers in the Bill
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.	The Government has strengthened the safeguards for sensitive professions across the Bill. These safeguards provide the required protections for the different levels of intrusiveness of each of the powers catered for in the Bill. • The Government has amended clause 68 of the draft Bill to remove the exemption which allowed the intelligence agencies

		to obtain communications data to identify journalistic sources without first gaining judicial approval • Clauses 25 and 100 of the revised Bill contain additional safeguards for information subject to legal privilege that has been acquired by targeted interception or equipment interference • Clauses 135 and 171 now set out on the face of the Bill the safeguards that apply before content that contains legally privileged material can be selected for examination • The provision in Schedule 7 of the Bill, making clear that any Code of Practice in relation to communications data must contain particular provision in relation to journalistic information and members of professions who hold confidential material or material that is subject to legal privilege, has been extended to apply to Codes of Practice in relation to all the powers under the Bill. • Further information is provided in: o Chapter 9 of the draft Interception of Communications Code of Practice o Chapter 6 of the draft Communications Data Code of Practice o Chapter 8 of the draft Equipment Interference Code of Practice o Chapter 9 of the draft Bulk Acquisition Code of Practice o Chapters 4 and 7 of the draft Code of Practice on the Security and Intelligence Agencies' retention and use of Bulk Personal Datasets Most Bulk Personal Datasets (BPD) do not include details which would identify someone as a member of a sensitive profession, and do not contain confidential information relating to sensitive professions. However, in the unlikely event that the security and intelligence agencies believed that a BPD contained a significant

		amount of confidential information relating to a member, or members, of a sensitive profession, the draft Code of Practice on the security and intelligence agencies' retention and use of Bulk Personal Datasets makes clear that the agency must seek a specific BPD warrant. Any subsequent use of records known to be sensitive is also governed by the strict procedures set out in the draft Code of Practice on the security and intelligence agencies' retention and use of Bulk Personal Datasets. These include prior consideration of applying particular restrictions to access to that data, including sensitive data-fields not being acquired, sensitive fields being acquired but suppressed or deleted, or additional justification required to access and examine sensitive data-fields.
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 the same safeguards.	The revised Bill updates the legislative framework that governs the powers available to obtain communications, data and other information through equipment interference. The oversight and safeguards applied to equipment interference for the purpose of acquiring communications, data and information have been carefully tailored in the revised Bill for these specific purposes. The Investigatory Powers Bill brings together existing powers available to the security and intelligence agencies to obtain communications and communications data. This reflects the shared recommendations of the reports published in 2015 by the Intelligence and Security Committee, the panel convened by the Royal United Services Institute, and David Anderson QC, the Independent Reviewer of Terrorism Legislation. The Investigatory Powers Bill does not seek to legislate for all of the powers available to the security and intelligence agencies or for the existence of those agencies. Seeking to do so would stray beyond the expectations for future legislation set by Parliament when it passed the Data Retention and Investigatory Powers Act 2014 and would add significant complexity to the Bill.
D	The Committee acknowledges that the Agencies need the	The Government welcomes the Committee's acknowledgment

	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.	that equipment interference powers are necessary. Further evidence on the operational requirement for bulk equipment interference warrants has been provided to the Intelligence and Security Committee in advance of publication of the revised Bill. The Government has published an operational case for bulk powers, including bulk EI, which provides further information about how bulk powers are used and why they are essential to the security and intelligence agencies. Chapters 4 and 5 of the draft Equipment Interference Code of Practice provides greater clarity on the differences between targeted and bulk warrants and the circumstances when it is appropriate to use each. A bulk EI warrant will be more appropriate for operations where additional access controls are required at the examination stage because the Secretary of State is not able to fully assess at the time of issuing the warrant the necessity and proportionality of each interference.
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.	Chapter 2 of the draft Equipment Interference Code of Practice provides greater clarity on where it would not be operationally feasible for the security and intelligence agencies to seek a targeted EI warrant when conducting EI operations overseas and clarifies the circumstances in which the agencies would be expected to seek an EI warrant. An EI warrant will be mandatory wherever an offence under the Computer Misuse Act 1990 would otherwise be committed, as well as where there is any British Islands connection. Where an EI operation falls outside the scope of the Bill, which would only be when all of the operation takes place overseas and there is no British Islands link, the activity will nevertheless continue to be authorised by a Secretary of State under the Intelligence Services Act 1994, and will be overseen by the new IPC.
F	The Committee considers that the acquisition, retention	Class BPD warrants provide an appropriate means of authorising

	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 retention of datasets that are similar in nature and in the level of intrusiveness. This would, for example, allow the Secretary of State to authorise a class of dataset relating to travel where these conditions were met. 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 draft Code of Practice provides clear guidance on the factors that the security and intelligence agencies will need to consider in determining whether it is appropriate to use a class warrant or whether it may be more appropriate to apply for a specific BPD warrant. These factors include whether the nature or the provenance of the dataset raises particularly novel or contentious issues; whether it contains a significant component of intrusive data; and whether it contains a significant component of confidential information relating to members of sensitive professions. The draft Code of Practice published alongside the revised Bill also sets out detailed requirements about how the security and intelligence agencies must keep under review the ongoing necessity of holding individual datasets, including those retained under a class warrant. In considering whether a class warrant should be renewed, the Secretary of State will consider whether continued retention of datasets held under the warrant remains necessary and proportionate. This decision will be subject to review by a Judicial Commissioner.
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	The Bill now specifies time limits for initial examination of the datasets. These are: as soon as reasonably practicable and in any event within a maximum of three months to undertake an initial examination of a UK-originated dataset and apply for a warrant; and as soon as reasonably practicable and in any event within a maximum of six months to undertake an initial examination of a foreign-originated dataset and apply for 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.	warrant.
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.	A targeted communications data authorisation must be approved by a designated senior officer within the requesting department. A bulk acquisition warrant or bulk interception warrant is subject to the double-lock at the point of authorisation, so that warrants for the acquisition of communications data in bulk that have been authorised by the Secretary of State must also be approved by a Judicial Commissioner before coming into force. Warrants for the acquisition of communications data in bulk will also specify the detailed Operational Purposes for which data obtained under the warrant may be examined. Analysts in the security and intelligence agencies may only select bulk CD for examination if it is necessary and proportionate to do so for one or more of the Operational Purposes specified on the warrant. This is also subject to retrospective oversight by Judicial Commissioners. These safeguards go beyond the existing statutory safeguards for examination of related communications data acquired under bulk interception warrants issued under the Regulation of Investigatory Powers Act 2000. The adequacy of these safeguards was upheld by the Investigatory Powers Tribunal in a 2014 judgment. These safeguards also go beyond those set out in the Handling Arrangements for bulk CD acquired under s.94 of the Telecommunications Act 1984 (that were published in November 2015). The application of the ‘double lock’ for the authorisation of

		warrants for the acquisition of bulk CD, combined with the robust additional safeguards in the Bill restricting the examination of that data, provide an effective, human rights compliant regime. The application of 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.
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.	Chapter 7 of the draft Code of Practice on Communications Data provides further information and clarity on how and for what purposes public authorities may obtain Internet Connection Records (ICRs). There may be circumstances where it is more appropriate for public authorities to utilise the alternative lawful powers available to them, such as interception or equipment interference warrants, to obtain information which is similar to, or includes, ICRs. The use of these powers will be subject to higher levels of authorisation, requiring a warrant to be issued by the Secretary of State and approved by a Judicial Commissioner. Before using such powers the relevant authority must consider whether a less intrusive means of collecting such data is appropriate.
J	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 well-being… 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	The Bill provides for warrants to be sought in the interests of the economic-well-being of the United Kingdom so far as also is relevant to national security. This replicates the current statutory purpose for which interception warrants may be authorised which is contained in RIPA, replicates language in the e-privacy directive, and is consistent with the statutory functions of GCHQ and the Secret Intelligence Service. 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. The UK's National Security Strategy and Strategic Defence and Security Review 2015 highlighted economic security as a

	category.	separate issue that is closely related to national security, and reflected the long-term shifts in the balance of global economic and military power and the emergence of more powerful non-state actors. It would not be appropriate to hinder the ability of the security and intelligence agencies to undertake investigative activity into issues where the primary risk is to economic security, which has an effect on national security. Such issues might include instability in parts of the world or unexpected crises which may undermine British markets and other economic interests, or create difficulties in the continued supply of a commodity on which our economic security depended. Such issues would also have a national security impact but their primary effect would be on economic well-being.
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	As the ISC has recognised, it would be contrary to the interests of national security to publish full details of the Operational Purposes. Nevertheless, a list of draft operational purposes has been provided to the ISC in advance of publication of the revised Bill. The list is indicative in that it provides a list of Operational Purposes that might apply in light of the current threat picture. It provides the Committee with a better understanding of the Operational Purposes that the Secretary of State and Judicial Commissioner would be asked to approve when authorising a bulk warrant, to specify the circumstances in which material can be selected for examination. Further information on Operational Purposes and how this safeguard will work in practice has been provided in the relevant draft Codes of Practice and the operational case for bulk powers, which have been published alongside the revised Bill. The operational case for bulk powers also provides examples of Operational Purposes.

	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.	
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 process for authorising the two categories of warrant is essentially the same; in drafting the Bill it was intended that this would be the case. This reflects the recommendation from David Anderson that the process for authorising a targeted interception warrant was clear and well understood, and the process for authorising the examination of the communications of a person in the UK when they had been collected in bulk should therefore mirror it. In drafting the Bill, the Government considered whether a single warrant could cover both eventualities. However, they authorise different activity - one allows for communications in respect of a person to be obtained, and the other for the examination of communications in relation to a person that have already been obtained under a bulk interception warrant. They could therefore not be brought together without adding significant complexity to the Bill.
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.	This provision is intended to allow for circumstances when an overseas target arrives in the UK for a short-term, unexpected visit. This replicates an equivalent provision under the Regulation of Investigatory Powers Act 2000. This provision is necessary, as the security and intelligence agencies may suddenly become aware that a suspect is in the UK or may have very limited notice of a suspect's travel to the UK; in such circumstances, the requirement to stop selecting the suspect's communications until a warrant has been obtained may lead to a considerable intelligence gap. Additional safeguards have been included in the revised Bill. Clause 134 in the revised Bill now requires the agencies to notify

		a Secretary of State where a person has entered the UK for a short period. The Judicial Commissioner will also provide retrospective oversight as part of their inspection regime. Chapter 6 of the draft Interception of Communications Code of Practice provides more information on how these provisions will work in practice.
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.	Clauses 22, 98 and 158 of the revised Bill now provide that urgent warrants must be approved by a Judicial Commissioner within three working days of authorisation by a Secretary of State, though they will continue to last for five working days before they must be renewed (if that is considered appropriate). The draft Codes of Practice for Interception and Equipment Interference include a flow chart to illustrate the urgency procedure. The Government believes that this approach will provide sufficient time for the Judicial Commissioner to review the Secretary of State's decision to issue an urgent warrant. The Bill makes clear that the Judicial Commissioner can refuse to approve the issuance of an urgent warrant and in such circumstances the activity must cease and the Judicial Commissioner can direct what happens to any material collected.
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.	Clause 203 of the revised Bill provides an information gateway which will allow anyone with concerns about the use of investigatory powers to raise those with the Investigatory Powers Commissioner. If the Commissioner is made aware of an instance where there has been a serious error in relation to the use of investigatory powers, then he or she may inform the individual(s) affected of this and their right to bring a claim or a complaint in the Investigatory Powers Tribunal (IPT).
vii	In the Committee's Report on *Privacy and Security*, we recommended that 'thematic' Targeted Interception	The Independent Reviewer of Terrorism Legislation, David Anderson QC, considered the question of whether interception

	warrants be used sparingly and subject to greater safeguards; unfortunately this has not been reflected in the draft 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	warrants should be authorised for a period of less than six months and determined that they should not. This reflected the view of the then Interception of Communications Commissioner. Warrants authorised for less than six months require renewal applications to be drafted and submitted before the value of the warrant has been properly established. This could make it difficult for the Secretary of State to assess the necessity and proportionality of continued interception under the warrant. In the Interception of Communications Commissioner's March 2015 annual report, Sir Anthony May also agreed that thematic warrants comply with the law '*so long as they sufficiently name of describe the combination or association of persons'*. The Investigatory Powers Tribunal (IPT) has just considered the issue in the context of GCHQ's use of computer network exploitation (or 'equipment interference' in the context of the Bill) and found it lawful (in the case of Privacy International and Greennet & Others (IPT 14/85/CH, IPT 14/120-126/CH) on 12 February 2016). Again the IPT made clear that the key point was that the description of the interference needed to be sufficiently foreseeable for the Secretary of State to be able to effectively consider necessity and proportionality. The draft Codes of Practice for Interception and Equipment Interference set out these requirements. The Investigatory Powers Bill preserves this essential ability for major modifications to be made, but only where they are necessary and proportionate and within the boundaries of the original Secretary of State / Judicial Commissioner approved warrant. The Government has provided for greater safeguards in the draft Bill to be applied to the use of thematic targeted warrants such that the Secretary of State must be notified of the addition of new subjects (major modifications) to a thematic warrant. The Investigatory Powers Commissioner also provides retrospective oversight of all modifications.
viii	The Committee recommended previously that there	The national security exemption from the requirement for the

	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.	designated senior officer to be independent from the investigation or operation applies only in exceptional cases and particular cases. It is not a blanket exemption. Chapter 4 of the draft Code of Practice on Communications Data provides further detailed information about the circumstances in which the exemptions apply, and requires a public authority which plans to use an exemption, other than in an immediate threat to life situation, to notify the IPC in advance. The IPC will oversee the use of the exemption and may publish details on its use in his or her reports.
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 189 in the revised Bill makes it explicit that the security and intelligence agencies must apply for a new BPD warrant as soon as reasonably practicable and in any event within a maximum of three months if they wish to continue to retain or examine any of the material obtained from a BPD warrant that has not been renewed, or is cancelled.
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.	Clauses 217 and 218 of the revised Bill make clear the obligations that can be imposed on Communication Service Providers (CSPs) with regard to encryption. This explains what is meant by 'removing electronic protection' and makes clear that CSPs can only be required to remove protection that they themselves have applied, or that has been applied on their behalf; or that they have already removed for their own business purposes. Clause 218 also sets out the considerations that must be taken into account when determining whether it is necessary and proportionate to issue a technical capability notice.

		The relevant draft Codes of Practice provide detailed information on technical capability notices and the obligations that can be imposed on CSPs.
xi	A key issue arising from the Committee's *Report on the intelligence relating to the murder of Fusilier Lee Rigby* was the difficulties the Agencies face in accessing communications content from CSPs based overseas. Whilst the draft Bill asserts extraterritoriality, the Agencies have told the Committee that additional measures are needed, and that the CSPs themselves are pressing for an international framework to be developed. Although some initial discussions have taken place, the Committee is disappointed that the Government has not done more to make progress on this crucial issue, and we reiterate our earlier recommendation that this matter must be resolved urgently; without proper progress, the Agencies' hands are tied.	As the Prime Minister and Home Secretary have previously stated, the Government is engaging in preliminary discussions with international partners on how a new international framework for access to data across jurisdictions might operate in principle. This would be based on strong, human rights-compliant domestic regulatory oversight.
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.	Whilst the routine exchange of intelligence with international partners sits outside the scope of the IP Bill, the Bill sets out the safeguards that apply when intercept material is shared. Clause 47 in the revised Bill makes it clear that the Secretary of State must be satisfied that satisfactory and equivalent handling arrangements are in place before sharing UK intercept material. Chapter 9 of the draft Interception of Communications Code of Practice also provides more information on the safeguards associated with sharing intercept material with international partners. In addition, Clause 7 of the revised Bill makes clear that an overseas authority cannot be tasked to undertake interception on behalf of a UK agency, in respect of an individual in the UK, without a targeted interception warrant or a targeted examination warrant being in place. The draft Code of Practice on Interception

		of Communications describes how those agencies that undertake bulk interception may request unanalysed intercepted content or secondary data from another government, where a relevant interception warrant has already been issued, or where it does not amount to a deliberate circumvention of the Act. The draft Code of Practice also makes clear that any information obtained by these means is subject to the same internal rules and safeguards that would apply to information intercepted by the Agency under the Bill.
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 UK is required to implement the EU Mutual Legal Assistance Convention in domestic law. The revised Bill also makes provision for any future international treaties on mutual assistance requests for interception. Locating the provisions with the other interception clauses is clearer for the reader and avoids unnecessary duplication of provisions. Clause 45 provides for certain mutual assistance requests and requests from overseas partners in accordance with other relevant international agreements to be given effect to by telecommunications and postal operators in the UK without the need for the Secretary of State to issue a warrant. Further conditions will be specified in secondary legislation and where appropriate, the secondary legislation will stipulate that the subject of a request must be outside the UK.

Government response to the recommendations of the House of Commons Science and Technology Committee on the draft Investigatory Powers Bill: Technology Issues

	Recommendation	Government response
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)	Part 4 of the revised 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 on Communications Data provides information about what internet connection records (ICRs) are and the practical steps which we take to consult a Communications Service Provider (CSP) before issuing a retention notice. CSPs configure their networks differently, which may affect exactly what a CSP may be required to retain in order to meet the obligations. It is important that nothing in the legislation prevents a CSP from meeting any obligation in a way that is feasible. Chapter 16 of the draft Code of Practice on Communications Data provides details on the security considerations that apply in relation to the retention of data, making clear that the security in place needs to be consistent with the sensitivity of the data being protected. The Government has been clear that it pays all reasonable costs in relation to data retention and further guidance on this is included in Chapter 19 of the draft Code of Practice on Communications Data.
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	The Government recognises the importance of clarity around the obligations placed on CSPs. The definition of data in Clause 225 of the Bill has been revised to make it as clear as possible. Chapter 2 of the draft Code of Practice on Communications Data provides further examples of key definitions, to assist with interpretation.

	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. (Paragraph 31)	Each draft Code of Practice issued alongside the Bill (with the exclusion of the Code of Practice on Bulk Personal Datasets where it is not relevant) contains a chapter setting out the obligations that can be imposed on a CSP and detailed information about their compliance.
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 217 of the Bill has been amended to make clear the obligations that can be imposed on CSPs with regard to encryption. This explains what is meant by 'removing electronic protection' and makes clear that CSPs can only be required to remove protection that they themselves have applied, or that has been applied on their behalf. Other provisions in the revised Bill at Clause 218 set out the factors that must be taken into account when considering whether it is necessary and proportionate to issue a technical capability notice.
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 relevant draft Codes of Practice provide detailed information on technical capability notices, the obligations that can be imposed on CSPs and more detail on the factors that will be taken into account in determining whether it is necessary and proportionate to impose such an obligation. The extent to which encryption has been applied, and the nature of that encryption will be part of the necessity and proportionality consideration.
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	The draft Equipment Interference Code of Practice, which has been published alongside the Bill, explains the consultation process that should take place whenever an agency seeks assistance from a CSP with equipment interference. Any potential impact on business will be considered carefully as part of the necessity and proportionality consideration applied to every warrant. The Government recognises the concerns that clients may

	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)	question whether equipment interference has taken place. The double-lock authorisation process provided for in the Bill ensures that equipment interference will only be permitted when necessary and proportionate. Clauses 91, 92, 93 and 96 ensure that a warrant may only be issued if the issuing authority believes that what is being sought to be achieved could not reasonably be achieved by other means.
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)	Clause 196 of the revised Bill provides for the Investigatory Powers Commissioner to have oversight of all of the powers in the Bill, including equipment interference. Clause 201 sets out the Commissioner's duties with regard to reporting. It will be open to the Commissioner to report on any aspects of the powers that he or she considers appropriate. Clause 201 requires the Commissioner's annual report to include statistics on the use of investigatory powers including equipment interference (including the number of warrants or authorisations issued, given, considered or approved).
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 Home Office continues to engage with CSPs to understand the likely cost of the ICR provisions in the Bill. The steps required by each CSP to implement those provisions may vary, meaning that it is unlikely that the Government will be able to publish final costs during the passage of the Bill. However, the Government will work with industry over the coming months to refine cost estimates. The Government has previously made available to Parliament the capital costs associated with data retention obligations, and expects to do so in future.
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	It would not be appropriate to commit future Governments to pay the full cost of compliance, as it would limit their discretion on this issue. However, in practice the Government has a long-standing position of reimbursing 100% of the costs associated with data retention. There are no current plans to change that policy. The Joint Committee also recommended that 100% cost recovery

	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)	should not be on the face of the revised Bill. Any retention notice must specify the level, or levels of contribution which the Secretary of State determines should apply in relation to that notice. Clause 80 of the Bill provides a clear route for CSPs to appeal to the Secretary of State should a company consider that the obligation placed on them would incur unreasonable costs. In considering their appeal, the Secretary of State must take advice from the Technical Advisory Board (TAB) on costs and technical feasibility and from the Investigatory Powers Commissioner (IPC) on proportionality.
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 has published six draft Codes of Practice alongside the Bill: 1. Interception of Communications 2. Communications Data 3. Bulk Acquisition 4. Equipment Interference 5. National Security Notices 6. Security and intelligence agencies' use of Bulk Personal Datasets They contain information on all the issues which the Committee has suggested.
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	The Government agrees with the importance of regular review of Codes of Practice. Schedule 7, paragraph 5 provides for the Secretary of State to revise the Codes. The Government will ensure the terms of reference for the TAB provide for them to play a role in ensuring the Codes are up-to-date.

	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)	
11	From the evidence we have received, it is clear that the Home Office has engaged with communications businesses and the wider internet community. This should remain a central strand of the Government's strategy to ensure effective implementation and for seeking to allay concerns over current uncertainties and confusion arising from the way some terms are defined in the draft Bill. (We have separately recommended clarifying definitions and strengthening consultation processes through the Technical Advisory Board once the Bill is enacted.) (Paragraph 75)	The Government will continue to consult broadly on the provisions in the Bill and its implementation.
12	Internet businesses and their users require assurances that investigatory powers will be imposed proportionately, and that the judgement as to what is proportionate should at all times be open to reasonable challenge. The proposed Investigatory Powers legislation, to the extent that it consolidates and clarifies mostly existing provisions, is itself an important response to that requirement. The Government should continue to consult and explain fully the likely implications of the proposed legislation. (Paragraph 76)	The Government will continue to consult broadly on the provisions in the Bill and its implementation.
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	TAB members are currently appointed on the basis of their knowledge and understanding of the cost and technical feasibility of providing permanent interception capabilities. In light of the proposed changes to its remit under the IP Bill, the Government is keen to ensure that members can give proper consideration to requirements detailed in data retention notices and technical capability notices. The membership of the Board will be audited to identify any gaps in knowledge; these will be addressed as a priority through the recruitment of new members.

	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)	Furthermore, the Chair may call on individuals to share expertise to assist the group in deciding reasonable costs and the technical feasibility of an obligation. The composition of the TAB has been re-examined and we intend to ensure it is sufficiently flexible such that particular expertise can be sought as required. This will be handled in secondary legislation, which will be published during the Bill's passage. The TAB terms of reference will set out how particular disputes will be dealt with.
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)	A number of bodies already exist to bring industry and government together in matters of interception and communications data, such as the Telecommunications Industry Security Advisory Council (TISAC) and the Interception and Communications Data Strategy Groups (LISG and CDSG respectively). In addition, the Investigatory Powers Commissioner will have access to an expanded team of technical inspectors, in-house legal advisers and a communications expert, who can provide information and advice on the implications of the evolution of the internet, digital technology and infrastructure. The Commissioner will have a budget to acquire further technical resource deemed necessary to fulfil their new remit.

ISBN 978-1-4741-2953-4